SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 28 June 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-2023-3432	Server-Side Request Forgery (SSRF) in GitHub repository plantuml/plantuml prior to 1.2023.9.	10.0	More Details
CVE-2023-35152	XWiki Platform is a generic wiki platform. Starting in version 12.9-rc-1 and prior to versions 14.4.8, 14.10.6, and 15.1, any logged in user can add dangerous content in their first name field and see it executed with programming rights. Leading to rights escalation. The vulnerability has been fixed on XWiki 14.4.8, 14.10.6, and 15.1. As a workaround, one may apply the patch manually.	9.9	More Details
CVE-2023-35150	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 2.40m-2 and prior to versions 14.4.8, 14.10.4, and 15.0, any user with view rights on any document can execute code with programming rights, leading to remote code execution by crafting an url with a dangerous payload. The problem has been patched in XWiki 15.0, 14.10.4 and 14.4.8.	9.9	More Details
CVE-2023-34465	XWiki Platform is a generic wiki platform. Starting in version 11.8-rc-1 and prior to versions 14.4.8, 14.10.6, and 15.2, `Mail.MailConfig` can be edited by any logged-in user by default. Consequently, they can change the mail obfuscation configuration and view and edit the mail sending configuration, including the smtp domain name and credentials. The problem has been patched in XWiki 14.4.8, 14.10.6, and 15.1. As a workaround, the rights of the `Mail.MailConfig` page can be manually updated so that only a set of trusted users can view, edit and delete it (e.g., the `XWiki.XWikiAdminGroup` group).	9.9	More Details
CVE-2023-36355	TP-Link TL-WR940N V4 was discovered to contain a buffer overflow via the ipStart parameter at /userRpm/WanDynamicIpV6CfgRpm. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted GET request.	9.9	More Details
CVE-2023-34340	Improper Authentication vulnerability in Apache Software Foundation Apache Accumulo. This issue affects Apache Accumulo: 2.1.0. Accumulo 2.1.0 contains a defect in the user authentication process that may succeed when invalid credentials are provided. Users are advised to upgrade to 2.1.1.	9.8	More Details
CVE-2022-48333	Widevine Trusted Application (TA) 5.0.0 through 5.1.1 has a drm_verify_keys prefix_len+feature_name_len integer overflow and resultant buffer overflow.	9.8	More Details
CVE-2023-3197	The MStore API plugin for WordPress is vulnerable to Unauthenticated Blind SQL Injection via the 'id' parameter in versions up to, and including, 4.0.1 due to insufficient escaping on the user supplied parameters and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.8	More Details
CVE-2023-36660	The OCB feature in libnettle in Nettle 3.9 before 3.9.1 allows memory corruption.	9.8	More Details
CVE-2023-30261	Command Injection vulnerability in OpenWB 1.6 and 1.7 allows remote attackers to run arbitrary commands via crafted GET request.	9.8	More Details
CVE-2022-48331	Widevine Trusted Application (TA) 5.0.0 through 5.1.1 has a drm_save_keys feature_name_len integer overflow and resultant buffer overflow.	9.8	More Details
CVE-2022-48332	Widevine Trusted Application (TA) 5.0.0 through 5.1.1 has a drm_save_keys file_name_len integer overflow and resultant buffer overflow.	9.8	More Details
CVE-2022-48334	Widevine Trusted Application (TA) 5.0.0 through 5.1.1 has a drm_verify_keys total_len+file_name_len integer overflow and resultant buffer overflow.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32419	The issue was addressed with improved bounds checks. This issue is fixed in iOS 16.5 and iPadOS 16.5. A remote attacker may be able to cause arbitrary code execution.	9.8	More Details
CVE-2022-48335	Widevine Trusted Application (TA) 5.0.0 through 7.1.1 has a PRDiagVerifyProvisioning integer overflow and resultant buffer overflow.	9.8	More Details
CVE-2022-48336	Widevine Trusted Application (TA) 5.0.0 through 7.1.1 has a PRDiagParseAndStoreData integer overflow and resultant buffer overflow.	9.8	More Details
CVE-2021-31635	Server-Side Template Injection (SSTI) vulnerability in jFinal v.4.9.08 allows a remote attacker to execute arbitrary code via the template function.	9.8	More Details
CVE-2023-33404	An Unrestricted Upload vulnerability, due to insufficient validation on UploadControlled.cs file, in BlogEngine.Net version 3.3.8.0 and earlier allows remote attackers to execute remote code.	9.8	More Details
CVE-2023-32557	A path traversal vulnerability in the Trend Micro Apex One and Apex One as a Service could allow an unauthenticated attacker to upload an arbitrary file to the Management Server which could lead to remote code execution with system privileges.	9.8	More Details
CVE-2023-30945	Multiple Services such as VHS(Video History Server) and VCD(Video Clip Distributor) and Clips2 were discovered to be vulnerable to an unauthenticated arbitrary file read/write vulnerability due to missing input validation on filenames. A malicious attacker could read sensitive files from the filesystem or write/delete arbitrary files on the filesystem as well.	9.8	More Details
CVE-2023-2032	The Custom 404 Pro WordPress plugin before 3.8.1 does not properly sanitize database inputs, leading to multiple SQL Injection vulnerabilities.	9.8	More Details
CVE-2023-2068	The File Manager Advanced Shortcode WordPress plugin through 2.3.2 does not adequately prevent uploading files with disallowed MIME types when using the shortcode. This leads to RCE in cases where the allowed MIME type list does not include PHP files. In the worst case, this is available to unauthenticated users.	9.8	More Details
CVE-2023-2601	The wpbrutalai WordPress plugin before 2.0.0 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by admin via CSRF.	9.8	More Details
CVE-2023-33584	Sourcecodester Enrollment System Project V1.0 is vulnerable to SQL Injection (SQLI) attacks, which allow an attacker to manipulate the SQL queries executed by the application. The application fails to properly validate user-supplied input in the username and password fields during the login process, enabling an attacker to inject malicious SQL code.	9.8	More Details
CVE-2020-19902	Directory Traversal vulnerability found in Cryptoprof WCMS v.0.3.2 allows a remote attacker to execute arbitrary code via the wex/cssjs.php parameter.	9.8	More Details
CVE-2023-32412	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, iOS 15.7.6 and iPadOS 15.7.6, macOS Big Sur 11.7.7, macOS Monterey 12.6.6, iOS 16.5 and iPadOS 16.5. A remote attacker may be able to cause unexpected app termination or arbitrary code execution.	9.8	More Details
CVE-2023-32571	Dynamic Linq 1.0.7.10 through 1.2.25 before 1.3.0 allows attackers to execute arbitrary code and commands when untrusted input to methods including Where, Select, OrderBy is parsed.	9.8	More Details
CVE-2023-32387	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.7.7, macOS Monterey 12.6.6, macOS Ventura 13.4. A remote attacker may be able to cause unexpected app termination or arbitrary code execution.	9.8	More Details
CVE-2023-29931	laravel-s 3.7.35 is vulnerable to Local File Inclusion via /src/Illuminate/Laravel.php.	9.8	More Details
CVE-2023-34601	Jeesite before commit 10742d3 was discovered to contain a SQL injection vulnerability via the component ${businessTable} at /act/ActDao.xml.	9.8	More Details
CVE-2023-29711	An incorrect access control issue was discovered in Interlink PSG-5124 version 1.0.4, allows attackers to execute arbitrary code via crafted GET request.	9.8	More Details
CVE-2023-34939	Onlyoffice Community Server before v12.5.2 was discovered to contain a remote code execution (RCE) vulnerability via the component UploadProgress.ashx.	9.8	More Details
CVE-2023-36097	funadmin v3.3.2 and v3.3.3 are vulnerable to Insecure file upload via the plugins install.	9.8	More Details
CVE-2022-22630	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Big Sur 11.6.6, macOS Monterey 12.3, Security Update 2022-004 Catalina. A remote user may cause an unexpected app termination or arbitrary code execution	9.8	More Details
CVE-2023-2611	Advantech R-SeeNet versions 2.4.22 is installed with a hidden root-level user that is not available in the users list. This hidden user has a password that cannot be changed by users.	9.8	More Details
CVE-2023-30258	Command Injection vulnerability in MagnusSolution magnusbilling 6.x and 7.x allows remote attackers to run arbitrary commands via unauthenticated HTTP request.	9.8	More Details
CVE-2023-33299	A deserialization of untrusted data in Fortinet FortiNAC below 7.2.1, below 9.4.3, below 9.2.8 and all earlier versions of 8.x allows attacker to execute unauthorized code or commands via specifically crafted request on inter-server communication port. Note FortiNAC versions 8.x will not be fixed.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3326	pam_krb5 authenticates a user by essentially running kinit with the password, getting a ticket-granting ticket (tgt) from the Kerberos KDC (Key Distribution Center) over the network, as a way to verify the password. However, if a keytab is not provisioned on the system, pam_krb5 has no way to validate the response from the KDC, and essentially trusts the tgt provided over the network as being valid. In a non-default FreeBSD installation that leverages pam_krb5 for authentication and does not have a keytab provisioned, an attacker that is able to control both the password and the KDC responses can return a valid tgt, allowing authentication to occur for any user on the system.	9.8	More Details
CVE-2023-0971	A logic error in SiLabs Z/IP Gateway SDK 7.18.02 and earlier allows authentication to be bypassed, remote administration of Z-Wave controllers, and S0/S2 encryption keys to be recovered.	9.6	More Details
CVE-2023-0972	Description: A vulnerability in SiLabs Z/IP Gateway 7.18.01 and earlier allows an unauthenticated attacker within Z-Wave range to overflow a stack buffer, leading to arbitrary code execution.	9.6	More Details
CVE-2023-3110	Description: A vulnerability in SiLabs Unify Gateway 1.3.1 and earlier allows an unauthenticated attacker within Z-Wave range to overflow a stack buffer, leading to arbitrary code execution.	9.6	More Details
CVE-2023-35156	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Users are able to forge an URL with a payload allowing to inject Javascript in the page (XSS). It's possible to exploit the delete template to perform a XSS, e.g. by using URL such as: > xwiki/bin/get/FlamingoThemes/Cerulean?xpage=xpart&vm=delete.vm&xredirect=javascript:alert(document.domain). This vulnerability exists since XWiki 6.0-rc-1. The vulnerability has been patched in XWiki 14.10.6 and 15.1. Note that a partial patch has been provided in 14.10.5 but wasn't enough to entirely fix the vulnerability.	9.6	More Details
CVE-2023-35162	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Users are able to forge an URL with a payload allowing to inject Javascript in the page (XSS). It's possible to exploit the previewactions template to perform a XSS, e.g. by using URL such as: > <hostname>/xwiki/bin/get/FlamingoThemes/Cerulean xpage=xpart&vm=previewactions.vm&xcontinue=javascript:alert(document.domain). This vulnerability exists since XWiki 6.1-rc-1. The vulnerability has been patched in XWiki 14.10.5 and 15.1-rc-1.	9.6	More Details
CVE-2023-35161	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Users are able to forge an URL with a payload allowing to inject Javascript in the page (XSS). It's possible to exploit the DeleteApplication page to perform a XSS, e.g. by using URL such as: > xwiki/bin/view/AppWithinMinutes/DeleteApplication?appName=Menu&resolve=true&xredirect=javascript:alert(document.domain). This vulnerability exists since XWiki 6.2-milestone-1. The vulnerability has been patched in XWiki 14.10.5 and 15.1-rc-1.	9.6	More Details
CVE-2023-35160	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Users are able to forge an URL with a payload allowing to inject Javascript in the page (XSS). It's possible to exploit the resubmit template to perform a XSS, e.g. by using URL such as: > xwiki/bin/view/XWiki/Main xpage=resubmit&resubmit=javascript:alert(document.domain)&xback=javascript:alert(document.domain). This vulnerability exists since XWiki 2.5-milestone-2. The vulnerability has been patched in XWiki 14.10.5 and 15.1-rc-1.	9.6	More Details
CVE-2023-35159	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Users are able to forge an URL with a payload allowing to inject Javascript in the page (XSS). It's possible to exploit the deletespace template to perform a XSS, e.g. by using URL such as: > xwiki/bin/deletespace/Sandbox/?xredirect=javascript:alert(document.domain). This vulnerability exists since XWiki 3.4-milestone-1. The vulnerability has been patched in XWiki 14.10.5 and 15.1-rc-1.	9.6	More Details
CVE-2023-35158	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Users are able to forge an URL with a payload allowing to inject Javascript in the page (XSS). It's possible to exploit the restore template to perform a XSS, e.g. by using URL such as: > /xwiki/bin/view/XWiki/Main?xpage=restore&showBatch=true&xredirect=javascript:alert(document.domain). This vulnerability exists since XWiki 9.4-rc-1. The vulnerability has been patched in XWiki 14.10.5 and 15.1-rc-1.	9.6	More Details
CVE-2023-3128	Grafana is validating Azure AD accounts based on the email claim. On Azure AD, the profile email field is not unique and can be easily modified. This leads to account takeover and authentication bypass when Azure AD OAuth is configured with a multi-tenant app.	9.4	More Details
CVE-2023-2989	Fortra Globalscape EFT versions before 8.1.0.16 suffer from an out of bounds memory read in their administration server, which can allow an attacker to crash the service or bypass authentication if successfully exploited	9.1	More Details
CVE-2023-1722	Yoga Class Registration System version 1.0 allows an administrator to execute commands on the server. This is possible because the application does not correctly validate the thumbnails of the classes uploaded by the administrators.	9.1	More Details
CVE-2023-1721	Yoga Class Registration System version 1.0 allows an administrator to execute commands on the server. This is possible because the application does not correctly validate the thumbnails of the classes uploaded by the administrators.	9.1	More Details
CVE-2023-32521	A path traversal exists in a specific service dll of Trend Micro Mobile Security (Enterprise) 9.8 SP5 which could allow an unauthenticated remote attacker to delete arbitrary files.	9.1	More Details
CVE-2023-35153	XWiki Platform is a generic wiki platform. Starting in version 5.4.4 and prior to versions 14.4.8, 14.10.4, and 15.0, a stored cross-site scripting vulnerability can be exploited by users with edit rights by adding a `AppWithinMinutes.FormFieldCategoryClass` class on a page and setting the payload on the page title. Then, any user visiting `/xwiki/bin/view/AppWithinMinutes/ClassEditSheet` executes the payload. The issue has been patched in XWiki 14.4.8, 14.10.4, and 15.0. As a workaround, update `AppWithinMinutes.ClassEditSheet` with a patch.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34464	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 2.2.1 until versions 14.4.8, 14.10.5, and 15.1RC1 of org.xwiki.platform:xwiki-platform-web and any version prior to 14.4.8, 14.10.5, and 15.1.RC1 of org.xwiki.platform:xwiki-platform-web-templates, any user who can edit a document in a wiki like the user profile can create a stored cross-site scripting attack. The attack occurs by putting plain HTML code into that document and then tricking another user to visit that document with the `displaycontent` or `rendercontent` template and plain output syntax. If a user with programming rights is tricked into visiting such a URL, arbitrary actions be performed with this user's rights, impacting the confidentiality, integrity, and availability of the whole XWiki installation. This has been patched in XWiki 14.4.8, 14.10.5 and 15.1RC1 by setting the content type of the response to plain text when the output syntax is not an HTML syntax.	9.0	More Details
CVE-2023-35169	PHP-IMAP is a wrapper for common IMAP communication without the need to have the php-imap module installed / enabled. Prior to version 5.3.0, an unsanitized attachment filename allows any unauthenticated user to leverage a directory traversal vulnerability, which results in a remote code execution vulnerability. Every application that stores attachments with `Attachment::save()` without providing a `$filename` or passing unsanitized user input is affected by this attack. An attacker can send an email with a malicious attachment to the inbox, which gets crawled with `webklex/php-imap` or `webklex/laravel-imap`. Prerequisite for the vulnerability is that the script stores the attachments without providing a `$filename`, or providing an unsanitized `$filename`, in `src/Attachment::save(string $path, string $filename = null)`. In this case, where no `$filename` gets passed into the `Attachment::save()` method, the package would use a series of unsanitized and insecure input values from the mail as fallback. Even if a developer passes a `$filename` into the `Attachment::save()` method, e.g. by passing the name or filename of the mail attachment itself (from email headers), the input values never get sanitized by the package. There is also no restriction about the file extension (e.g. ".php") or the contents of a file. This allows an attacker to upload malicious code of any type and content at any location where the underlying user has write permissions. The attacker can also overwrite existing files and inject malicious code into files that, e.g. get executed by the system via cron or requests. Version 5.3.0 contains a patch for this issue.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2023-3420	Type Confusion in V8 in Google Chrome prior to 114.0.5735.198 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium s
CVE-2023-36630	In CloudPanel before 2.3.1, insecure file upload leads to privilege escalation and authentication bypass.
CVE-2023-34203	In Progress OpenEdge OEM (OpenEdge Management) and OEE (OpenEdge Explorer) before 12.7, a remote user (who has any OEM or OEE role) could perform a UI before 11.7.16, 12.x before 12.2.12, and 12.3.x through 12.6.x before 12.7.
CVE-2023-3422	Use after free in Guest View in Google Chrome prior to 114.0.5735.198 allowed an attacker who convinced a user to install a malicious extension to potentially exploit h
CVE-2023-36274	LibreDWG v0.12.5 was discovered to contain a heap buffer overflow via the function bit_write_TF at bits.c.
CVE-2023-3421	Use after free in Media in Google Chrome prior to 114.0.5735.198 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium
CVE-2020-18418	A Cross site request forgery (CSRF) vulnerability was discovered in FeiFeiCMS v4.1.190209, which allows attackers to create administrator accounts via /index.php?s=
CVE-2023-36345	A Cross-Site Request Forgery (CSRF) in POS Codekop v2.0 allows attackers to escalate privileges.
CVE-2023-32530	Vulnerable modules of Trend Micro Apex Central (on-premise) contain vulnerabilities which would allow authenticated users to perform a SQL injection that could lead t exploit these vulnerabilities. This is similar to, but not identical to CVE-2023-32529.
CVE-2023-36348	POS Codekop v2.0 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the filename parameter.
CVE-2023-32529	Vulnerable modules of Trend Micro Apex Central (on-premise) contain vulnerabilities which would allow authenticated users to perform a SQL injection that could lead t exploit these vulnerabilities. This is similar to, but not identical to CVE-2023-32530.
CVE-2023-31469	A REST interface in Apache StreamPipes (versions 0.69.0 to 0.91.0) was not properly restricted to admin-only access. This allowed a non-admin user with valid login c StreamPipes 0.92.0.

CVE Number	Description
CVE-2023-3423	Weak Password Requirements in GitHub repository cloudexplorer-dev/cloudexplorer-lite prior to v 1.2.0.
CVE-2023-36239	libming listswf 0.4.7 was discovered to contain a buffer overflow in the parseSWF_DEFINEFONTINFO() function at parser.c.
CVE-2023-2628	The KiviCare WordPress plugin before 3.2.1 does not have CSRF checks (either flawed or missing completely) in various AJAX actions, which could allow attackers to arbitrary appointments/medical records/etc, create/update various users (patients, doctors etc)
CVE-2023-32527	Trend Micro Mobile Security (Enterprise) 9.8 SP5 contains vulnerable .php files that could allow a remote attacker to execute arbitrary code on affected installations. Pl exploit this vulnerability. This is similar to, but not identical to CVE-2023-32528.
CVE-2023-36663	it-novum openITCOCKPIT (aka open IT COCKPIT) 4.6.4 before 4.6.5 allows SQL Injection (by authenticated users) via the sort parameter of the API interface.
CVE-2023-35155	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Users are able to forge an URL with a payload allowing to inject Java host>/xwiki/bin/view/Main/? viewer=share&send=1&target=&target=%3Cimg+src+onerror%3Dalert%28document.domain%29%3E+%3Cimg+src+onerror%3Dalert%28document.domain%29%3E+ where `<xwiki-host>` is the URL of your XWiki installation. The vulnerability has been patched in XWiki 15.0-rc-1, 14.10.4, and 14.4.8.
CVE-2023-34672	Improper Access Control leads to adding a high-privilege user affecting Elenos ETG150 FM transmitter running on version 3.12 by exploiting user's role within the admi
CVE-2023-34671	Improper Access Control leads to privilege escalation affecting Elenos ETG150 FM transmitter running on version 3.12 by exploiting user's role in the user profile. An at
CVE-2023-32439	A type confusion issue was addressed with improved checks. This issue is fixed in iOS 16.5.1 and iPadOS 16.5.1, iOS 15.7.7 and iPadOS 15.7.7, macOS Ventura 13.4 of a report that this issue may have been actively exploited.
CVE-2023-30260	Command injection vulnerability in RaspAP raspap-webgui 2.8.8 and earlier allows remote attackers to run arbitrary commands via crafted POST request to hostapd se
CVE-2023-32373	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, iOS 15.7.6 and iPadO code execution. Apple is aware of a report that this issue may have been actively exploited.
CVE-2022-3372	There is a CSRF vulnerability on Netman-204 version 02.05. An attacker could manage to change administrator passwords through a Cross Site Request Forgery due administrator panel, being able to modify different parameters that are critical for industrial operations.
CVE-2022-45287	An access control issue in Registration.aspx of Temenos CWX 8.5.6 allows authenticated attackers to escalate privileges and perform arbitrary Administrative comman
CVE-2023-36252	An issue in Ateme Flamingo XL v.3.6.20 and XS v.3.6.5 allows a remote authenticated attacker to execute arbitrary code and cause a denial of service via a the sessio
CVE-2023-2996	The Jetpack WordPress plugin before 12.1.1 does not validate uploaded files, allowing users with author roles or above to manipulate existing files on the site, deleting
CVE-2023-2877	The Formidable Forms WordPress plugin before 6.3.1 does not adequately authorize the user or validate the plugin URL in its functionality for installing add-ons. This a WordPress.org plugin repository onto the site, leading to Remote Code Execution.
CVE-2020-20210	Bludit 3.9.2 is vulnerable to Remote Code Execution (RCE) via /admin/ajax/upload-images.
CVE-2023-32524	Affected versions of Trend Micro Mobile Security (Enterprise) 9.8 SP5 contain some widgets that would allow a remote user to bypass authentication and potentially ch the target system in order to exploit these vulnerabilities. This is similar to, but not identical to CVE-2023-32523.
CVE-2023-3256	Advantech R-SeeNet versions 2.4.22 allows low-level users to access and load the content of local files.

CVE Number	Description
CVE-2023-32523	Affected versions of Trend Micro Mobile Security (Enterprise) 9.8 SP5 contain some widgets that would allow a remote user to bypass authentication and potentially ch the target system in order to exploit these vulnerabilities. This is similar to, but not identical to CVE-2023-32524.
CVE-2023-32435	A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3, Safari 16.4, iOS 16.4 and iPadOS 16.4, iOS 1 that this issue may have been actively exploited against versions of iOS released before iOS 15.7.
CVE-2023-36271	LibreDWG v0.12.5 was discovered to contain a heap buffer overflow via the function bit_wcs2nlen at bits.c.
CVE-2023-36272	LibreDWG v0.12.5 was discovered to contain a heap buffer overflow via the function bit_utf8_to_TU at bits.c.
CVE-2023-36273	LibreDWG v0.12.5 was discovered to contain a heap buffer overflow via the function bit_calc_CRC at bits.c.
CVE-2023-32528	Trend Micro Mobile Security (Enterprise) 9.8 SP5 contains vulnerable .php files that could allow a remote attacker to execute arbitrary code on affected installations. Pl exploit this vulnerability. This is similar to, but not identical to CVE-2023-32527.
CVE-2023-35172	NextCloud Server and NextCloud Enterprise Server provide file storage for Nextcloud, a self-hosted productivity platform. In NextCloud Server versions 25.0.0 until 25. 23.0.0 until 23.0.12.7, 24.0.0 until 24.0.12.2, 25.0.0 until 25.0.7, and 26.0.0 until 26.0.2, an attacker can bruteforce the password reset links. Nextcloud Server n 25.0.7 a patch for this issue. No known workarounds are available.
CVE-2023-32320	Nextcloud Server is a data storage system for Nextcloud, a self-hosted productivity platform. When multiple requests are sent in parallel, all of them were executed eve someone to send as many requests the server could handle in parallel to bruteforce protected details instead of the configured limit, default 8. Nextcloud Server versior and 26.0.2 contain patches for this issue.
CVE-2023-35174	Livebook is a web application for writing interactive and collaborative code notebooks. On Windows, it is possible to open a `livebook://` link from a browser which open Windows is potentially vulnerable to arbitrary code execution when they expect Livebook to be opened from browser. This vulnerability has been fixed in version 0.8.2 a
CVE-2023-32409	The issue was addressed with improved bounds checks. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, iOS 15.7.8 and iPadOS 15.7.8, Safari 16 aware of a report that this issue may have been actively exploited.
CVE-2023-32414	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.4. An app may be able to break out of its sandbox.
CVE-2022-47593	Auth. (subscriber+) SQL Injection (SQLi) vulnerability in RapidLoad RapidLoad Power-Up for Autoptimize plugin <= 1.6.35 versions.
CVE-2023-35157	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible to perform an XSS by forging a request to a delete attac token of the user, or if the user ignores the warning about the missing CSRF token. The vulnerability has been patched in XWiki 15.1-rc-1 and XWiki 14.10.6.
CVE-2023-35928	Nextcloud Server is a space for data storage on Nextcloud, a self-hosted productivity playform. In NextCloud Server versions 25.0.0 until 25.0.7 and 26.0.0 until 26.0.2 22.0.0 until 22.2.10.12, 23.0.0 until 23.0.12.7, 24.0.0 until 24.0.12.2, 25.0.0 until 25.0.7, and 26.0.0 until 26.0.2, a user could use this functionality to get access to the lo versions 25.0.7 and 26.0.2 and NextCloud Enterprise Server versions 19.0.13.9, 20.0.14.14, 21.0.9.12, 22.2.10.12, 23.0.12.7, 24.0.12.2, 25.0.7, and 26.0.2. Three worl disabled in "Administration" > "External storage" settings `…/index.php/settings/admin/externalstorages`. Change config setting to disallow users to create external stor FTP, Nextcloud, SFTP, and/or WebDAV.
CVE-2023-28956	IBM Spectrum Protect Backup-Archive Client 8.1.0.0 through 8.1.17.2 may allow a local user to escalate their privileges due to improper access controls.
CVE-2023-3113	An unauthenticated XML external entity injection (XXE) vulnerability exists in LXCA's Common Information Model (CIM) server that could result in read-only access to s
CVE-2023-28073	Dell BIOS contains an improper authentication vulnerability. A locally authenticated malicious user may potentially exploit this vulnerability by bypassing certain authent
CVE-2023-28799	A URL parameter during login flow was vulnerable to injection. An attacker could insert a malicious domain in this parameter, which would redirect the user after auth a
CVE-2023-34418	A valid, authenticated LXCA user may be able to gain unauthorized access to events and other data stored in LXCA due to a SQL injection vulnerability in a specific we

CVE Number	Description
CVE-2023-2842	The WP Inventory Manager WordPress plugin before 2.1.0.14 does not have CSRF checks, which could allow attackers to make logged-in admins delete Inventory Iter
CVE-2023-28094	Pega platform clients who are using versions 7.4 through 8.8.x and have upgraded from a version prior to 8.x may be utilizing default credentials.
CVE-2023-35801	A directory traversal vulnerability in Safe Software FME Server before 2022.2.5 allows an attacker to bypass validation when editing a network-based resource connect to have access to a user account with write privileges. FME Flow 2023.0 is also a fixed version.
CVE-2023-28800	When using local accounts for administration, the redirect url parameter was not encoded correctly, allowing for an XSS attack providing admin login.
CVE-2023-20892	The vCenter Server contains a heap overflow vulnerability due to the usage of uninitialized memory in the implementation of the DCERPC protocol. A malicious actor w underlying operating system that hosts vCenter Server.
CVE-2023-32522	A path traversal exists in a specific dll of Trend Micro Mobile Security (Enterprise) 9.8 SP5 which could allow an authenticated remote attacker to delete arbitrary files. F exploit this vulnerability.
CVE-2023-34923	XML Signature Wrapping (XSW) in SAML-based Single Sign-on feature in TOPdesk v12.10.12 allows bad actors with credentials to authenticate with the Identity Provi
CVE-2023-34463	DataEase is an open source data visualization analysis tool to analyze data and gain insight into business trends. In affected versions Unauthorized users can delete a are no known workarounds for this vulnerability.
CVE-2023-20895	The VMware vCenter Server contains a memory corruption vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCent
CVE-2023-20893	The VMware vCenter Server contains a use-after-free vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Se
CVE-2023-20894	The VMware vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCe
CVE-2023-35926	Backstage is an open platform for building developer portals. The Backstage scaffolder-backend plugin uses a templating library that requires sandbox, as it by design vulnerabilities and existing vulnerabilities that may not have a fix, the plugin has switched to using a different sandbox library. A malicious actor with write access to a re scaffolder-backend instance. This was only exploitable in the template YAML definition itself and not by user input data. This is vulnerability is fixed in version 1.15.0 of
CVE-2023-32353	A logic issue was addressed with improved checks. This issue is fixed in iTunes 12.12.9 for Windows. An app may be able to elevate privileges.
CVE-2023-34395	Improper Neutralization of Argument Delimiters in a Command ('Argument Injection') vulnerability in Apache Software Foundation Apache Airflow ODBC Provider. In O allow the loading of arbitrary dynamic-link libraries, resulting in command execution. Starting version 4.0.0 driver can be set only from the hook constructor. This issue a
CVE-2023-32405	A logic issue was addressed with improved checks. This issue is fixed in macOS Big Sur 11.7.7, macOS Monterey 12.6.6, macOS Ventura 13.4. An app may be able to
CVE-2023-36664	Artifex Ghostscript through 10.01.2 mishandles permission validation for pipe devices (with the %pipe% prefix or the | pipe character prefix).
CVE-2023-25515	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability where unexpected untrusted data is parsed, which may lead to code execution, denial of se
CVE-2023-23539	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.2. Mounting a maliciously crafted Samba network sha
CVE-2023-3302	Improper Neutralization of Formula Elements in a CSV File in GitHub repository admidio/admidio prior to 4.2.9.

CVE Number	Description
CVE-2023-25004	A maliciously crafted pskernel.dll file in Autodesk products is used to trigger integer overflow vulnerabilities. Exploitation of these vulnerabilities may lead to code execu
CVE-2023-25001	A maliciously crafted SKP file in Autodesk Navisworks 2023 and 2022 be used to trigger use-after-free vulnerability. Exploitation of this vulnerability may lead to code e
CVE-2023-23516	The issue was addressed with improved memory handling. This issue is fixed in macOS Big Sur 11.7.3, macOS Ventura 13.2, macOS Monterey 12.6.3. An app may be
CVE-2023-25002	A maliciously crafted SKP file in Autodesk products is used to trigger use-after-free vulnerability. Exploitation of this vulnerability may lead to code execution.
CVE-2023-32380	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.7.7, macOS Monterey 12.6.6, macOS Ventura 13
CVE-2023-32384	A buffer overflow was addressed with improved bounds checking. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, iOS 15.7.6 and iPadOS 15.7.6, arbitrary code execution.
CVE-2023-32398	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, iOS 15.7.6 and iPadO execute arbitrary code with kernel privileges.
CVE-2023-34144	An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges o target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34145.
CVE-2023-32434	An integer overflow was addressed with improved input validation. This issue is fixed in watchOS 9.5.2, macOS Big Sur 11.7.8, iOS 15.7.7 and iPadOS 15.7.7, macOS execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15
CVE-2023-25307	nothub mrpack-install <= v0.16.2 is vulnerable to Directory Traversal.
CVE-2023-29068	A maliciously crafted file consumed through pskernel.dll file could lead to memory corruption vulnerabilities. These vulnerabilities in conjunction with other vulnerabilities
CVE-2023-34148	An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerabilit
CVE-2023-34147	An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerabilit
CVE-2023-27908	A maliciously crafted DLL file can be forced to write beyond allocated boundaries in the Autodesk installer when parsing the DLL files and could lead to a Privilege Esca
CVE-2023-27930	A type confusion issue was addressed with improved checks. This issue is fixed in iOS 16.5 and iPadOS 16.5, watchOS 9.5, tvOS 16.5, macOS Ventura 13.4. An app
CVE-2023-28929	Trend Micro Security 2021, 2022, and 2023 (Consumer) are vulnerable to a DLL Hijacking vulnerability which could allow an attacker to use a specific executable file as file is started.
CVE-2023-36193	Gifsicle v1.9.3 was discovered to contain a heap buffer overflow via the ambiguity_error component at /src/clp.c.
CVE-2023-34146	An exposed dangerous function vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate privileges attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This is a similar, but not identical vulnerabilit
CVE-2023-36631	Lack of access control in wfc.exe in Malwarebytes Binisoft Windows Firewall Control 6.9.2.0 allows local unprivileged users to bypass Windows Firewall restrictions via locked using a password."

CVE Number	Description
CVE-2023-36192	Sngrep v1.6.0 was discovered to contain a heap buffer overflow via the function capture_ws_check_packet at /src/capture.c.
CVE-2023-25003	A maliciously crafted pskernel.dll file in Autodesk AutoCAD 2023 and Maya 2022 may be used to trigger out-of-bound read write / read vulnerabilities. Exploitation of thi
CVE-2023-32351	A logic issue was addressed with improved checks. This issue is fixed in iTunes 12.12.9 for Windows. An app may be able to gain elevated privileges.
CVE-2023-34145	An untrusted search path vulnerability in the Trend Micro Apex One and Apex One as a Service security agent could allow a local attacker to escalate their privileges o target system in order to exploit this vulnerability. This is a similar, but not identical vulnerability as CVE-2023-34144.
CVE-2023-36243	FLVMeta v1.2.1 was discovered to contain a buffer overflow via the xml_on_metadata_tag_only function at dump_xml.c.
CVE-2023-36358	TP-Link TL-WR940N V2/V3/V4, TL-WR941ND V5/V6, TL-WR743ND V1 and TL-WR841N V8 were discovered to contain a buffer overflow in the component /userRpm/ GET request.
CVE-2023-36356	TP-Link TL-WR940N V2/V4/V6, TL-WR841N V8, TL-WR941ND V5, and TL-WR740N V1/V2 were discovered to contain a buffer read out-of-bounds via the component GET request.
CVE-2023-36357	An issue in the /userRpm/LocalManageControlRpm component of TP-Link TL-WR940N V2/V4/V6, TL-WR841N V8/V10, and TL-WR941ND V5 allows attackers to caus
CVE-2023-34254	The GLPI Agent is a generic management agent. Prior to version 1.5, if glpi-agent is running remoteinventory task against an Unix platform with ssh command, an adm privileges it uses. In the case, the agent is running with administration privileges, a malicious user could gain high privileges on the computer glpi-agent is running on. A vulnerability has been patched in glpi-agent 1.5.
CVE-2023-35927	NextCloud Server and NextCloud Enterprise Server provide file storage for Nextcloud, a self-hosted productivity platform. In NextCloud Server versions 25.0.0 until 25.(23.0.0 until 23.0.12.7, 24.0.0 until 24.0.12.2, 25.0.0 until 25.0.7, and 26.0.0 until 26.0.2, when two server are registered as trusted servers for each other and successfu the origin server. This would impact the available and shown information in certain places, such as the user search and avatar menu. If a manipulated user modifies the Enterprise Server 21.0.9.12, 22.2.10.12, 23.0.12.7, 24.0.12.2, 25.0.7, and 26.0.2 contain a patch for this issue. A workaround is available. Remove all trusted servers ir the local system addressbook with the following `occ dav:sync-system-addressbook`.
CVE-2023-35133	An issue in the logic used to check 0.0.0.0 against the cURL blocked hosts lists resulted in an SSRF risk. This flaw affects Moodle versions 4.2, 4.1 to 4.1.3, 4.0 to 4.0.8
CVE-2023-33141	Yet Another Reverse Proxy (YARP) Denial of Service Vulnerability
CVE-2023-35151	XWiki Platform is a generic wiki platform. Starting in version 7.3-milestone-1 and prior to versions 14.4.8, 14.10.6, and 15.1, ny user can call a REST endpoint and obta 14.4.8, 14.10.6, and 15.1. There is no known workaround.
CVE-2023-34467	XWiki Platform is a generic wiki platform. Starting in version 3.5-milestone-1 and prior to versions 14.4.8, 14.10.4, and 15.0-rc-1, the mail obfuscation configuration was containing the mail unobfuscated and users were able to filter and sort on the unobfuscated, allowing them to infer the mail content. The consequence was the possibili 14.10.4, and 15.0-rc-1.
CVE-2023-36284	An unauthenticated Time-Based SQL injection found in Webkul QloApps 1.6.0 via GET parameter date_from, date_to, and id_product allows a remote attacker to bypa database.
CVE-2023-35695	A remote attacker could leverage a vulnerability in Trend Micro Mobile Security (Enterprise) 9.8 SP5 to download a particular log file which may contain sensitive inform
CVE-2023-36359	TP-Link TL-WR940N V4, TL-WR841N V8/V10, TL-WR940N V2/V3 and TL-WR941ND V5/V6 were discovered to contain a buffer overflow in the component /userRpm/
CVE-2022-47614	Unauth. SQL Injection (SQLi) vulnerability in InspireUI MStore API plugin <= 3.9.7 versions.
CVE-2023-30362	Buffer Overflow vulnerability in coap_send function in libcoap library 4.3.1-103-g52cfd56 fixed in 4.3.1-120-ge242200 allows attackers to obtain sensitive information via

CVE Number	Description
CVE-2023-2992	An unauthenticated denial of service vulnerability exists in the SMM v1, SMM v2, and FPC management web server which can be triggered under crafted conditions. F
CVE-2023-36362	An issue in the rel_sequences component of MonetDB Server v11.45.17 and v11.46.0 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.
CVE-2023-36354	TP-Link TL-WR940N V4, TL-WR841N V8/V10, TL-WR740N V1/V2, TL-WR940N V2/V3, and TL-WR941ND V5/V6 were discovered to contain a buffer overflow in the c (DoS) via a crafted GET request.
CVE-2023-34188	The HTTP server in Mongoose before 7.10 accepts requests containing negative Content-Length headers. By sending a single attack payload over TCP, an attacker ca requests.
CVE-2023-29708	An issue was discovered in /cgi-bin/adm.cgi in WavLink WavRouter version RPT70HA1.x, allows attackers to force a factory reset via crafted payload.
CVE-2023-2990	Fortra Globalscape EFT versions before 8.1.0.16 suffer from a denial of service vulnerability, where a compressed message that decompresses to itself can cause infir
CVE-2023-36612	Directory traversal can occur in the Basecamp com.basecamp.bc3 application before 4.2.1 for Android, which may allow an attacker to write arbitrary files in the applica (containing sensitive information) to third-party applications by using a custom-crafted deeplink scheme.
CVE-2023-36632	The legacy email.utils.parseaddr function in Python through 3.11.4 allows attackers to trigger "RecursionError: maximum recursion depth exceeded while calling a Pyth that was supposed to contain a name and an e-mail address. NOTE: email.utils.parseaddr is categorized as a Legacy API in the documentation of the Python email pa vendor's perspective is that this is neither a vulnerability nor a bug. The email package is intended to have size limits and to throw an exception when limits are exceed
CVE-2023-36661	Shibboleth XMLTooling before 3.2.4, as used in OpenSAML and Shibboleth Service Provider, allows SSRF via a crafted KeyInfo element. (This is fixed in, for example,
CVE-2023-34924	H3C Magic B1STW B1STV100R012 was discovered to contain a stack overflow via the function SetAPInfoById. This vulnerability allows attackers to cause a Denial of
CVE-2023-1150	Uncontrolled resource consumption in Series WAGO 750-3x/-8x products may allow an unauthenticated remote attacker to DoS the MODBUS server with specially cra
CVE-2023-33289	The urlnorm crate through 0.1.4 for Rust allows Regular Expression Denial of Service (ReDos) via a crafted URL to lib.rs.
CVE-2023-3398	Denial of Service in GitHub repository jgraph/drawio prior to 18.1.3.
CVE-2023-25306	MultiMC Launcher <= 0.6.16 is vulnerable to Directory Traversal.
CVE-2023-2911	If the `recursive-clients` quota is reached on a BIND 9 resolver configured with both `stale-answer-enable yes;` and `stale-answer-client-timeout 0;`, a sequence of serv issue affects BIND 9 versions 9.16.33 through 9.16.41, 9.18.7 through 9.18.15, 9.16.33-S1 through 9.16.41-S1, and 9.18.11-S1 through 9.18.15-S1.
CVE-2023-2829	A `named` instance configured to run as a DNSSEC-validating recursive resolver with the Aggressive Use of DNSSEC-Validated Cache (RFC 8198) option (`synth-fron BIND 9 versions 9.16.8-S1 through 9.16.41-S1 and 9.18.11-S1 through 9.18.15-S1.
CVE-2023-2828	Every `named` instance configured to run as a recursive resolver maintains a cache database holding the responses to the queries it has recently sent to authoritative s configuration file; it defaults to 90% of the total amount of memory available on the host. When the size of the cache reaches 7/8 of the configured limit, a cache-cleanir the configured limit. It has been discovered that the effectiveness of the cache-cleaning algorithm used in `named` can be severely diminished by querying the resolver exceeded. This issue affects BIND 9 versions 9.11.0 through 9.16.41, 9.18.0 through 9.18.15, 9.19.0 through 9.19.13, 9.11.3-S1 through 9.16.41-S1, and 9.18.11-S1 th
CVE-2023-0026	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, netw established BGP session, and that message contains a specific, optional transitive attribute, this session will be torn down with an update message error. This issue ca issue is exploitable remotely as the respective attribute can propagate through unaffected systems and intermediate AS (if any). Continuous receipt of a BGP update cc these BGP session flaps which prompted Juniper SIRT to release this advisory out of cycle before fixed releases are widely available as there is an effective workarour 21.1R1 and later versions prior to 21.2R3-S6; 21.3 versions prior to 21.3R3-S5; 21.4 versions prior to 21.4R3-S4; 22.1 versions prior to 22.1R3-S4; 22.2 versions prior versions prior to 23.1R1-S1, 23.1R2. Juniper Networks Junos OS Evolved All versions prior to 20.4R3-S8-EVO; 21.1 version 21.1R1-EVO and later versions prior to 21 22.1R3-S4-EVO; 22.2 versions prior to 22.2R3-S2-EVO; 22.3 versions prior to 22.3R2-S2-EVO, 22.3R3-S1-EVO; 22.4 versions prior to 22.4R2-S1-EVO, 22.4R3-EVO;

CVE Number	Description
CVE-2023-27243	An access control issue in Makves DCAP v3.0.0.122 allows unauthenticated attackers to obtain cleartext credentials via a crafted web request to the product API.
CVE-2023-36301	Talend Data Catalog before 8.0-20230221 contain a directory traversal vulnerability in HeaderImageServlet.
CVE-2023-34981	A regression in the fix for bug 66512 in Apache Tomcat 11.0.0-M5, 10.1.8, 9.0.74 and 8.5.88 meant that, if a response did not include any HTTP headers no AJP SEND (mod_proxy_ajp) would use the response headers from the previous request leading to an information leak.
CVE-2023-29709	An issue was discovered in /cgi-bin/login_rj.cgi in Wildix WSG24POE version 103SP7D190822, allows attackers to bypass authentication.
CVE-2023-29860	An insecure permissions in /Taier/API/tenant/listTenant interface in DTStack Taier 1.3.0 allows attackers to view sensitive information via the getCookie method.
CVE-2023-36370	An issue in the gc_col component of MonetDB Server v11.45.17 and v11.46.0 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.
CVE-2023-36364	An issue in the rel_deps component of MonetDB Server v11.45.17 and v11.46.0 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.
CVE-2023-36365	An issue in the sql_trans_copy_key component of MonetDB Server v11.45.17 and v11.46.0 allows attackers to cause a Denial of Service (DoS) via crafted SQL statem
CVE-2023-36366	An issue in the log_create_delta component of MonetDB Server v11.45.17 and v11.46.0 allows attackers to cause Denial of Service (DoS) via crafted SQL statements.
CVE-2023-32397	A logic issue was addressed with improved state management. This issue is fixed in iOS 15.7.6 and iPadOS 15.7.6, macOS Big Sur 11.7.7, macOS Monterey 12.6.6, n
CVE-2020-18406	An issue was discovered in cmseasy v7.0.0 that allows user credentials to be sent in clear text due to no encryption of form data.
CVE-2023-3405	Unchecked parameter value in M-Files Server in versions before 23.6.12695.3 (excluding 23.2 SR2 and newer) allows anonymous user to cause denial of service
CVE-2023-36371	An issue in the GDKfree component of MonetDB Server v11.45.17 and v11.46.0 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.
CVE-2023-36367	An issue in the BLOBcmp component of MonetDB Server v11.45.17 and v11.46.0 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.
CVE-2023-36369	An issue in the list_append component of MonetDB Server v11.45.17 and v11.46.0 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.
CVE-2023-36363	An issue in the __nss_database_lookup component of MonetDB Server v11.45.17 and v11.46.0 allows attackers to cause a Denial of Service (DoS) via crafted SQL st
CVE-2023-36368	An issue in the cs_bind_ubat component of MonetDB Server v11.45.17 and v11.46.0 allows attackers to cause a Denial of Service (DoS) via crafted SQL statements.
CVE-2023-1724	Faveo Helpdesk Enterprise version 6.0.1 allows an attacker with agent permissions to perform privilege escalation on the application. This occurs because the applicati
CVE-2023-31867	Sage X3 version 12.14.0.50-0 is vulnerable to CSV Injection.

CVE Number	Description
CVE-2023-35154	Knowage is an open source analytics and business intelligence suite. Starting in version 6.0.0 and prior to version 8.1.8, an attacker can register and activate their acc user. This issue has been patched in version 8.1.8.
CVE-2023-34420	A valid, authenticated LXCA user with elevated privileges may be able to execute command injections through crafted calls to a specific web API.
CVE-2023-27083	An issue discovered in /admin.php in Pluck CMS 4.7.15 through 4.7.16-dev5 allows remote attackers to run arbitrary code via manage file functionality.
CVE-2023-24261	A vulnerability in GL.iNET GL-E750 Mudi before firmware v3.216 allows authenticated attackers to execute arbitrary code via a crafted POST request.
CVE-2019-25152	The Abandoned Cart Lite for WooCommerce and Abandoned Cart Pro for WooCommerce plugins for WordPress are vulnerable to Stored Cross-Site Scripting via mult and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in user input that will execute on the admin dashboard.
CVE-2023-3388	The Beautiful Cookie Consent Banner for WordPress is vulnerable to Stored Cross-Site Scripting via the 'nsc_bar_content_href' parameter in versions up to, and includ attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. A partial patch was made available in 2.10.1 and the issu
CVE-2023-2744	The ERP WordPress plugin before 1.12.4 does not properly sanitise and escape the `type` parameter in the `erp/v1/accounting/v1/people` REST API endpoint before u
CVE-2023-3393	Code Injection in GitHub repository fossbilling/fossbilling prior to 0.5.1.
CVE-2023-2592	The FormCraft WordPress plugin before 3.9.7 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploit
CVE-2023-2482	The Responsive CSS EDITOR WordPress plugin through 1.0 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL i
CVE-2023-32449	Dell PowerStore versions prior to 3.5 contain an improper verification of cryptographic signature vulnerability. An attacker can trick a high privileged user to install a mal
CVE-2023-28992	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Elliot Sowersby, RelyWP Coupon Affiliates – WooCommerce Affiliate Plugin plugin <= 5.4.3 versions.
CVE-2023-32357	An authorization issue was addressed with improved state management. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, macOS Big Sur 11.7.7, n files even after its permission is revoked.
CVE-2023-32420	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 16.5 and iPadOS 16.5, watchOS 9.5, tvOS 16.5, macOS Ventura 13.4.
CVE-2023-29424	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Plainware ShiftController Employee Shift Scheduling plugin <= 4.9.23 versions.
CVE-2023-3317	A use-after-free flaw was found in mt7921_check_offload_capability in drivers/net/wireless/mediatek/mt76/mt7921/init.c in wifi mt76/mt7921 sub-component in the Linu could even lead to a kernel information leak problem.
CVE-2023-29430	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in CTHthemes TheRoof theme <= 1.0.3 versions.
CVE-2023-29100	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Dream-Theme The7 plugin <= 11.6.0 versions.
CVE-2023-34021	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Andy Moyle Church Admin plugin <= 3.7.29 versions.

CVE Number	Description
CVE-2023-25518	NVIDIA Jetson contains a vulnerability in CBoot, where the PCIe controller is initialized without IOMMU, which may allow an attacker with physical access to the target denial of service, information disclosure, and loss of integrity.
CVE-2023-35932	jcvi is a Python library to facilitate genome assembly, annotation, and comparative genomics. A configuration injection happens when user input is considered by the ap that may lead to a command injection. The impact of a configuration injection may vary. Under some conditions, it may lead to command injection if there is for instance
CVE-2023-29427	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in TMS Booking for Appointments and Events Calendar – Amelia plugin <= 1.0.75 versions.
CVE-2023-34012	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Premium Addons for Elementor Premium Addons PRO plugin <= 2.8.24 versions.
CVE-2023-32960	Cross-Site Request Forgery (CSRF) vulnerability in UpdraftPlus.Com, DavidAnderson UpdraftPlus WordPress Backup Plugin <= 1.23.3 versions leads to sitewide Cros
CVE-2023-28750	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Ignazio Scimone Albo Pretorio On line plugin <= 4.6 versions.
CVE-2023-27450	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Teplitsa of social technologies Leyka plugin <= 3.29.2 versions.
CVE-2023-35918	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WooCommerce Bulk Stock Management plugin <= 2.2.33 versions.
CVE-2023-28166	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Aakif Kadiwala Tags Cloud Manager plugin <= 1.0.0 versions.
CVE-2023-28784	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Contest Gallery plugin <= 21.1.2 versions.
CVE-2023-27414	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Popup Box Team Popup box plugin <= 3.4.4 versions.
CVE-2023-28776	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution Continuous Image Carousel With Lightbox plugin <= 1.0.15 versions.
CVE-2023-27432	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WpSimpleTools Manage Upload Limit plugin <= 1.0.4 versions.
CVE-2023-23795	Cross-Site Request Forgery (CSRF) vulnerability in Muneeb Form Builder plugin <= 1.9.9.0 versions.
CVE-2023-0970	Multiple buffer overflow vulnerabilities in SiLabs Z/IP Gateway SDK version 7.18.01 and earlier allow an attacker with invasive physical access to a Z-Wave controller d
CVE-2023-33997	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Robin Wilson bbp style pack plugin <= 5.5.5 versions.
CVE-2023-28006	The OSD Bare Metal Server uses a cryptographic algorithm that is no longer considered sufficiently secure.
CVE-2023-32554	A Time-of-Check Time-Of-Use vulnerability in the Trend Micro Apex One and Apex One as a Service agent could allow a local attacker to escalate privileges on affecte system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32555.
CVE-2023-32413	A race condition was addressed with improved state handling. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, iOS 15.7.6 and iPadOS 15.7.6, mac privileges.

CVE Number	Description
CVE-2023-32555	A Time-of-Check Time-Of-Use vulnerability in the Trend Micro Apex One and Apex One as a Service agent could allow a local attacker to escalate privileges on affecte system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32554.
CVE-2020-18416	An cross site request forgery (CSRF) vulnerability discovered in Jymusic v2.0.0.,that allows attackers to execute arbitrary code via /admin.php?s=/addons/config.html&i
CVE-2023-30993	IBM Cloud Pak for Security (CP4S) 1.9.0.0 through 1.9.2.0 could allow an attacker with a valid API key for one tenant to access data from another tenant's account. IBM
CVE-2023-34839	A Cross Site Request Forgery (CSRF) vulnerability in Issabel issabel-pbx v.4.0.0-6 allows a remote attacker to gain privileges via a Custom CSRF exploit to create new
CVE-2020-18409	Cross Site Request Forgery (CSRF) vulnerability was discovered in CatfishCMS 4.8.63 that would allow attackers to obtain administrator permissions via /index.php/ad
CVE-2023-32480	Dell BIOS contains an Improper Input Validation vulnerability. An unauthenticated physical attacker may potentially exploit this vulnerability to perform arbitrary code ex
CVE-2023-28065	Dell Command | Update, Dell Update, and Alienware Update versions 4.8.0 and prior contain an Insecure Operation on Windows Junction / Mount Point vulnerability. A
CVE-2023-35165	AWS Cloud Development Kit (AWS CDK) is an open-source software development framework to define cloud infrastructure in code and provision it through AWS Cloud `eks.Cluster` and `eks.FargateCluster` constructs create two roles, `CreationRole` and `default MastersRole`, that have an overly permissive trust policy. The first, refer (e.g `KubernetesManifest`, `HelmChart`, ...) onto it. Users with CDK version higher or equal to 1.62.0 (including v2 users) may be affected. The second, referred to as t execute `kubectl` commands on the cluster. Users with CDK version higher or equal to 1.57.0 (including v2 users) may be affected. The issue has been fixed in `@aws they restrict the trust policy to the specific roles of lambda handlers that need it. There is no workaround available for CreationRole. To avoid creating the `default Maste
CVE-2023-28204	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, iOS 15.7.6 and iPadOS 15.7 aware of a report that this issue may have been actively exploited.
CVE-2023-34462	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. The `SniHand does not have an idle timeout, it can be used to make a TCP server using the `SniHandler` to allocate 16MB of heap. The `SniHandler` class is a handler that waits for For this matter it allocates a `ByteBuf` using the value defined in the `ClientHello` record. Normally the value of the packet should be smaller than the handshake packe `SslClientHelloHandler`. This vulnerability has been fixed in version 4.1.94.Final.
CVE-2023-31213	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WPBakery Page Builder plugin <= 6.13.0 versions.
CVE-2023-29435	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Zwaply Cryptocurrency All-in-One plugin <= 3.0.19 versions.
CVE-2023-29436	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Flyn San IFrame Shortcode plugin <= 1.0.5 versions.
CVE-2023-1783	OrangeScrum version 2.0.11 allows an external attacker to remotely obtain AWS instance credentials. This is possible because the application does not properly valida
CVE-2023-35090	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in StylemixThemes MasterStudy LMS WordPress Plugin – for Online Courses and Education plugin
CVE-2023-35168	DataEase is an open source data visualization analysis tool to analyze data and gain insight into business trends. Affected versions of DataEase has a privilege bypass hashes of passwords, username, email, and phone number. The vulnerability has been fixed in v1.18.8. Users are advised to upgrade. There are no known workaroun
CVE-2023-27413	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Shazzad Hossain Khan W4 Post List plugin <= 2.4.4 versions.
CVE-2023-27612	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Paul Ryley Site Reviews plugin <= 6.5.1 versions.

CVE Number	Description
CVE-2023-34240	Cloudexplorer-lite is an open source cloud software stack. Weak passwords can be easily guessed and are an easy target for brute force attacks. This can lead to an a enforce strong passwords. This vulnerability has been fixed in version 1.2.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.
CVE-2023-27629	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Paul Ryley Site Reviews plugin <= 6.5.1 versions.
CVE-2023-36000	A missing authorization check in the MacOS agent configuration endpoint of the Insider Threat Management Server enables an anonymous attacker on an adjacent ne authentication token. All versions before 7.14.3 are affected.
CVE-2023-32402	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, Safari 16.5, iOS 16.5 and iP
CVE-2023-27631	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in mmrs151 Daily Prayer Time plugin <= 2023.05.04 versions.
CVE-2023-34927	Casdoor v1.331.0 and below was discovered to contain a Cross-Site Request Forgery (CSRF) in the endpoint /api/set-password. This vulnerability allows attackers to a
CVE-2022-34352	IBM QRadar SIEM 7.5.0 is vulnerable to information exposure allowing a delegated Admin tenant user with a specific domain security profile assigned to see data from
CVE-2023-35093	Broken Access Control vulnerability in StylemixThemes MasterStudy LMS WordPress Plugin – for Online Courses and Education plugin <= 3.0.8 versions allows any lo like email, username, and more.
CVE-2023-28534	Auth. (subscriber+) Stored Cross-Site Scripting (XSS) vulnerability in WP Job Portal WP Job Portal – A Complete Job Board plugin <= 2.0.0 versions.
CVE-2023-34673	Elenos ETG150 FM transmitter running on version 3.12 was discovered to be leaking SMTP credentials and other sensitive information by exploiting the publicly acces
CVE-2023-32423	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, Safari 16.5, iOS 16.5 and
CVE-2023-29437	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Steven A. Zahm Connections Business Directory plugin <= 10.4.36 versions.
CVE-2023-34553	An issue was discovered in WAFU Keyless Smart Lock v1.0 allows attackers to unlock a device via code replay attack.
CVE-2023-34422	A valid, authenticated LXCA user with elevated privileges may be able to delete folders in the LXCA filesystem through a specifically crafted web API call due to insuffic
CVE-2023-2623	The KiviCare WordPress plugin before 3.2.1 does not restrict the information returned in a response and returns all user data, allowing low privilege users such as subs
CVE-2023-34421	A valid, authenticated LXCA user with elevated privileges may be able to replace filesystem data through a specifically crafted web API call due to insufficient input vali
CVE-2023-32525	Trend Micro Mobile Security (Enterprise) 9.8 SP5 contains widget vulnerabilities that could allow a remote attacker to create arbitrary files on affected installations. Plea exploit this vulnerability. This is similar to, but not identical to CVE-2023-32526.
CVE-2023-32526	Trend Micro Mobile Security (Enterprise) 9.8 SP5 contains widget vulnerabilities that could allow a remote attacker to create arbitrary files on affected installations. Plea exploit this vulnerability. This is similar to, but not identical to CVE-2023-32525.
CVE-2023-2326	The Gravity Forms Google Sheet Connector WordPress plugin before 1.3.5, gsheetconnector-gravityforms-pro WordPress plugin through 1.3.5 does not have CSRF ch to an arbitrary one via a CSRF attack

CVE Number	Description
CVE-2023-27443	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Grant Kimball Simple Vimeo Shortcode plugin <= 2.9.1 versions.
CVE-2023-3412	The Image Map Pro – Drag-and-drop Builder for Interactive Images – Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting in versions up to, and inclu authenticated attackers, with minimal permissions such as a subscriber, to modify plugin settings and inject malicious web scripts.
CVE-2023-3387	The Lana Text to Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'lana_text_to_image' and 'lana_text_to_img' shortcode in versions up 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 acc
CVE-2023-2290	A potential vulnerability in the LenovoFlashDeviceInterface SMI handler may allow an attacker with local access and elevated privileges to execute arbitrary code.
CVE-2023-2005	Vulnerability in Tenable Tenable.Io, Tenable Nessus, Tenable Security Center.This issue affects Tenable.Io: before Plugin Feed ID #202306261202 ; Nessus: before P allow a malicious actor with sufficient permissions on a scan target to place a binary in a specific filesystem location, and abuse the impacted plugin in order to escalate
CVE-2023-3339	A vulnerability has been found in code-projects Agro-School Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-232015.
CVE-2023-3396	A vulnerability was found in Campcodes Retro Cellphone Online Store 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of t can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-232351.
CVE-2023-3383	A vulnerability, which was classified as critical, was found in SourceCodester Game Result Matrix System 1.0. This affects an unknown part of the file /dipam/athlete-pr possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-232239.
CVE-2023-32371	The issue was addressed with improved checks. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4. An app may be able to break out of its sandbo
CVE-2023-27940	The issue was addressed with additional permissions checks. This issue is fixed in iOS 15.7.6 and iPadOS 15.7.6, macOS Monterey 12.6.6, macOS Ventura 13.4. A sa
CVE-2023-35132	A limited SQL injection risk was identified on the Mnet SSO access control page. This flaw affects Moodle versions 4.2, 4.1 to 4.1.3, 4.0 to 4.0.8, 3.11 to 3.11.14, 3.9 to
CVE-2023-3391	A vulnerability was found in SourceCodester Human Resource Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-232288.
CVE-2023-28071	Dell Command | Update, Dell Update, and Alienware Update versions 4.9.0, A01 and prior contain an Insecure Operation on Windows Junction / Mount Point vulnerabi Denial of Service (DOS).
CVE-2023-35164	DataEase is an open source data visualization analysis tool to analyze data and gain insight into business trends. In affected versions a missing authorization check all version 1.18.8. Users are advised to upgrade. There are no known workarounds for this vulnerability.
CVE-2023-35925	FastAsyncWorldEdit (FAWE) is designed for efficient world editing. This vulnerability enables the attacker to select a region with the `Infinity` keyword (case-sensitive!) fixed in version 2.6.3.
CVE-2023-36464	pypdf is an open source, pure-python PDF library. In affected versions an attacker may craft a PDF which leads to an infinite loop if `__parse_content_stream` is execu request #969 and resolved in pull request #1828. Users are advised to upgrade. Users unable to upgrade may modify the line `while peek not in (b"\r", b"\n")` in `pypdf/
CVE-2023-33842	IBM SPSS Modeler on Windows 17.0, 18.0, 18.2.2, 18.3, 18.4, and 18.5 requires the end user to have access to the server SSL key which could allow a local user to d
CVE-2023-33591	User Registration & Login and User Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /admin/search-res
CVE-2021-30203	A reflected cross-site scripting (XSS) vulnerability in the zero parameter of dzzoffice 2.02.1_SC_UTF8 allows attackers to execute arbitrary web scripts or HTML.

CVE Number	Description
CVE-2023-36346	POS Codekop v2.0 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the nm_member parameter at print.php.
CVE-2023-36289	An unauthenticated Cross-Site Scripting (XSS) vulnerability found in Webkul QloApps 1.6.0 allows an attacker to obtain a user's session cookie and then impersonate t
CVE-2023-35759	In Progress WhatsUp Gold before 23.0.0, an SNMP-related application endpoint failed to adequately sanitize malicious input. This could allow an unauthenticated attac
CVE-2023-3411	The Image Map Pro – Drag-and-drop Builder for Interactive Images – Lite plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and inclu unauthenticated attackers to modify plugin settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an a
CVE-2023-33725	Broadleaf 5.x and 6.x (including 5.2.25-GA and 6.2.6-GA) was discovered to contain a cross-site scripting (XSS) vulnerability via a customer signup with a crafted emai
CVE-2023-32531	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote
CVE-2023-36287	An unauthenticated Cross-Site Scripting (XSS) vulnerability found in Webkul QloApps 1.6.0 allows an attacker to obtain a user's session cookie and then impersonate t
CVE-2023-32532	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote
CVE-2023-33405	Blogengine.net 3.3.8.0 and earlier is vulnerable to Open Redirect.
CVE-2023-2605	The wpbrutalai WordPress plugin before 2.0.1 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripti
CVE-2023-36666	INEX IXP-Manager before 6.3.1 allows XSS. list-preamble.foil.php, page-header-preamble.foil.php, edit-form.foil.php, page-header-preamble.foil.php, overview.foil.php
CVE-2023-2624	The KiviCare WordPress plugin before 3.2.1 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting
CVE-2023-2743	The ERP WordPress plugin before 1.12.4 does not sanitise and escape the employee_name parameter before outputting it back in the page, leading to a Reflected Cro
CVE-2023-32533	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote
CVE-2023-35131	Content on the groups page required additional sanitizing to prevent an XSS risk. This flaw affects Moodle versions 4.2, 4.1 to 4.1.3, 4.0 to 4.0.8 and 3.11 to 3.11.14.
CVE-2023-29459	The laola.redbull application through 5.1.9-R for Android exposes the exported activity at.redbullsalzburg.android.AppMode.Default.Splash.SplashActivity, which accep loading of arbitrary content into the context of the application. This can occur via the fcrbs schema or an explicit intent invocation.
CVE-2023-1891	The Accordion & FAQ WordPress plugin before 1.9.9 does not escape various generated URLs, before outputting them in attributes when some notices are displayed,
CVE-2023-36675	An issue was discovered in MediaWiki before 1.35.11, 1.36.x through 1.38.x before 1.38.7, and 1.39.x before 1.39.4. BlockLogFormatter.php in BlockLogFormatter allo
CVE-2023-32339	IBM Business Automation Workflow is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering th 255587.

CVE Number	Description
CVE-2023-0588	The Catalyst Connect Zoho CRM Client Portal WordPress plugin before 2.1.0 does not sanitize and escape a parameter before outputting it back in the page, leading t
CVE-2023-34796	Cross site scripting (XSS) vulnerabiliy in dmarcts-report-viewer dashboard versions 1.1 and thru commit 8a1d882b4c481a05e296e9b38a7961e912146a0f, allows unau
CVE-2023-32534	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote
CVE-2023-33387	A reflected cross-site scripting (XSS) vulnerability in DATEV eG Personal-Management System Comfort/Comfort Plus v15.1.0 to v16.1.1 P4 allows attackers to steal ta
CVE-2023-32535	Certain dashboard widgets on Trend Micro Apex Central (on-premise) are vulnerable to cross-site scripting (XSS) attacks that may allow an attacker to achieve remote
CVE-2023-32369	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7.7, macOS Monterey 12.6.6, macOS Ventura 13.4. An app ma
CVE-2023-35163	Vega is a decentralized trading platform that allows pseudo-anonymous trading of derivatives on a blockchain. Prior to version 0.71.6, a vulnerability exists that allows a bridge. For example, a deposit to the collateral bridge for 100USDT that credits a party's general account on Vega, can be re-processed 50 times resulting in 5000USD Despite this exploit requiring access to a validator's Vega key, a validator key can be obtained at the small cost of 3000VEGA, the amount needed to announce a new n are mitigations in place should this vulnerability be exploited. There are monitoring alerts for `mainnet1` in place to identify any issues of this nature including this vulner vulnerability be exploited.
CVE-2023-28751	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Wpmet Wp Ultimate Review plugin <= 2.0.3 versions.
CVE-2023-27427	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in NTZApps CRM Memberships plugin <= 1.6 versions.
CVE-2023-28174	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in eLightUp eRocket plugin <= 1.2.4 versions.
CVE-2023-28695	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Drew Phillips VigilanTor plugin <= 1.3.10 versions.
CVE-2023-27452	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Wow-Company Button Generator – easily Button Builder plugin <= 2.3.3 versions.
CVE-2023-26539	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Max Chirkov Advanced Text Widget plugin <= 2.1.2 versions.
CVE-2023-26534	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in OneWebsite WP Repost plugin <= 0.1 versions.
CVE-2023-23811	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Neil Gee Smoothscroller plugin <= 1.0.0 versions.
CVE-2023-23807	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Qumos MojoPlug Slide Panel plugin <= 1.1.2 versions.
CVE-2023-35048	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in MagePeople Team Booking and Rental Manager for Bike plugin <= 1.2.1 versions.
CVE-2023-27439	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in gl_SPICE New Adman plugin <= 1.6.8 versions.
CVE-2023-26276	IBM QRadar SIEM 7.5.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 2481

CVE Number	Description
CVE-2023-28778	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in BestWebSoft Pagination plugin <= 1.2.2 versions.
CVE-2023-28774	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Grade Us, Inc. Review Stream plugin <= 1.6.5 versions.
CVE-2023-29434	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in FancyThemes Optin Forms – Simple List Building Plugin for WordPress plugin <= 1.3.1 versions.
CVE-2023-32580	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPExperts Password Protected plugin <= 2.6.2 versions.
CVE-2023-29423	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in PI Websolution Cancel order request / Return order / Repeat Order / Reorder for WooCommerce plug
CVE-2023-29093	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PI Websolution Conditional cart fee plugin <= 1.0.96 versions.
CVE-2023-28991	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in PI Websolution Order date, Order pickup, Order date time, Pickup Location, delivery date for WooCom
CVE-2023-34170	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WP Overnight Quick/Bulk Order Form for WooCommerce plugin <= 3.5.7 versions.
CVE-2023-28988	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in PI Websolution Direct checkout, Add to cart redirect, Quick purchase button, Buy now button, Quick V
CVE-2023-27429	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Automattic - Jetpack CRM team Jetpack CRM plugin <= 5.4.4 versions.
CVE-2023-27618	Auth. (editor+) Stored Cross-Site Scripting (XSS) vulnerability in AGILELOGIX Store Locator WordPress plugin <= 1.4.9 versions.
CVE-2023-34368	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Kanban for WordPress Kanban Boards for WordPress plugin <= 2.5.20 versions.
CVE-2023-34006	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Marco Milesi Telegram Bot & Channel plugin <= 3.6.2 versions.
CVE-2023-29438	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Eric Martin SimpleModal Contact Form (SMCF) plugin <= 1.2.9 versions.
CVE-2023-28423	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Prism Tech Studios Modern Footnotes plugin <= 1.4.15 versions.
CVE-2023-33323	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Repute InfoSystems ARMember plugin <= 4.0.2 versions.
CVE-2023-3132	The MainWP Child plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 4.4.1.1 due to insufficient controls on the stora entire installations database if a backup occurs and the deletion of the back-up files fail.
CVE-2023-35933	OPenFGA is an open source authorization/permission engine built for developers. OpenFGA versions v1.1.0 and prior are vulnerable to a DoS attack when Check and affected by this vulnerability if they are using OpenFGA v1.1.0 or earlier, and if you are executing `Check` or `ListObjects` calls against a vulnerable authorization mode do not have circular relationships in their models are not affected.
CVE-2023-28496	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in SMTP2GO – Email Made Easy plugin <= 1.4.2 versions.

CVE Number	Description
CVE-2023-20896	The VMware vCenter Server contains an out-of-bounds read vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCe certain services (vmcad, vmdird, and vmafdd).
CVE-2023-30500	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WPForms WPForms Lite (wpforms-lite), WPForms WPForms Pro (wpforms) plugins <= 1.8.1.2 versions.
CVE-2023-35173	Nextcloud End-to-end encryption app provides all the necessary APIs to implement End-to-End encryption on the client side. By providing an invalid meta data file, an a encryption app is upgraded to version 1.12.4 that contains the fix.
CVE-2023-25499	When adding non-visible components to the UI in server side, content is sent to the browser in Vaadin 10.0.0 through 10.0.22, 11.0.0 through 14.10.0, 15.0.0 through 2 information disclosure.
CVE-2015-20109	end_pattern (called from internal_fnmatch) in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent attackers to cause a denial of service (a the same as CVE-2015-8984; also, some Linux distributions have fixed CVE-2015-8984 but have not fixed this additional fnmatch issue.
CVE-2023-25435	libtiff 4.5.0 is vulnerable to Buffer Overflow via extractContigSamplesShifted8bits() at /libtiff/tools/tiffcrop.c:3753.
CVE-2023-32411	This issue was addressed with improved entitlements. This issue is fixed in tvOS 16.5, macOS Ventura 13.4, macOS Big Sur 11.7.7, macOS Monterey 12.6.6, iOS 16.5
CVE-2023-35799	Stormshield Endpoint Security Evolution 2.0.0 through 2.3.2 has Insecure Permissions. An interactive user can use the SES Evolution agent to create arbitrary files witl
CVE-2023-32385	A denial-of-service issue was addressed with improved memory handling. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4. Opening a PDF file m
CVE-2023-32376	This issue was addressed with improved entitlements. This issue is fixed in iOS 16.5 and iPadOS 16.5, watchOS 9.5, tvOS 16.5, macOS Ventura 13.4. An app may be
CVE-2023-32375	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Monterey 12.6.6, macOS Ventura 13.4. Processing a 3D model may
CVE-2023-32367	This issue was addressed with improved entitlements. This issue is fixed in iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4. An app may be able to access user-sens
CVE-2023-32363	A permissions issue was addressed by removing vulnerable code and adding additional checks. This issue is fixed in macOS Ventura 13.4. An app may be able to byp
CVE-2023-32360	An authentication issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7.7, macOS Monterey 12.6.6, macOS Ventura 13.4.
CVE-2023-32355	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7.7, macOS Monterey 12.6.6, macOS Ventura 13.4. An app ma
CVE-2023-32354	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 9.5, tvOS 16.5, iOS 16.5 and iPadOS 16.5. An app may be able to
CVE-2023-32352	A logic issue was addressed with improved checks. This issue is fixed in watchOS 9.5, macOS Ventura 13.4, macOS Big Sur 11.7.7, macOS Monterey 12.6.6, iOS 16.5
CVE-2023-28202	This issue was addressed with improved state management. This issue is fixed in iOS 16.5 and iPadOS 16.5, watchOS 9.5, tvOS 16.5, macOS Ventura 13.4. An app fi
CVE-2023-28191	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, macOS Big Sur 11.7.7

CVE Number	Description
CVE-2022-46718	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 15.7.2 and iPadOS 15.7.2, macOS Ventura 13.1, macOS Big Sur 11.7.2, macOS Mon
CVE-2022-46715	A logic issue was addressed with improved checks. This issue is fixed in iOS 16.1 and iPadOS 16. An app may be able to bypass certain Privacy preferences
CVE-2022-42860	This issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in macOS Monterey 12.6.1, macOS Big Sur 11.7.1, macOS Ventur
CVE-2022-42792	This issue was addressed with improved data protection. This issue is fixed in iOS 16.1 and iPadOS 16. An app may be able to read sensitive location information
CVE-2023-32556	A link following vulnerability in the Trend Micro Apex One and Apex One as a Service agent could allow a local attacker to disclose sensitive information. Please note: a vulnerability.
CVE-2023-32382	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Big Sur 11.7.7, macOS Monterey 12.6.6, macOS Ventura 13.4. Proc
CVE-2023-32372	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 16.5 and iPadOS 16.5, watchOS 9.5, tvOS 16.5, macOS Ventura 13.4.
CVE-2023-32407	A logic issue was addressed with improved state management. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, iOS 15.7.6 and iPadOS 15.7.6, ma preferences.
CVE-2023-32403	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, iOS 15.7.6 and iPadOS sensitive location information.
CVE-2023-32422	This issue was addressed by adding additional SQLite logging restrictions. This issue is fixed in iOS 16.5 and iPadOS 16.5, tvOS 16.5, macOS Ventura 13.4. An app m
CVE-2023-30902	A privilege escalation vulnerability in the Trend Micro Apex One and Apex One as a Service agent could allow a local attacker to unintentionally delete privileged Trend
CVE-2023-32415	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 16.5 and iPadOS 16.5, tvOS 16.5, macOS Ventura 13.4. An app n
CVE-2023-32410	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 15.7.6 and iPadOS 15.7.6, macOS Big Sur 11.7.7, macOS Monterey 12
CVE-2023-32408	The issue was addressed with improved handling of caches. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, iOS 15.7.6 and iPadOS 15.7.6, macO
CVE-2023-32388	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in watchOS 9.5, macOS Ventura 13.4, iOS 15.7.6 and iPadOS 15 Privacy preferences.
CVE-2023-32404	This issue was addressed with improved entitlements. This issue is fixed in iOS 16.5 and iPadOS 16.5, watchOS 9.5, macOS Ventura 13.4. An app may be able to byp
CVE-2023-32368	An out-of-bounds read was addressed with improved input validation. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, macOS Monterey 12.6.6, iO
CVE-2023-32400	This issue was addressed with improved checks. This issue is fixed in iOS 16.5 and iPadOS 16.5, watchOS 9.5, macOS Ventura 13.4. Entitlements and privacy permis
CVE-2023-32399	The issue was addressed with improved handling of caches. This issue is fixed in iOS 16.5 and iPadOS 16.5, watchOS 9.5, tvOS 16.5, macOS Ventura 13.4. An app m

CVE Number	Description
CVE-2023-32395	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.7.7, macOS Monterey 12.6.6, macOS Ventura 13.4. An app ma
CVE-2023-32392	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in watchOS 9.5, tvOS 16.5, macOS Ventura 13.4, macOS Big Su information.
CVE-2023-2818	An insecure filesystem permission in the Insider Threat Management Agent for Windows enables local unprivileged users to disrupt agent monitoring. All versions prior
CVE-2023-32389	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 16.5 and iPadOS 16.5, watchOS 9.5, tvOS 16.5, macOS Ventura
CVE-2023-34835	A Cross Site Scripting vulnerability in Microworld Technologies eScan Management console v.14.0.1400.2281 allows a remote attacker to execute arbitrary JavaScript
CVE-2023-34830	i-doit Open v24 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the timeout parameter on the login page.
CVE-2022-4115	The Editorial Calendar WordPress plugin before 3.8.3 does not sanitise and escape its settings, allowing users with roles as low as contributor to inject arbitrary web sc users.
CVE-2023-32605	Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validatio system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32604.
CVE-2023-32604	Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validatio system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32605.
CVE-2023-32537	Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validatio system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32536.
CVE-2023-2993	A valid, authenticated user with limited privileges may be able to use specifically crafted web management server API calls to execute a limited number of commands o
CVE-2023-32536	Affected versions Trend Micro Apex Central (on-premise) are vulnerable to potential authenticated reflected cross-site scripting (XSS) attacks due to user input validatio system in order to exploit this vulnerability. This is similar to, but not identical to CVE-2023-32537.
CVE-2023-34838	A Cross Site Scripting vulnerability in Microworld Technologies eScan Management console v.14.0.1400.2281 allows a remote attacker to execute arbitrary code via a
CVE-2023-34836	A Cross Site Scripting vulnerability in Microworld Technologies eScan Management console v.14.0.1400.2281 allows a remote attacker to execute arbitrary code via a
CVE-2023-34837	A Cross Site Scripting vulnerability in Microworld Technologies eScan Management console v.14.0.1400.2281 allows a remote attacker to execute arbitrary code via a
CVE-2023-36093	There is a storage type cross site scripting (XSS) vulnerability in the filing number of the Basic Information tab on the backend management page of EyouCMS v1.6.3
CVE-2023-3394	Session Fixation in GitHub repository fossbilling/fossbilling prior to 0.5.1.
CVE-2020-23065	Cross Site Scripting vulnerabiltiy in eZ Systems AS eZPublish Platform v.5.4 and eZ Publish Legacy v.5.4 allows a remote authenticated attacker to execute arbitrary c
CVE-2022-40010	Tenda AC6 AC1200 Smart Dual-Band WiFi Router 15.03.06.50_multi was discovered to contain a cross-site scripting (XSS) vulnerability via the deviceId parameter in

CVE Number	Description
CVE-2023-28171	Auth. (subscriber+) Stored Cross-Site Scripting (XSS) vulnerability in WP Chill Brilliance theme <= 1.3.1 versions.
CVE-2023-28485	A stored cross-site scripting (Stored XSS) vulnerability in file preview in WeKan before 6.75 allows remote authenticated users to inject arbitrary web script or HTML via BoardAdmin access), and renameAttachment does not block XSS payloads.
CVE-2023-31868	Sage X3 version 12.14.0.50-0 is vulnerable to Cross Site Scripting (XSS). Some parts of the Web application are dynamically built using user's inputs. Yet, those inputs HTML/JavaScript code is injected into those fields, this code will be saved by the application and executed by the web browser of the user viewing the web page. Sever a common account, he can then target an Administrator. All others endpoints need the malicious user to be authenticated as an Administrator. Therefore, the impact is
CVE-2023-28418	Auth. (subscriber+) Reflected Cross-Site Scripting (XSS) vulnerability in Yudlee themes Mediciti Lite theme <= 1.3.0 versions.
CVE-2023-27964	An authentication issue was addressed with improved state management. This issue is fixed in AirPods Firmware Update 5E133. When your headphones are seeking the intended source device and gain access to your headphones.
CVE-2023-36288	An unauthenticated Cross-Site Scripting (XSS) vulnerability found in Webkul QloApps 1.6.0 allows an attacker to obtain a user's session cookie and then impersonate t
CVE-2023-32239	Auth. (subscriber+) Stored Cross-Site Scripting (XSS) vulnerability in xtemos WoodMart theme <= 7.2.1 versions.
CVE-2023-36662	The TechTime User Management components for Atlassian products allow stored XSS on the Bulk User Actions page. This affects User Management for Jira 2.0.0 thr through 2.15.24.
CVE-2023-3304	Improper Access Control in GitHub repository admidio/admidio prior to 4.2.9.
CVE-2023-32553	An Improper access control vulnerability in Trend Micro Apex One and Apex One as a Service could allow an unauthenticated user under certain circumstances to disc
CVE-2021-30205	Incorrect access control in the component /index.php?mod=system&op=orgtree of dzzoffice 2.02.1_SC_UTF8 allows unauthenticated attackers to browse departments
CVE-2023-32552	An Improper access control vulnerability in Trend Micro Apex One and Apex One as a Service could allow an unauthenticated user under certain circumstances to disc
CVE-2023-3371	The User Registration plugin for WordPress is vulnerable to Sensitive Information Exposure due to hardcoded encryption key on the 'lock_content_form_handler' and 'c attackers to decrypt and view the password protected content.
CVE-2023-36463	Meldekarten generator is an open source project to create a program, running locally in the browser without the need for an internet-connection, to create, store and pri (fully) sanitized after submission. This issue has been addressed in commit `77e04f4af` which is included in the `1.0.0b1.1.2` release. Users are advised to upgrade. Th
CVE-2022-25883	Versions of the package semver before 7.5.2 are vulnerable to Regular Expression Denial of Service (ReDoS) via the function new Range, when untrusted user data is
CVE-2023-3431	Improper Access Control in GitHub repository plantuml/plantuml prior to 1.2023.9.
CVE-2023-26115	All versions of the package word-wrap are vulnerable to Regular Expression Denial of Service (ReDoS) due to the usage of an insecure regular expression within the re
CVE-2023-34241	OpenPrinting CUPS is a standards-based, open source printing system for Linux and other Unix-like operating systems. Starting in version 2.0.0 and prior to version 2.4 have logged the data right before. This is a use-after-free bug that impacts the entire cupsd process. The exact cause of this issue is the function `httpClose(con->http)` the pointer at the end of the call, only for cupsdLogClient to pass the pointer to httpGetHostname. This issue happens in function `cupsdAcceptClient` if LogLevel is wa `cupsd.conf`) which fails to resolve, or if CUPS is compiled with TCP wrappers and the connection is refused by rules from `/etc/hosts.allow` and `/etc/hosts.deny`. Vers
CVE-2023-34099	Shopware is an open source e-commerce software. The mail validation in the registration process had some flaws, so it was possible to construct different mail address addressed in version 5.7.18 and users are advised to update. There are no known workarounds for this vulnerability.

CVE Number	Description
CVE-2023-2991	Fortra Globalscape EFT's administration server suffers from an information disclosure vulnerability where the serial number of the harddrive that Globalscape is installe
CVE-2023-34098	Shopware is an open source e-commerce software. Due to an incorrect configuration in the `.htaccess` file, the configuration file of the Javascript could be read in prod deployment might be determined by an attacker, which could be used for further attacks. Users are advised to update to version 5.7.18. There are no known workarour
CVE-2023-28040	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28056	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-23468	IBM Robotic Process Automation for Cloud Pak 21.0.1 through 21.0.7.3 and 23.0.0 through 23.0.3 is vulnerable to insufficient security configuration which may allow cr
CVE-2023-28052	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28042	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28041	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28028	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28039	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28061	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28035	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28033	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28032	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28030	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-25936	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28029	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-25937	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28059	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i

CVE Number	Description
CVE-2023-28054	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28044	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28058	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-25938	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28026	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28027	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28031	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28034	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28036	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28060	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-28050	Dell BIOS contains an improper input validation vulnerability. A local authenticated malicious user with administrator privileges may potentially exploit this vulnerability i
CVE-2023-35167	Remult is a CRUD framework for full-stack TypeScript. If you used the apiPrefilter option of the `@Entity` decorator, by setting it to a function that returns a filter that pre access, can gain read, update and delete access to it. The issue is fixed in version 0.20.6. As a workaround, set the `apiPrefilter` option to a filter object instead of a fur
CVE-2023-3114	Terraform Enterprise since v202207-1 did not properly implement authorization rules for agent pools, allowing the workspace to be targeted by unauthorized agents. Th workspace in the same organization that targeted an agent pool. This vulnerability, CVE-2023-3114, is fixed in Terraform Enterprise v202306-1.
CVE-2023-1619	Multiple WAGO devices in multiple versions may allow an authenticated remote attacker with high privileges to DoS the device by sending a malformed packet.
CVE-2023-1620	Multiple WAGO devices in multiple versions may allow an authenticated remote attacker with high privileges to DoS the device by sending a specifically crafted packet
CVE-2023-2711	The Ultimate Product Catalog WordPress plugin before 5.2.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to multisite setup)
CVE-2023-34460	Tauri is a framework for building binaries for all major desktop platforms. The 1.4.0 release includes a regression on the Filesystem scope check for dotfiles on Unix. Pr introduced when a configuration option for this behavior was implemented. Only Tauri applications using wildcard scopes in the `fs` endpoint are affected. The regressi
CVE-2023-33580	Phpgurukul Student Study Center Management System V1.0 is vulnerable to Cross Site Scripting (XSS) in the "Admin Name" field on Admin Profile page.
CVE-2020-18414	Stored cross site scripting (XSS) vulnerability in Chaoji CMS v2.18 that allows attackers to execute arbitrary code via /index.php?admin-master-webset.

CVE Number	Description
CVE-2023-27082	Cross Site Scripting (XSS) vulnerability in /admin.php in Pluck CMS 4.7.15 through 4.7.16-dev4 allows remote attackers to run arbitrary code via upload of crafted html
CVE-2023-2795	The CodeColorer WordPress plugin before 0.10.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform S setup)
CVE-2023-30347	Cross Site Scripting (XSS) vulnerability in Neox Contact Center 2.3.9, via the serach_sms_api_name parameter to the SMA API search.
CVE-2020-18413	Stored cross site scripting (XSS) vulnerability in /index.php?admin-master-navmenu-add of Chaoji CMS v2.18 that allows attackers to execute arbitrary code.
CVE-2023-29707	Cross Site Scripting (XSS) vulnerability in GBCOM LAC WEB Control Center version lac-1.3.x, allows attackers to create an arbitrary device.
CVE-2020-18404	An issue was discovered in espcms version P8.18101601. There is a cross site scripting (XSS) vulnerability that allows arbitrary code to be executed via the title param
CVE-2020-18410	A stored cross site scripting (XSS) vulnerability in /index.php?admin-master-article-edit of Chaoji CMS v2.18 that allows attackers to obtain administrator privileges.
CVE-2023-0873	The Kanban Boards for WordPress plugin before 2.5.21 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perf multisite setup)
CVE-2023-2580	The AI Engine WordPress plugin before 1.6.83 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stor setup).
CVE-2023-33176	BigBlueButton is an open source virtual classroom designed to help teachers teach and learners learn. In affected versions are affected by a Server-Side Request Forg presentation should be downloaded. This URL was being used without having been successfully validated first. An update to the `followRedirect` method in the `Preser properties `presentationDownloadSupportedProtocols` and `presentationDownloadBlockedHosts` have also been added to `bigbluebutton.properties` to allow administ downloaded from. All URLs passed to `insertDocument` must conform to the requirements of the two previously mentioned properties. Additionally, these URLs must re workarounds. Users are advised to upgrade to a patched version of BigBlueButton.
CVE-2023-2178	The Aajoda Testimonials WordPress plugin before 2.2.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perf multisite setup).
CVE-2023-1166	The USM-Premium WordPress plugin before 16.3 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform S setup).
CVE-2023-3380	A vulnerability classified as critical has been found in Wavlink WN579X3 up to 20230615. Affected is an unknown function of the file /cgi-bin/adm.cgi of the component The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-232236. NOTE: The vendor was contacted early about this disc
CVE-2023-32391	The issue was addressed with improved checks. This issue is fixed in iOS 15.7.6 and iPadOS 15.7.6, watchOS 9.5, iOS 16.5 and iPadOS 16.5, macOS Ventura 13.4. A
CVE-2023-26274	IBM QRadar SIEM 7.5.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended
CVE-2023-23679	Authorization Bypass Through User-Controlled Key vulnerability in JS Help Desk js-support-ticket allows Accessing Functionality Not Properly Constrained by ACLs.Th
CVE-2023-35998	A missing authorization check in multiple SOAP endpoints of the Insider Threat Management Server enables an attacker on an adjacent network to read and write unau versions before 7.14.3 are affected.
CVE-2023-25520	NVIDIA Jetson Linux Driver Package contains a vulnerability in nvbootctrl, where a privileged local attacker can configure invalid settings, resulting in denial of service.
CVE-2023-3212	A NULL pointer dereference issue was found in the gfs2 file system in the Linux kernel. It occurs on corrupt gfs2 file systems when the evict code tries to reference the cause a kernel panic.

CVE Number	Description
CVE-2023-26273	IBM QRadar SIEM 7.5.0 could allow an authenticated user to perform unauthorized actions due to hazardous input validation. IBM X-Force ID: 248134.
CVE-2023-35800	Stormshield Endpoint Security Evolution 2.0.0 through 2.4.2 has Insecure Permissions. An ACL entry on the SES Evolution agent directory that contains the agent logs administrators.
CVE-2022-42807	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13. A user may accidentally add a participant to a Shared Album t
CVE-2023-36002	A missing authorization check in multiple URL validation endpoints of the Insider Threat Management Server enables an anonymous attacker on an adjacent network t
CVE-2023-34028	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 WOLF – WordPress Posts Bulk Editor and Manager Professional plugin <= 1.0.7 versions.
CVE-2023-34466	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. Starting in version 5.0-milestone-1 and prior to versions 14.4.8, 14.1 can also be exploited to infer the document reference of non-viewable pages. This vulnerability has been patched in XWiki 14.4.8, 14.10.4, and 15.0-rc-1.
CVE-2023-35798	Input Validation vulnerability in Apache Software Foundation Apache Airflow ODBC Provider, Apache Software Foundation Apache Airflow MSSQL Provider.This vulne to connection resources specifically updating the connection to exploit it. This issue affects Apache Airflow ODBC Provider: before 4.0.0; Apache Airflow MSSQL Provi
CVE-2023-22359	User enumeration in Checkmk <=2.2.0p4 allows an authenticated attacker to enumerate usernames.
CVE-2023-2627	The KiviCare WordPress plugin before 3.2.1 does not have proper CSRF and authorisation checks in various AJAX actions, allowing any authenticated users, such as plugin's settings
CVE-2023-35917	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce PayPal Payments plugin <= 2.0.4 versions.
CVE-2023-35171	NextCloud Server and NextCloud Enterprise Server provide file storage for Nextcloud, a self-hosted productivity platform. Starting in version 26.0.0 and prior to version attacker's site. Nextcloud Server and Nextcloud Enterprise Server 26.0.2 contain a patch for this issue. No known workarounds are available.
CVE-2023-22593	IBM Robotic Process Automation for Cloud Pak 21.0.1 through 21.0.7.3 and 23.0.0 through 23.0.3 is vulnerable to security misconfiguration of the Redis container whic
CVE-2023-28857	Apereo CAS is an open source multilingual single sign-on solution for the web. Apereo CAS can be configured to use authentication based on client X509 certificates. T checking the validity of the provided client certificate, X509CredentialsAuthenticationHandler performs check that this certificate is not revoked. To do so, it fetches URL therefore can be controlled by a malicious user. If the CAS server is configured to use an LDAP server for x509 authentication with a password, for example by setting a X509CredentialsAuthenticationHandler fetches revocation URLs from the certificate, which can be LDAP urls. When making requests to this LDAP urls, Apereo CAS us unauthenticated user can leak the password used to LDAP connection configured on server. This issue has been addressed in version 6.6.6. Users are advised to upg
CVE-2023-35930	SpiceDB is an open source, Google Zanzibar-inspired, database system for creating and managing security-critical application permissions. Any user making a negativ using `LookupResources` to find a list of resources to allow access to be okay: some subjects that should have access to a resource may not. But if using `LookupResc `LookupResources` is not and should not be to gate access in this way - that's what the `Check` API is for. Additionally, version 1.22.0 has included a warning about thi avoid using `LookupResources` for negative authorization decisions.
CVE-2023-0969	A vulnerability in SiLabs Z/IP Gateway 7.18.01 and earlier allows an authenticated attacker within Z-Wave range to manipulate an array pointer to disclose the contents
CVE-2023-3382	A vulnerability, which was classified as problematic, has been found in SourceCodester Game Result Matrix System 1.0. Affected by this issue is some unknown functi argument del_name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-232238 is
CVE-2023-25500	Possible information disclosure in Vaadin 10.0.0 to 10.0.23, 11.0.0 to 14.10.1, 15.0.0 to 22.0.28, 23.0.0 to 23.3.13, 24.0.0 to 24.0.6, 24.1.0.alpha1 to 24.1.0.rc2, resultir
CVE-2023-3381	A vulnerability classified as problematic was found in SourceCodester Online School Fees System 1.0. Affected by this vulnerability is an unknown functionality of the fi leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-232237 was assig

CVE Number	Description
CVE-2023-3303	Improper Access Control in GitHub repository admidio/admidio prior to 4.2.9.
CVE-2023-28064	Dell BIOS contains an Out-of-bounds Write vulnerability. An unauthenticated physical attacker may potentially exploit this vulnerability, leading to denial of service.
CVE-2023-32463	Dell VxRail, version(s) 8.0.100 and earlier contain a denial-of-service vulnerability in the upgrade functionality. A remote unauthenticated attacker could potentially expl
CVE-2023-3436	Xpdf 4.04 will deadlock on a PDF object stream whose "Length" field is itself in another object stream.
CVE-2023-32386	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Big Sur 11.7.7, macOS Monterey 12.6.6, macOS Ventura 13.4.
CVE-2022-42834	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Monterey 12.6.3, macOS Ventura 13, macOS Big Sur 11.7.3. An app r
CVE-2023-28016	Host Header Injection vulnerability in the HCL BigFix OSD Bare Metal Server version 311.12 or lower allows attacker to supply invalid input to cause the OSD Bare Met
CVE-2023-35931	Shescape is a simple shell escape library for JavaScript. An attacker may be able to get read-only access to environment variables. This bug has been patched in versi
CVE-2023-23344	A permission issue in BigFix WebUI Insights site version 14 allows an authenticated, unprivileged operator to access an administrator page.
CVE-2023-22834	The Contour Service was not checking that users had permission to create an analysis for a given dataset. This could allow an attacker to clutter up Compass folders w
CVE-2023-34110	Flask-AppBuilder is an application development framework, built on top of Flask. Prior to version 4.3.2, an authenticated malicious actor with Admin privileges, could by actor on the UI. On certain database engines this error can include the entire user row including the pbkdf2:sha256 hashed password. This vulnerability has been fixed
CVE-2023-32464	Dell VxRail, versions prior to 7.0.450, contain an improper certificate validation vulnerability. A high privileged remote attacker may potentially exploit this vulnerability to modify a victim’s data in transit.
CVE-2023-32390	The issue was addressed with improved checks. This issue is fixed in iOS 16.5 and iPadOS 16.5, watchOS 9.5, macOS Ventura 13.4. Photos belonging to the Hidden
CVE-2023-23343	A clickjacking vulnerability in the HCL BigFix OSD Bare Metal Server version 311.12 or lower allows attacker to use transparent or opaque layers to trick a user into clic
CVE-2023-32417	This issue was addressed by restricting options offered on a locked device. This issue is fixed in watchOS 9.5. An attacker with physical access to a locked Apple Watc
CVE-2023-32394	The issue was addressed with improved checks. This issue is fixed in iOS 16.5 and iPadOS 16.5, watchOS 9.5, tvOS 16.5, macOS Ventura 13.4. A person with physica
CVE-2023-32365	The issue was addressed with improved checks. This issue is fixed in iOS 15.7.6 and iPadOS 15.7.6, iOS 16.5 and iPadOS 16.5. Shake-to-undo may allow a deleted p
CVE-2023-3351	Rejected reason: Wrong year requested.
CVE-2023-36191	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that

CVE Number	Description
CVE-2023-33567	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that
CVE-2023-33566	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that
CVE-2023-33565	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that
CVE-2020-23064	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-11023. Reason: This candidate is a duplicate of CVE-2020-11023. Notes: All CV candidate have been removed to prevent accidental usage.
CVE-2020-23066	Rejected reason: DO NOT USE THIS CVE ID NUMBER. Consult IDs: CVE-2020-17480. Reason: This CVE Record is a duplicate of CVE-2020-17480. Notes: All CVE
CVE-2023-35170	Rejected reason: This CVE is a duplicate of another CVE.
CVE-2023-3327	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-35823. Reason: This candidate is a reservation duplicate of CVE-2023-35823. N this candidate have been removed to prevent accidental usage.