SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 04 October 2023

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-38586	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sonoma 14. A sandboxed process may be able to circumvent sandbox restrictions.	10.0	More Details
CVE-2023-40044	In WS_FTP Server versions prior to 8.7.4 and 8.8.2, a pre-authenticated attacker could leverage a .NET deserialization vulnerability in the Ad Hoc Transfer module to execute remote commands on the underlying WS_FTP Server operating system.	10.0	More Details
CVE-2023-40455	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14. A sandboxed process may be able to circumvent sandbox restrictions.	10.0	More Details
CVE-2022-47893	There is a remote code execution vulnerability that affects all versions of NetMan 204. A remote attacker could upload a firmware file containing a webshell, that could allow him to execute arbitrary code as root.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43654	TorchServe is a tool for serving and scaling PyTorch models in production. TorchServe default configuration lacks proper input validation, enabling third parties to invoke remote HTTP download requests and write files to the disk. This issue could be taken advantage of to compromise the integrity of the system and sensitive data. This issue is present in versions 0.1.0 to 0.8.1. A user is able to load the model of their choice from any URL that they would like to use. The user of TorchServe is responsible for configuring both the allowed_urls and specifying the model URL to be used. A pull request to warn the user when the default value for allowed_urls is used has been merged in PR #2534. TorchServe release 0.8.2 includes this change. Users are advised to upgrade. There are no known workarounds for this issue.	10.0	More Details
CVE-2023-5183	Unsafe deserialization of untrusted JSON allows execution of arbitrary code on affected releases of the Illumio PCE. Authentication to the API is required to exploit this vulnerability. The flaw exists within the network_traffic API endpoint. An attacker can leverage this vulnerability to execute code in the context of the PCE's operating system user.	9.9	More Details
CVE-2023-42657	In WS_FTP Server versions prior to 8.7.4 and 8.8.2, a directory traversal vulnerability was discovered. An attacker could leverage this vulnerability to perform file operations (delete, rename, rmdir, mkdir) on files and folders outside of their authorized WS_FTP folder path. Attackers could also escape the context of the WS_FTP Server file structure and perform the same level of operations (delete, rename, rmdir, mkdir) on file and folder locations on the underlying operating system.	9.9	More Details
CVE-2023-3744	Server-Side Request Forgery vulnerability in SLims version 9.6.0. This vulnerability could allow an authenticated attacker to send requests to internal services or upload the contents of relevant files via the "scrape_image.php" file in the imageURL parameter.	9.9	More Details
CVE-2023-5201	The OpenHook plugin for WordPress is vulnerable to Remote Code Execution in versions up to, and including, 4.3.0 via the 'php' shortcode. This allows authenticated attackers with subscriber-level permissions or above, to execute code on the server. This requires the [php] shortcode setting to be enabled on the vulnerable site.	9.9	More Details
CVE-2023-5227	Unrestricted Upload of File with Dangerous Type in GitHub repository thorsten/phpmyfaq prior to 3.1.8.	9.8	More Details
CVE-2023-43891	Netis N3Mv2-V1.0.1.865 was discovered to contain a command injection vulnerability in the Changing Username and Password function. This vulnerability is exploited via a crafted payload.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44009	File Upload vulnerability in mojoPortal v.2.7.0.0 allows a remote attacker to execute arbitrary code via the Skin Management function.	9.8	More Details
CVE-2023-44008	File Upload vulnerability in mojoPortal v.2.7.0.0 allows a remote attacker to execute arbitrary code via the File Manager function.	9.8	More Details
CVE-2023-4659	Cross-Site Request Forgery vulnerability, whose exploitation could allow an attacker to perform different actions on the platform as an administrator, simply by changing the token value to "admin". It is also possible to perform POST, GET and DELETE requests without any token value. Therefore, an unprivileged remote user is able to create, delete and modify users within theapplication.	9.8	More Details
CVE-2023-20819	In CDMA PPP protocol, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege with no additional execution privilege needed. User interaction is not needed for exploitation. Patch ID: MOLY01068234; Issue ID: ALPS08010003.	9.8	More Details
CVE-2021-38243	xunruicms up to v4.5.1 was discovered to contain a remote code execution (RCE) vulnerability in /index.php. This vulnerability allows attackers to execute arbitrary code via a crafted GET request.	9.8	More Details
CVE-2023-5288	A remote unauthorized attacker may connect to the SIM1012, interact with the device and change configuration settings. The adversary may also reset the SIM and in the worst case upload a new firmware version to the device.	9.8	More Details
CVE-2023-43893	Netis N3Mv2-V1.0.1.865 was discovered to contain a command injection vulnerability via the wakeup_mac parameter in the Wake-On-LAN (WoL) function. This vulnerability is exploited via a crafted payload.	9.8	More Details
CVE-2023-44166	The 'age' parameter of the process_registration.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-44164	The 'Email' parameter of the process_login.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-44163	The 'search' parameter of the process_search.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-43739	The 'bookisbn' parameter of the cart.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5053	Hospital management system version 378c157 allows to bypass authentication. This is possible because the application is vulnerable to SQLI.	9.8	More Details
CVE-2023-5004	Hospital management system version 378c157 allows to bypass authentication. This is possible because the application is vulnerable to SQLI.	9.8	More Details
CVE-2023-43892	Netis N3Mv2-V1.0.1.865 was discovered to contain a command injection vulnerability via the Hostname parameter within the WAN settings. This vulnerability is exploited via a crafted payload.	9.8	More Details
CVE-2023-24855	Memory corruption in Modem while processing security related configuration before AS Security Exchange.	9.8	More Details
CVE-2023-44011	An issue in mojoPortal v.2.7.0.0 allows a remote attacker to execute arbitrary code via a crafted script to the layout.master skin file at the Skin management component.	9.8	More Details
CVE-2023-43980	Presto Changeo testsitecreator up to v1.1.1 was discovered to contain a SQL injection vulnerability via the component disable_json.php.	9.8	More Details
CVE-2023-39651	Improper neutralization of SQL parameter in Theme Volty CMS BrandList module for PrestaShop In the module “Theme Volty CMS BrandList” (tvcmsbrandlist) up to version 4.0.1 from Theme Volty for PrestaShop, a guest can perform SQL injection in affected versions.	9.8	More Details
CVE-2023-39649	Improper neutralization of SQL parameter in Theme Volty CMS Category Slider module for PrestaShop. In the module “Theme Volty CMS Category Slider” (tvcmscategoryslider) up to version 4.0.1 from Theme Volty for PrestaShop, a guest can perform SQL injection in affected versions.	9.8	More Details
CVE-2023-39648	Improper neutralization of SQL parameter in Theme Volty CMS Testimonial module for PrestaShop. In the module “Theme Volty CMS Testimonial” (tvcmstestimonial) up to version 4.0.1 from Theme Volty for PrestaShop, a guest can perform SQL injection in affected versions.	9.8	More Details
CVE-2023-39646	Improper neutralization of SQL parameter in Theme Volty CMS Category Chain Slider module for PrestaShop. In the module “Theme Volty CMS Category Chain Slide"(tvcmscategorychainslider) up to version 4.0.1 from Theme Volty for PrestaShop, a guest can perform SQL injection in affected versions.	9.8	More Details
CVE-2023-44974	An arbitrary file upload vulnerability in the component /admin/plugin.php of Emlog Pro v2.2.0 allows attackers to execute arbitrary code via uploading a crafted PHP file.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44973	An arbitrary file upload vulnerability in the component /content/templates/ of Emlog Pro v2.2.0 allows attackers to execute arbitrary code via uploading a crafted PHP file.	9.8	More Details
CVE-2023-39645	Improper neutralization of SQL parameter in Theme Volty CMS Payment Icon module for PrestaShop. In the module “Theme Volty CMS Payment Icon” (tvcmspaymenticon) up to version 4.0.1 from Theme Volty for PrestaShop, a guest can perform SQL injection in affected versions.	9.8	More Details
CVE-2023-33273	An issue was discovered in DTS Monitoring 3.57.0. The parameter url within the WGET check function is vulnerable to OS command injection (blind).	9.8	More Details
CVE-2023-33272	An issue was discovered in DTS Monitoring 3.57.0. The parameter ip within the Ping check function is vulnerable to OS command injection (blind).	9.8	More Details
CVE-2023-33271	An issue was discovered in DTS Monitoring 3.57.0. The parameter common_name within the SSL Certificate check function is vulnerable to OS command injection (blind).	9.8	More Details
CVE-2023-33270	An issue was discovered in DTS Monitoring 3.57.0. The parameter url within the Curl check function is vulnerable to OS command injection (blind).	9.8	More Details
CVE-2023-33269	An issue was discovered in DTS Monitoring 3.57.0. The parameter options within the WGET check function is vulnerable to OS command injection (blind).	9.8	More Details
CVE-2023-33268	An issue was discovered in DTS Monitoring 3.57.0. The parameter port within the SSL Certificate check function is vulnerable to OS command injection (blind).	9.8	More Details
CVE-2023-40830	Tenda AC6 v15.03.05.19 is vulnerable to Buffer Overflow as the Index parameter does not verify the length.	9.8	More Details
CVE-2023-3656	cashIT! - serving solutions. Devices from "PoS/ Dienstleistung, Entwicklung & Vertrieb GmbH" to 03.A06rks 2023.02.37 are affected by an unauthenticated remote code execution vulnerability. This vulnerability can be triggered by an HTTP endpoint exposed to the network.	9.8	More Details
CVE-2023-33028	Memory corruption in WLAN Firmware while doing a memory copy of pmk cache.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35071	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in MRV Tech Logging Administration Panel allows SQL Injection.This issue affects Logging Administration Panel: before 20230915 .	9.8	More Details
CVE-2023-43013	Asset Management System v1.0 is vulnerable to an unauthenticated SQL Injection vulnerability on the 'email' parameter of index.php page, allowing an external attacker to dump all the contents of the database contents and bypass the login control.	9.8	More Details
CVE-2023-30415	Sourcecodester Packers and Movers Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /inquiries/view_inquiry.php.	9.8	More Details
CVE-2023-43869	D-Link DIR-619L B1 2.02 is vulnerable to Buffer Overflow via formSetWAN_Wizard56 function.	9.8	More Details
CVE-2023-44023	Tenda AC10U v1.0 US_AC10UV1.0RTL_V15.03.06.49_multi_TDE01 was discovered to contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function.	9.8	More Details
CVE-2023-44273	Consensys gnark-crypto through 0.11.2 allows Signature Malleability. This occurs because deserialisation of EdDSA and ECDSA signatures does not ensure that the data is in a certain interval.	9.8	More Details
CVE-2023-44020	Tenda AC10U v1.0 US_AC10UV1.0RTL_V15.03.06.49_multi_TDE01 was discovered to contain a stack overflow via the security parameter in the formWifiBasicSet function.	9.8	More Details
CVE-2023-44019	Tenda AC10U v1.0 US_AC10UV1.0RTL_V15.03.06.49_multi_TDE01 was discovered to contain a stack overflow via the mac parameter in the GetParentControlInfo function.	9.8	More Details
CVE-2023-44018	Tenda AC10U v1.0 US_AC10UV1.0RTL_V15.03.06.49_multi_TDE01 was discovered to contain a stack overflow via the domain parameter in the add_white_node function.	9.8	More Details
CVE-2023-44017	Tenda AC10U v1.0 US_AC10UV1.0RTL_V15.03.06.49_multi_TDE01 was discovered to contain a stack overflow via the timeZone parameter in the fromSetSysTime function.	9.8	More Details
CVE-2023-44016	Tenda AC10U v1.0 US_AC10UV1.0RTL_V15.03.06.49_multi_TDE01 was discovered to contain a stack overflow via the deviceId parameter in the addWifiMacFilter function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44015	Tenda AC10U v1.0 US_AC10UV1.0RTL_V15.03.06.49_multi_TDE01 was discovered to contain a stack overflow via the schedEndTime parameter in the setSchedWifi function.	9.8	More Details
CVE-2023-44014	Tenda AC10U v1.0 US_AC10UV1.0RTL_V15.03.06.49_multi_TDE01 was discovered to contain multiple stack overflows in the formSetMacFilterCfg function via the macFilterType and deviceList parameters.	9.8	More Details
CVE-2023-44013	Tenda AC10U v1.0 US_AC10UV1.0RTL_V15.03.06.49_multi_TDE01 was discovered to contain a stack overflow via the list parameter in the fromSetIpMacBind function.	9.8	More Details
CVE-2023-43291	Deserialization of Untrusted Data in emlog pro v.2.1.15 and earlier allows a remote attacker to execute arbitrary code via the cache.php component.	9.8	More Details
CVE-2023-43234	DedeBIZ v6.2.11 was discovered to contain multiple remote code execution (RCE) vulnerabilities at /admin/file_manage_control.php via the $activepath and $filename parameters.	9.8	More Details
CVE-2023-43222	SeaCMS v12.8 has an arbitrary code writing vulnerability in the /jxz7g2/admin_ping.php file.	9.8	More Details
CVE-2023-43216	SeaCMS V12.9 was discovered to contain an arbitrary file write vulnerability via the component admin_ip.php.	9.8	More Details
CVE-2023-43187	A remote code execution (RCE) vulnerability in the xmlrpc.php endpoint of NodeBB Inc NodeBB forum software prior to v1.18.6 allows attackers to execute arbitrary code via crafted XML-RPC requests.	9.8	More Details
CVE-2023-43154	In Macrob7 Macs Framework Content Management System (CMS) 1.1.4f, loose comparison in "isValidLogin()" function during login attempt results in PHP type confusion vulnerability that leads to authentication bypass and takeover of the administrator account.	9.8	More Details
CVE-2023-40400	This issue was addressed with improved checks. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10, macOS Sonoma 14. A remote user may cause an unexpected app termination or arbitrary code execution.	9.8	More Details
CVE-2023-3767	An OS command injection vulnerability has been found on EasyPHP Webserver affecting version 14.1. This vulnerability could allow an attacker to get full access to the system by sending a specially crafted exploit to the /index.php?zone=settings parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44022	Tenda AC10U v1.0 US_AC10UV1.0RTL_V15.03.06.49_multi_TDE01 was discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function.	9.8	More Details
CVE-2023-44021	Tenda AC10U v1.0 US_AC10UV1.0RTL_V15.03.06.49_multi_TDE01 was discovered to contain a stack overflow via the formSetClientState function.	9.8	More Details
CVE-2023-5172	A hashtable in the Ion Engine could have been mutated while there was a live interior reference, leading to a potential use-after-free and exploitable crash. This vulnerability affects Firefox < 118.	9.8	More Details
CVE-2023-5168	A compromised content process could have provided malicious data to `FilterNodeD2D1` resulting in an out-of-bounds write, leading to a potentially exploitable crash in a privileged process. *This bug only affects Firefox on Windows. Other operating systems are unaffected.* This vulnerability affects Firefox < 118, Firefox ESR < 115.3, and Thunderbird < 115.3.	9.8	More Details
CVE-2023-38870	A SQL injection vulnerability exists in gugoan Economizzer commit 3730880 (April 2023) and v.0.9-beta1. The cash book has a feature to list accomplishments by category, and the 'category_id' parameter is vulnerable to SQL Injection.	9.8	More Details
CVE-2023-41449	An issue in phpkobo AjaxNewsTicker v.1.0.5 allows a remote attacker to execute arbitrary code via a crafted payload to the reque parameter.	9.8	More Details
CVE-2023-44080	An issue in PGYER codefever v.2023.8.14-2ce4006 allows a remote attacker to execute arbitrary code via a crafted request to the branchList component.	9.8	More Details
CVE-2023-20252	A vulnerability in the Security Assertion Markup Language (SAML) APIs of Cisco Catalyst SD-WAN Manager Software could allow an unauthenticated, remote attacker to gain unauthorized access to the application as an arbitrary user. This vulnerability is due to improper authentication checks for SAML APIs. An attacker could exploit this vulnerability by sending requests directly to the SAML API. A successful exploit could allow the attacker to generate an authorization token sufficient to gain access to the application.	9.8	More Details
CVE-2023-5176	Memory safety bugs present in Firefox 117, Firefox ESR 115.2, and Thunderbird 115.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 118, Firefox ESR < 115.3, and Thunderbird < 115.3.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5175	During process shutdown, it was possible that an `ImageBitmap` was created that would later be used after being freed from a different codepath, leading to a potentially exploitable crash. This vulnerability affects Firefox < 118.	9.8	More Details
CVE-2023-5174	If Windows failed to duplicate a handle during process creation, the sandbox code may have inadvertently freed a pointer twice, resulting in a use-after-free and a potentially exploitable crash. *This bug only affects Firefox on Windows when run in non-standard configurations (such as using `runas`). Other operating systems are unaffected.* This vulnerability affects Firefox < 118, Firefox ESR < 115.3, and Thunderbird < 115.3.	9.8	More Details
CVE-2023-44169	SeaCMS V12.9 was discovered to contain an arbitrary file write vulnerability via the component admin_notify.php.	9.8	More Details
CVE-2023-39647	Improper neutralization of SQL parameter in Theme Volty CMS Category Product module for PrestaShop. In the module “Theme Volty CMS Category Product” (tvcmscategoryproduct) up to version 4.0.1 from Theme Volty for PrestaShop, a guest can perform SQL injection in affected versions.	9.8	More Details
CVE-2023-4737	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Hedef Tracking Admin Panel allows SQL Injection.This issue affects Admin Panel: before 1.2.	9.8	More Details
CVE-2023-44172	SeaCMS V12.9 was discovered to contain an arbitrary file write vulnerability via the component admin_weixin.php.	9.8	More Details
CVE-2023-44171	SeaCMS V12.9 was discovered to contain an arbitrary file write vulnerability via the component admin_smtp.php.	9.8	More Details
CVE-2023-44170	SeaCMS V12.9 was discovered to contain an arbitrary file write vulnerability via the component admin_ping.php.	9.8	More Details
CVE-2023-3654	cashIT! - serving solutions. Devices from "PoS/ Dienstleistung, Entwicklung & Vertrieb GmbH" to 03.A06rks 2023.02.37 are affected by a origin bypass via the host header in an HTTP request. This vulnerability can be triggered by an HTTP endpoint exposed to the network.	9.4	More Details
CVE-2023-4523	Real Time Automation 460 Series products with versions prior to v8.9.8 are vulnerable to cross-site scripting, which could allow an attacker to run any JavaScript reference from the URL string. If this were to occur, the gateway's HTTP interface would redirect to the main page, which is index.htm.	9.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5350	SQL Injection in GitHub repository salesagility/suitecrm prior to 7.14.1.	9.1	More Details
CVE-2023-43909	Hospital Management System thru commit 4770d was discovered to contain a SQL injection vulnerability via the app_contact parameter in appsearch.php.	9.1	More Details
CVE-2023-44206	Sensitive information disclosure and manipulation due to improper authorization. The following products are affected: Acronis Cyber Protect 15 (Linux, Windows) before build 35979.	9.1	More Details
CVE-2023-28540	Cryptographic issue in Data Modem due to improper authentication during TLS handshake.	9.1	More Details
CVE-2023-40436	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14. An attacker may be able to cause unexpected system termination or read kernel memory.	9.1	More Details
CVE-2023-5185	Gym Management System Project v1.0 is vulnerable to an Insecure File Upload vulnerability on the 'file' parameter of profile/i.php page, allowing an authenticated attacker to obtain Remote Code Execution on the server hosting the application.	9.1	More Details
CVE-2023-44152	Sensitive information disclosure and manipulation due to improper authentication. The following products are affected: Acronis Cyber Protect 15 (Linux, macOS, Windows) before build 35979.	9.1	More Details
CVE-2023-32670	Cross-Site Scripting vulnerability in BuddyBoss 2.2.9 version , which could allow a local attacker with basic privileges to execute a malicious payload through the "[name]=image.jpg" parameter, allowing to assign a persistent javascript payload that would be triggered when the associated image is loaded.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference

CVE Number	Description	Base Score	Reference
CVE-2023-42819	JumpServer is an open source bastion host. Logged-in users can access and modify the contents of any file on the system. A user can use the 'Job-Template' menu and create a playbook named 'test'. Get the playbook id from the detail page, like 'e0adabef-c38f-492d-bd92-832bacc3df5f'. An attacker can exploit the directory traversal flaw using the provided URL to access and retrieve the contents of the file. `https://jumpserver-ip/api/v1/ops/playbook/e0adabef-c38f-492d-bd92-832bacc3df5f/file/?key=../../../../../../etc/passwd` a similar method to modify the file content is also present. This issue has been addressed in version 3.6.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.9	More Details
CVE-2023-4934	Authorization Bypass Through User-Controlled Key vulnerability in Usta AYBS allows Authentication Abuse, Authentication Bypass.This issue affects AYBS: before 1.0.3.	8.8	More Details
CVE-2023-42771	Authentication bypass vulnerability in ACERA 1320 firmware ver.01.26 and earlier, and ACERA 1310 firmware ver.01.26 and earlier allows a network-adjacent unauthenticated attacker who can access the affected product to download configuration files and/or log files, and upload configuration files and/or firmware. They are affected when running in ST(Standalone) mode.	8.8	More Details
CVE-2023-41074	The issue was addressed with improved checks. This issue is fixed in tvOS 17, Safari 17, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-39378	SiberianCMS - CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') by an unauthenticated user	8.8	More Details
CVE-2023-39434	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17 and iPadOS 17, watchOS 10, macOS Sonoma 14. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-36628	A flaw exists in VASA which allows users with access to a vSphere/ESXi VMware admin on a FlashArray to gain root access through privilege escalation.	8.8	More Details
CVE-2023-41450	An issue in phpkobo AjaxNewsTicker v.1.0.5 allows a remote attacker to execute arbitrary code via a crafted payload to the reque parameter.	8.8	More Details
CVE-2023-43014	Asset Management System v1.0 is vulnerable to an Authenticated SQL Injection vulnerability on the 'first_name' and 'last_name' parameters of user.php page, allowing an authenticated attacker to dump all the contents of the database contents.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39222	OS command injection vulnerability in FURUNO SYSTEMS wireless LAN access point devices allows an authenticated user to execute an arbitrary OS command that is not intended to be executed from the web interface by sending a specially crafted request. Affected products and versions are as follows: ACERA 1320 firmware ver.01.26 and earlier, ACERA 1310 firmware ver.01.26 and earlier, ACERA 1210 firmware ver.02.36 and earlier, ACERA 1150i firmware ver.01.35 and earlier, ACERA 1150w firmware ver.01.35 and earlier, ACERA 1110 firmware ver.01.76 and earlier, ACERA 1020 firmware ver.01.86 and earlier, ACERA 1010 firmware ver.01.86 and earlier, ACERA 950 firmware ver.01.60 and earlier, ACERA 850F firmware ver.01.60 and earlier, ACERA 900 firmware ver.02.54 and earlier, ACERA 850M firmware ver.02.06 and earlier, ACERA 810 firmware ver.03.74 and earlier, and ACERA 800ST firmware ver.07.35 and earlier. They are affected when running in ST(Standalone) mode.	8.8	More Details
CVE-2023-43740	Online Book Store Project v1.0 is vulnerable to an Insecure File Upload vulnerability on the 'image' parameter of admin_edit.php page, allowing an authenticated attacker to obtain Remote Code Execution on the server hosting the application.	8.8	More Details
CVE-2023-43226	An arbitrary file upload vulnerability in dede/baidunews.php in DedeCMS 5.7.111 and earlier allows attackers to execute arbitrary code via uploading a crafted PHP file.	8.8	More Details
CVE-2023-43610	SQL injection vulnerability in Order Data Edit page of Welcart e-Commerce versions 2.7 to 2.8.21 allows a user with editor (without setting authority) or higher privilege to perform unintended database operations.	8.8	More Details
CVE-2023-41086	Cross-site request forgery (CSRF) vulnerability exists in FURUNO SYSTEMS wireless LAN access point devices. If a user views a malicious page while logged in, unintended operations may be performed. Affected products and versions are as follows: ACERA 1210 firmware ver.02.36 and earlier, ACERA 1150i firmware ver.01.35 and earlier, ACERA 1150w firmware ver.01.35 and earlier, ACERA 1110 firmware ver.01.76 and earlier, ACERA 1020 firmware ver.01.86 and earlier, ACERA 1010 firmware ver.01.86 and earlier, ACERA 950 firmware ver.01.60 and earlier, ACERA 850F firmware ver.01.60 and earlier, ACERA 900 firmware ver.02.54 and earlier, ACERA 850M firmware ver.02.06 and earlier, ACERA 810 firmware ver.03.74 and earlier, and ACERA 800ST firmware ver.07.35 and earlier. They are affected when running in ST(Standalone) mode.	8.8	More Details
CVE-2023-5217	Heap buffer overflow in vp8 encoding in libvpx in Google Chrome prior to 117.0.5938.132 and libvpx 1.13.1 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44466	An issue was discovered in net/ceph/messenger_v2.c in the Linux kernel before 6.4.5. There is an integer signedness error, leading to a buffer overflow and remote code execution via HELLO or one of the AUTH frames. This occurs because of an untrusted length taken from a TCP packet in ceph_decode_32.	8.8	More Details
CVE-2023-5187	Use after free in Extensions in Google Chrome prior to 117.0.5938.132 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-5186	Use after free in Passwords in Google Chrome prior to 117.0.5938.132 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: High)	8.8	More Details
CVE-2023-2681	An SQL Injection vulnerability has been found on Jorani version 1.0.0. This vulnerability allows an authenticated remote user, with low privileges, to send queries with malicious SQL code on the "/leaves/validate" path and the “id” parameter, managing to extract arbitrary information from the database.	8.8	More Details
CVE-2023-4098	It has been identified that the web application does not correctly filter input parameters, allowing SQL injections, DoS or information disclosure. As a prerequisite, it is necessary to log into the application.	8.8	More Details
CVE-2023-4097	The file upload functionality is not implemented correctly and allows uploading of any type of file. As a prerequisite, it is necessary for the attacker to log into the application with a valid username.	8.8	More Details
CVE-2023-43192	SQL injection can exist in a newly created part of the SpringbootCMS 1.0 background, and the parameters submitted by users are not filtered. As a result, special characters in parameters destroy the original logic of SQL statements. Attackers can use this vulnerability to execute any SQL statement.	8.8	More Details
CVE-2023-41452	Cross Site Request Forgery vulnerability in phpkobo AjaxNewTicker v.1.0.5 allows a remote attacker to execute arbitrary code via a crafted payload to the txt parameter in the index.php component.	8.8	More Details
CVE-2023-43320	An issue in Proxmox Server Solutions GmbH Proxmox VE v.5.4 thru v.8.0, Proxmox Backup Server v.1.1 thru v.3.0, and Proxmox Mail Gateway v.7.1 thru v.8.0 allows a remote authenticated attacker to escalate privileges via bypassing the two-factor authentication component.	8.8	More Details
CVE-2023-40451	This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in Safari 17. An attacker with JavaScript execution may be able to execute arbitrary code.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38877	A host header injection vulnerability exists in gugoan's Economizzer v.0.9-beta1 and commit 3730880 (April 2023). By sending a specially crafted host header in the reset password request, it is possible to send password reset links to users which, once clicked, lead to an attacker-controlled server and thus leak the password reset token. This allows an attacker to reset other users' passwords.	8.8	More Details
CVE-2023-38874	A remote code execution (RCE) vulnerability via an insecure file upload exists in gugoan's Economizzer v.0.9-beta1 and commit 3730880 (April 2023). A malicious attacker can upload a PHP web shell as an attachment when adding a new cash book entry. Afterwards, the attacker may visit the web shell and execute arbitrary commands.	8.8	More Details
CVE-2023-20231	A vulnerability in the web UI of Cisco IOS XE Software could allow an authenticated, remote attacker to perform an injection attack against an affected device. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to execute arbitrary Cisco IOS XE Software CLI commands with level 15 privileges. Note: This vulnerability is exploitable only if the attacker obtains the credentials for a Lobby Ambassador account. This account is not configured by default.	8.8	More Details
CVE-2023-42222	WebCatalog before 49.0 is vulnerable to Incorrect Access Control. WebCatalog calls the Electron shell.openExternal function without verifying that the URL is for an http or https resource, in some circumstances.	8.8	More Details
CVE-2023-5289	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.8.4.	8.8	More Details
CVE-2022-35908	Cambium Enterprise Wi-Fi System Software before 6.4.2 does not sanitize the ping host argument in device-agent.	8.8	More Details
CVE-2023-28055	Dell NetWorker, Version 19.7 has an improper authorization vulnerability in the NetWorker client. An unauthenticated attacker within the same network could potentially exploit this by manipulating a command leading to gain of complete access to the server file further resulting in information leaks, denial of service, and arbitrary code execution. Dell recommends customers to upgrade at the earliest opportunity.	8.8	More Details
CVE-2023-35793	An issue was discovered in Cassia Access Controller 2.1.1.2303271039. Establishing a web SSH session to gateways is vulnerable to Cross Site Request Forgery (CSRF) attacks.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0506	The web service of ByDemes Group Airspace CCTV Web Service in its 2.616.BY00.11 version, contains a privilege escalation vulnerability, detected in the Camera Control Panel, whose exploitation could allow a low-privileged attacker to gain administrator access.	8.8	More Details
CVE-2023-43176	A deserialization vulnerability in Afterlogic Aurora Files v9.7.3 allows attackers to execute arbitrary code via supplying a crafted .sabredav file.	8.8	More Details
CVE-2023-43835	Super Store Finder 3.7 and below is vulnerable to authenticated Arbitrary PHP Code Injection that could lead to Remote Code Execution when settings overwrite config.inc.php content.	8.8	More Details
CVE-2023-4103	QSige statistics are affected by a remote SQLi vulnerability. It has been identified that the web application does not correctly filter input parameters, allowing SQL injections, DoS or information disclosure. As a prerequisite, it is necessary to log into the application.	8.8	More Details
CVE-2023-35074	The issue was addressed with improved memory handling. This issue is fixed in tvOS 17, Safari 17, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-43890	Netis N3Mv2-V1.0.1.865 was discovered to contain a command injection vulnerability in the diagnostic tools page. This vulnerability is exploited via a crafted HTTP request.	8.8	More Details
CVE-2023-43268	Deyue Remote Vehicle Management System v1.1 was discovered to contain a deserialization vulnerability.	8.8	More Details
CVE-2023-32541	A use-after-free vulnerability exists in the footerr functionality of Hancom Office 2020 HWord 11.0.0.7520. A specially crafted .doc file can lead to a use-after-free. An attacker can trick a user into opening a malformed file to trigger this vulnerability.	8.8	More Details
CVE-2023-44218	A flaw within the SonicWall NetExtender Pre-Logon feature enables an unauthorized user to gain access to the host Windows operating system with 'SYSTEM' level privileges, leading to a local privilege escalation (LPE) vulnerability.	8.8	More Details
CVE-2023-4102	QSige login SSO does not have an access control mechanism to verify whether the user requesting a resource has sufficient permissions to do so. As a prerequisite, it is necessary to log into the application.	8.8	More Details
CVE-2023-4101	The QSige login SSO does not have an access control mechanism to verify whether the user requesting a resource has sufficient permissions to do so. As a prerequisite, it is necessary to log into the application.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21673	Improper Access to the VM resource manager can lead to Memory Corruption.	8.7	More Details
CVE-2023-20033	A vulnerability in Cisco IOS XE Software for Cisco Catalyst 3650 and Catalyst 3850 Series Switches could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper resource management when processing traffic that is received on the management interface. An attacker could exploit this vulnerability by sending a high rate of traffic to the management interface. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2023-43662	ShokoServer is a media server which specializes in organizing anime. In affected versions the `/api/Image/WithPath` endpoint is accessible without authentication and is supposed to return default server images. The endpoint accepts the parameter `serverImagePath`, which is not sanitized in any way before being passed to `System.IO.File.OpenRead`, which results in an arbitrary file read. This issue may lead to an arbitrary file read which is exacerbated in the windows installer which installs the ShokoServer as administrator. Any unauthenticated attacker may be able to access sensitive information and read files stored on the server. The `/api/Image/WithPath` endpoint has been removed in commit `6c57ba0f0` which will be included in subsequent releases. Users should limit access to the `/api/Image/WithPath` endpoint or manually patch their installations until a patched release is made. This issue was discovered by the GitHub Security lab and is also indexed as GHSL-2023-191.	8.6	More Details
CVE-2023-43646	get-func-name is a module to retrieve a function's name securely and consistently both in NodeJS and the browser. Versions prior to 2.0.1 are subject to a regular expression denial of service (redos) vulnerability which may lead to a denial of service when parsing malicious input. This vulnerability can be exploited when there is an imbalance in parentheses, which results in excessive backtracking and subsequently increases the CPU load and processing time significantly. This vulnerability can be triggered using the following input: '\t'.repeat(54773) + '\t/function/i'. This issue has been addressed in commit `f934b228b` which has been included in releases from 2.0.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20227	A vulnerability in the Layer 2 Tunneling Protocol (L2TP) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of certain L2TP packets. An attacker could exploit this vulnerability by sending crafted L2TP packets to an affected device. A successful exploit could allow the attacker to cause the device to reload unexpectedly, resulting in a DoS condition. Note: Only traffic directed to the affected system can be used to exploit this vulnerability.	8.6	More Details
CVE-2023-20226	A vulnerability in Application Quality of Experience (AppQoE) and Unified Threat Defense (UTD) on Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to the mishandling of a crafted packet stream through the AppQoE or UTD application. An attacker could exploit this vulnerability by sending a crafted packet stream through an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2023-20223	A vulnerability in Cisco DNA Center could allow an unauthenticated, remote attacker to read and modify data in a repository that belongs to an internal service on an affected device. This vulnerability is due to insufficient access control enforcement on API requests. An attacker could exploit this vulnerability by sending a crafted API request to an affected device. A successful exploit could allow the attacker to read and modify data that is handled by an internal service on the affected device.	8.6	More Details
CVE-2023-3769	Incorrect data input validation vulnerability, which could allow an attacker with access to the network to implement fuzzing techniques that would allow him to gain knowledge about specially crafted packets that would create a DoS condition through the MMS protocol when initiating communication, achieving a complete system reboot of the device and its services.	8.6	More Details
CVE-2023-40448	The issue was addressed with improved handling of protocols. This issue is fixed in tvOS 17, iOS 16.7 and iPadOS 16.7, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. A remote attacker may be able to break out of Web Content sandbox.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20187	A vulnerability in the Multicast Leaf Recycle Elimination (mLRE) feature of Cisco IOS XE Software for Cisco ASR 1000 Series Aggregation Services Routers could allow an unauthenticated, remote attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability is due to incorrect handling of certain IPv6 multicast packets when they are fanned out more than seven times on an affected device. An attacker could exploit this vulnerability by sending a specific IPv6 multicast or IPv6 multicast VPN (MVPNv6) packet through the affected device. A successful exploit could allow the attacker to cause a reload of the affected device, resulting in a DoS condition.	8.6	More Details
CVE-2023-3768	Incorrect data input validation vulnerability, which could allow an attacker with access to the network to implement fuzzing techniques that would allow him to gain knowledge about specially crafted packets that would create a DoS condition through the MMS protocol when initiating communication, achieving a complete system reboot of the device and its services.	8.6	More Details
CVE-2023-43651	JumpServer is an open source bastion host. An authenticated user can exploit a vulnerability in MongoDB sessions to execute arbitrary commands, leading to remote code execution. This vulnerability may further be leveraged to gain root privileges on the system. Through the WEB CLI interface provided by the koko component, a user logs into the authorized mongoDB database and exploits the MongoDB session to execute arbitrary commands. This vulnerability has been addressed in versions 2.28.20 and 3.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3440	Incorrect Default Permissions vulnerability in Hitachi JP1/Performance Management on Windows allows File Manipulation.This issue affects JP1/Performance Management - Manager: from 09-00 before 12-50-07; JP1/Performance Management - Base: from 09-00 through 10-50-*; JP1/Performance Management - Agent Option for Application Server: from 11-00 before 11-50-16; JP1/Performance Management - Agent Option for Enterprise Applications: from 09-00 before 12-00-14; JP1/Performance Management - Agent Option for HiRDB: from 09-00 before 12-00-14; JP1/Performance Management - Agent Option for IBM Lotus Domino: from 10-00 before 11-50-16; JP1/Performance Management - Agent Option for Microsoft(R) Exchange Server: from 09-00 before 12-00-14; JP1/Performance Management - Agent Option for Microsoft(R) Internet Information Server: from 09-00 before 12-00-14; JP1/Performance Management - Agent Option for Microsoft(R) SQL Server: from 09-00 before 12-50-07; JP1/Performance Management - Agent Option for Oracle: from 09-00 before 12-10-08; JP1/Performance Management - Agent Option for Platform: from 09-00 before 12-50-07; JP1/Performance Management - Agent Option for Service Response: from 09-00 before 11-50-16; JP1/Performance Management - Agent Option for Transaction System: from 11-00 before 12-00-14; JP1/Performance Management - Remote Monitor for Microsoft(R) SQL Server: from 09-00 before 12-50-07; JP1/Performance Management - Remote Monitor for Oracle: from 09-00 before 12-10-08; JP1/Performance Management - Remote Monitor for Platform: from 09-00 before 12-10-08; JP1/Performance Management - Remote Monitor for Virtual Machine: from 10-00 before 12-50-07; JP1/Performance Management - Agent Option for Domino: from 09-00 through 09-00-*; JP1/Performance Management - Agent Option for IBM WebSphere Application Server: from 09-00 through 10-00-*; JP1/Performance Management - Agent Option for IBM WebSphere MQ: from 09-00 through 10-00-*; JP1/Performance Management - Agent Option for JP1/AJS3: from 09-00 through 10-00-*; JP1/Performance Management - Agent Option for OpenTP1: from 09-00 through 10-00-*; JP1/Performance Management - Agent Option for Oracle WebLogic Server: from 09-00 through 10-00-*; JP1/Performance Management - Agent Option for uCosminexus Application Server: from 09-00 through 10-00-*; JP1/Performance Management - Agent Option for Virtual Machine: from 09-00 through 09-01-*.	8.4	More Details
CVE-2023-24844	Memory Corruption in Core while invoking a call to Access Control core library with hardware protected address range.	8.4	More Details
CVE-2023-33029	Memory corruption in DSP Service during a remote call from HLOS to DSP.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24853	Memory Corruption in HLOS while registering for key provisioning notify.	8.4	More Details
CVE-2023-33039	Memory corruption in Automotive Display while destroying the image handle created using connected display driver.	8.4	More Details
CVE-2023-40047	In WS_FTP Server version prior to 8.8.2, a stored cross-site scripting (XSS) vulnerability exists in WS_FTP Server's Management module. An attacker with administrative privileges could import a SSL certificate with malicious attributes containing cross-site scripting payloads. Once the cross-site scripting payload is successfully stored, an attacker could leverage this vulnerability to target WS_FTP Server admins with a specialized payload which results in the execution of malicious JavaScript within the context of the victims browser.	8.3	More Details
CVE-2023-40045	In WS_FTP Server versions prior to 8.7.4 and 8.8.2, a reflected cross-site scripting (XSS) vulnerability exists in WS_FTP Server's Ad Hoc Transfer module. An attacker could leverage this vulnerability to target WS_FTP Server users with a specialized payload which results in the execution of malicious JavaScript within the context of the victims browser.	8.3	More Details
CVE-2023-40046	In WS_FTP Server versions prior to 8.7.4 and 8.8.2, a SQL injection vulnerability exists in the WS_FTP Server manager interface. An attacker may be able to infer information about the structure and contents of the database and execute SQL statements that alter or delete database elements.	8.2	More Details
CVE-2023-5207	A vulnerability was discovered in GitLab CE and EE affecting all versions starting 16.0 prior to 16.2.8, 16.3 prior to 16.3.5, and 16.4 prior to 16.4.1. An authenticated attacker could perform arbitrary pipeline execution under the context of another user.	8.2	More Details
CVE-2023-22385	Memory Corruption in Data Modem while making a MO call or MT VOLTE call.	8.2	More Details
CVE-2023-24849	Information Disclosure in data Modem while parsing an FMTP line in an SDP message.	8.2	More Details
CVE-2023-24848	Information Disclosure in Data Modem while performing a VoLTE call with an undefined RTCP FB line value.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43650	JumpServer is an open source bastion host. The verification code for resetting user's password is vulnerable to brute-force attacks due to the absence of rate limiting. JumpServer provides a feature allowing users to reset forgotten passwords. Affected users are sent a 6-digit verification code, ranging from 000000 to 999999, to facilitate the password reset. Although the code is only available in 1 minute, this window potentially allows for up to 1,000,000 validation attempts. This issue has been addressed in versions 2.28.20 and 3.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.2	More Details
CVE-2023-5106	An issue has been discovered in Ultimate-licensed GitLab EE affecting all versions starting 13.12 prior to 16.2.8, 16.3.0 prior to 16.3.5, and 16.4.0 prior to 16.4.1 that could allow an attacker to impersonate users in CI pipelines through direct transfer group imports.	8.2	More Details
CVE-2023-3349	Information exposure vulnerability in IBERMATICA RPS 2019, which exploitation could allow an unauthenticated user to retrieve sensitive information, such as usernames, IP addresses or SQL queries sent to the application. By accessing the URL /RPS2019Service/status.html, the application enables the logging mechanism by generating the log file, which can be downloaded.	8.2	More Details
CVE-2023-43652	JumpServer is an open source bastion host. As an unauthenticated user, it is possible to authenticate to the core API with a username and an SSH public key without needing a password or the corresponding SSH private key. An SSH public key should be considered public knowledge and should not used as an authentication secret alone. JumpServer provides an API for the KoKo component to validate user private key logins. This API does not verify the source of requests and will generate a personal authentication token. Given that public keys can be easily leaked, an attacker can exploit the leaked public key and username to authenticate, subsequently gaining access to the current user's information and authorized actions. This issue has been addressed in versions 2.28.20 and 3.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.2	More Details
CVE-2023-3350	A Cryptographic Issue vulnerability has been found on IBERMATICA RPS, affecting version 2019. By firstly downloading the log file, an attacker could retrieve the SQL query sent to the application in plaint text. This log file contains the password hashes coded with AES-CBC-128 bits algorithm, which can be decrypted with a .NET function, obtaining the username's password in plain text.	8.2	More Details
CVE-2022-47891	All versions of NetMan 204 allow an attacker that knows the MAC and serial number of the device to reset the administrator password via the legitimate recovery function.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44154	Sensitive information disclosure and manipulation due to improper authorization. The following products are affected: Acronis Cyber Protect 15 (Linux, Windows) before build 35979.	8.1	More Details
CVE-2023-41326	GLPI stands for Gestionnaire Libre de Parc Informatique is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. A logged user from any profile can hijack the Kanban feature to alter any user field, and end-up with stealing its account. Users are advised to upgrade to version 10.0.10. There are no known workarounds for this vulnerability.	8.1	More Details
CVE-2023-41320	GLPI stands for Gestionnaire Libre de Parc Informatique is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. UI layout preferences management can be hijacked to lead to SQL injection. This injection can be use to takeover an administrator account. Users are advised to upgrade to version 10.0.10. There are no known workarounds for this vulnerability.	8.1	More Details
CVE-2023-2315	Path Traversal in OpenCart versions 4.0.0.0 to 4.0.2.2 allows an authenticated user with access/modify privilege on the Log component to empty out arbitrary files on the server	8.1	More Details
CVE-2023-41324	GLPI stands for Gestionnaire Libre de Parc Informatique is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. An API user that have read access on users resource can steal accounts of other users. Users are advised to upgrade to version 10.0.10. There are no known workarounds for this vulnerability.	8.1	More Details
CVE-2023-43976	An issue in CatoNetworks CatoClient before v.5.4.0 allows attackers to escalate privileges and winning the race condition (TOCTOU) via the PrivilegedHelperTool component.	8.1	More Details
CVE-2023-20186	A vulnerability in the Authentication, Authorization, and Accounting (AAA) feature of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker to bypass command authorization and copy files to or from the file system of an affected device using the Secure Copy Protocol (SCP). This vulnerability is due to incorrect processing of SCP commands in AAA command authorization checks. An attacker with valid credentials and level 15 privileges could exploit this vulnerability by using SCP to connect to an affected device from an external machine. A successful exploit could allow the attacker to obtain or change the configuration of the affected device and put files on or retrieve files from the affected device.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26218	The Web Client component of TIBCO Software Inc.'s TIBCO Nimbus contains easily exploitable Reflected Cross Site Scripting (XSS) vulnerabilities that allow a low privileged attacker to social engineer a legitimate user with network access to execute scripts targeting the affected system or the victim's local system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Nimbus: versions 10.6.0 and below.	8.0	More Details
CVE-2023-41444	An issue in Binalyze IREC.sys v.3.11.0 and before allows a local attacker to execute arbitrary code and escalate privileges via the fun_1400084d0 function in IREC.sys driver.	7.8	More Details
CVE-2023-24850	Memory Corruption in HLOS while importing a cryptographic key into KeyMaster Trusted Application.	7.8	More Details
CVE-2023-41063	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.6, tvOS 17, iOS 16.7 and iPadOS 16.7, iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-41068	An access issue was addressed with improved access restrictions. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10, iOS 16.7 and iPadOS 16.7. A user may be able to elevate privileges.	7.8	More Details
CVE-2023-41071	A use-after-free issue was addressed with improved memory management. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10, macOS Ventura 13.6. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-5197	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. Addition and removal of rules from chain bindings within the same transaction causes leads to use-after-free. We recommend upgrading past commit f15f29fd4779be8a418b66e9d52979bb6d6c2325.	7.8	More Details
CVE-2023-33035	Memory corruption while invoking callback function of AFE from ADSP.	7.8	More Details
CVE-2023-33034	Memory corruption while parsing the ADSP response command.	7.8	More Details
CVE-2023-41174	The issue was addressed with improved memory handling. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40412	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.6, tvOS 17, macOS Monterey 12.7, watchOS 10, iOS 17 and iPadOS 17. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-40443	The issue was addressed with improved checks. This issue is fixed in iOS 17 and iPadOS 17. An app may be able to gain root privileges.	7.8	More Details
CVE-2023-44464	pretix before 2023.7.2 allows Pillow to parse EPS files.	7.8	More Details
CVE-2023-41984	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.6, tvOS 17, iOS 16.7 and iPadOS 16.7, macOS Monterey 12.7, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-44157	Local privilege escalation due to insecure folder permissions. The following products are affected: Acronis Cyber Protect 15 (Windows) before build 35979.	7.8	More Details
CVE-2023-4911	A buffer overflow was discovered in the GNU C Library's dynamic loader ld.so while processing the GLIBC_TUNABLES environment variable. This issue could allow a local attacker to use maliciously crafted GLIBC_TUNABLES environment variables when launching binaries with SUID permission to execute code with elevated privileges.	7.8	More Details
CVE-2023-43361	Buffer Overflow vulnerability in Vorbis-tools v.1.4.2 allows a local attacker to execute arbitrary code and cause a denial of service during the conversion of wav files to ogg files.	7.8	More Details
CVE-2023-5345	A use-after-free vulnerability in the Linux kernel's fs/smb/client component can be exploited to achieve local privilege escalation. In case of an error in smb3_fs_context_parse_param, ctx->password was freed but the field was not set to NULL which could lead to double free. We recommend upgrading past commit e6e43b8aa7cd3c3af686caf0c2e11819a886d705.	7.8	More Details
CVE-2023-32396	This issue was addressed with improved checks. This issue is fixed in Xcode 15, tvOS 17, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to gain elevated privileges.	7.8	More Details
CVE-2023-40409	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.6, tvOS 17, macOS Monterey 12.7, watchOS 10, iOS 17 and iPadOS 17. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44217	A local privilege escalation vulnerability in SonicWall Net Extender MSI client for Windows 10.2.336 and earlier versions allows a local low-privileged user to gain system privileges through running repair functionality.	7.8	More Details
CVE-2023-40419	The issue was addressed with improved checks. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10. An app may be able to gain elevated privileges.	7.8	More Details
CVE-2023-32377	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-43825	Relative path traversal vulnerability in Shihonkanri Plus Ver9.0.3 and earlier allows a local attacker to execute an arbitrary code by having a legitimate user import a specially crafted backup file of the product..	7.8	More Details
CVE-2023-32477	Dell Common Event Enabler 8.9.8.2 for Windows and prior, contain an improper access control vulnerability. A local low-privileged malicious user may potentially exploit this vulnerability to gain elevated privileges.	7.8	More Details
CVE-2023-41995	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-4956	A vulnerability classified as critical has been found in Caphyon Advanced Installer 19.7. This affects an unknown part of the component WinSxS DLL Handler. The manipulation leads to uncontrolled search path. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used. Upgrading to version 19.7.1 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-240903.	7.8	More Details
CVE-2023-40431	The issue was addressed with improved memory handling. This issue is fixed in iOS 17 and iPadOS 17. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-40432	The issue was addressed with improved memory handling. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10, macOS Sonoma 14. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-43907	OptiPNG v0.7.7 was discovered to contain a global buffer overflow via the 'buffer' variable at gifread.c.	7.8	More Details
CVE-2023-38615	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42462	GLPI stands for Gestionnaire Libre de Parc Informatique is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. The document upload process can be diverted to delete some files. Users are advised to upgrade to version 10.0.10. There are no known workarounds for this vulnerability.	7.7	More Details
CVE-2023-31042	A flaw exists in FlashBlade Purity whereby an authenticated user with access to FlashBlade's object store protocol can impact the availability of the system's data access and replication protocols.	7.7	More Details
CVE-2023-36627	A flaw exists in FlashBlade Purity whereby a user with access to an administrative account on a FlashBlade that is configured with timezone-dependent snapshot schedules can configure a timezone to prevent the schedule from functioning properly.	7.7	More Details
CVE-2023-39347	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. An attacker with the ability to update pod labels can cause Cilium to apply incorrect network policies. This issue arises due to the fact that on pod update, Cilium incorrectly uses user-provided pod labels to select the policies which apply to the workload in question. This can affect Cilium network policies that use the namespace, service account or cluster constructs to restrict traffic, Cilium clusterwide network policies that use Cilium namespace labels to select the Pod and Kubernetes network policies. Non-existent construct names can be provided, which bypass all network policies applicable to the construct. For example, providing a pod with a non-existent namespace as the value of the `io.kubernetes.pod.namespace` label results in none of the namespaced CiliumNetworkPolicies applying to the pod in question. This attack requires the attacker to have Kubernetes API Server access, as described in the Cilium Threat Model. This issue has been resolved in: Cilium versions 1.14.2, 1.13.7, and 1.12.14. Users are advised to upgrade. As a workaround an admission webhook can be used to prevent pod label updates to the `k8s:io.kubernetes.pod.namespace` and `io.cilium.k8s.policy.*` keys.	7.6	More Details
CVE-2023-4099	The QSige Monitor application does not have an access control mechanism to verify whether the user requesting a resource has sufficient permissions to do so. As a prerequisite, it is necessary to log into the application.	7.6	More Details
CVE-2023-4003	One Identity Password Manager version 5.9.7.1 - An unauthenticated attacker with physical access to a workstation may upgrade privileges to SYSTEM through an unspecified method. CWE-250: Execution with Unnecessary Privileges.	7.6	More Details
CVE-2023-5077	The Vault and Vault Enterprise ("Vault") Google Cloud secrets engine did not preserve existing Google Cloud IAM Conditions upon creating or updating rolesets. Fixed in Vault 1.13.0.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43381	SQL Injection vulnerability in Tianchoy Blog v.1.8.8 allows a remote attacker to obtain sensitive information via the id parameter in the login.php	7.5	More Details
CVE-2023-44159	Sensitive information disclosure due to cleartext storage of sensitive information. The following products are affected: Acronis Cyber Protect 15 (Linux, Windows) before build 35979.	7.5	More Details
CVE-2023-44158	Sensitive information disclosure due to insufficient token field masking. The following products are affected: Acronis Cyber Protect 15 (Linux, Windows) before build 35979.	7.5	More Details
CVE-2023-43856	Dreamer CMS v4.1.3 was discovered to contain an arbitrary file read vulnerability via the component /admin/TemplateController.java.	7.5	More Details
CVE-2023-44153	Sensitive information disclosure due to cleartext storage of sensitive information in memory. The following products are affected: Acronis Cyber Protect 15 (Linux, macOS, Windows) before build 35979.	7.5	More Details
CVE-2023-44155	Sensitive information leak through log files. The following products are affected: Acronis Cyber Protect 15 (Linux, Windows) before build 35979.	7.5	More Details
CVE-2023-44156	Sensitive information disclosure due to spell-jacking. The following products are affected: Acronis Cyber Protect 15 (Linux, Windows) before build 35979.	7.5	More Details
CVE-2022-48606	Stability-related vulnerability in the binder background management and control module. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2023-5157	A vulnerability was found in MariaDB. An OpenVAS port scan on ports 3306 and 4567 allows a malicious remote client to cause a denial of service.	7.5	More Details
CVE-2023-43866	D-Link DIR-619L B1 2.02 is vulnerable to Buffer Overflow via formSetWAN_Wizard7 function.	7.5	More Details
CVE-2023-32820	In wlan firmware, there is a possible firmware assertion due to improper input handling. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07932637; Issue ID: ALPS07932637.	7.5	More Details
CVE-2023-44488	VP9 in libvpx before 1.13.1 mishandles widths, leading to a crash related to encoding.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5318	Use of Hard-coded Credentials in GitHub repository microweber/microweber prior to 2.0.	7.5	More Details
CVE-2023-39410	When deserializing untrusted or corrupted data, it is possible for a reader to consume memory beyond the allowed constraints and thus lead to out of memory on the system. This issue affects Java applications using Apache Avro Java SDK up to and including 1.11.2. Users should update to apache-avro version 1.11.3 which addresses this issue.	7.5	More Details
CVE-2023-41580	Phpipam before v1.5.2 was discovered to contain a LDAP injection vulnerability via the dname parameter at /users/ad-search-result.php. This vulnerability allows attackers to enumerate arbitrary fields in the LDAP server and access sensitive data via a crafted POST request.	7.5	More Details
CVE-2023-5344	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1969.	7.5	More Details
CVE-2023-30591	Denial-of-service in NodeBB <= v2.8.10 allows unauthenticated attackers to trigger a crash, when invoking `eventName.startsWith()` or `eventName.toString()`, while processing Socket.IO messages via crafted Socket.IO messages containing array or object type for the event name respectively.	7.5	More Details
CVE-2023-4316	Zod in versions 3.21.0 up to and including 3.22.3 allows an attacker to perform a denial of service while validating emails.	7.5	More Details
CVE-2023-5256	In certain scenarios, Drupal's JSON:API module will output error backtraces. With some configurations, this may cause sensitive information to be cached and made available to anonymous users, leading to privilege escalation. This vulnerability only affects sites with the JSON:API module enabled, and can be mitigated by uninstalling JSON:API. The core REST and contributed GraphQL modules are not affected.	7.5	More Details
CVE-2023-26152	All versions of the package static-server are vulnerable to Directory Traversal due to improper input sanitization passed via the validPath function of server.js.	7.5	More Details
CVE-2023-43868	D-Link DIR-619L B1 2.02 is vulnerable to Buffer Overflow via websGetVar function.	7.5	More Details
CVE-2023-43867	D-Link DIR-619L B1 2.02 is vulnerable to Buffer Overflow via formSetWanL2TP function.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43865	D-Link DIR-619L B1 2.02 is vulnerable to Buffer Overflow via formSetWanPPTP function.	7.5	More Details
CVE-2023-5173	In a non-standard configuration of Firefox, an integer overflow could have occurred based on network traffic (possibly under influence of a local unprivileged webpage), leading to an out-of-bounds write to privileged process memory. *This bug only affects Firefox if a non-standard preference allowing non-HTTPS Alternate Services (`network.http.altsvc.oe`) is enabled.* This vulnerability affects Firefox < 118.	7.5	More Details
CVE-2023-43864	D-Link DIR-619L B1 2.02 is vulnerable to Buffer Overflow via formSetWAN_Wizard55 function.	7.5	More Details
CVE-2023-43863	D-Link DIR-619L B1 2.02 is vulnerable to Buffer Overflow via formSetWanDhcpplus function.	7.5	More Details
CVE-2023-43862	D-Link DIR-619L B1 2.02 is vulnerable to Buffer Overflow via formLanguageChange function.	7.5	More Details
CVE-2023-43861	D-Link DIR-619L B1 2.02 is vulnerable to Buffer Overflow via formSetWanPPPoE function.	7.5	More Details
CVE-2023-43860	D-Link DIR-619L B1 2.02 is vulnerable to Buffer Overflow via formSetWanNonLogin function.	7.5	More Details
CVE-2023-24843	Transient DOS in Modem while triggering a camping on an 5G cell.	7.5	More Details
CVE-2023-42487	Soundminer – CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7.5	More Details
CVE-2023-24847	Transient DOS in Modem while allocating DSM items.	7.5	More Details
CVE-2023-43314	** UNSUPPORTED WHEN ASSIGNED **The buffer overflow vulnerability in the Zyxel PMG2005-T20B firmware version V1.00(ABNK.2)b11_C0 could allow an unauthenticated attacker to cause a denial of service condition via a crafted uid.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33026	Transient DOS in WLAN Firmware while parsing a NAN management frame.	7.5	More Details
CVE-2023-33027	Transient DOS in WLAN Firmware while parsing rsn ies.	7.5	More Details
CVE-2023-3655	cashIT! - serving solutions. Devices from "PoS/ Dienstleistung, Entwicklung & Vertrieb GmbH" to 03.A06rks 2023.02.37 are affected by a dangerous methods, that allows to leak the database (system settings, user accounts,...). This vulnerability can be triggered by an HTTP endpoint exposed to the network.	7.5	More Details
CVE-2022-47186	There is an unrestricted upload of file vulnerability in Generex CS141 below 2.06 version. An attacker could upload and/or delete any type of file, without any format restriction and without any authentication, in the "upload" directory.	7.5	More Details
CVE-2023-20034	Vulnerability in the Elasticsearch database used in the of Cisco SD-WAN vManage software could allow an unauthenticated, remote attacker to access the Elasticsearch configuration database of an affected device with the privileges of the elasticsearch user. These vulnerability is due to the presence of a static username and password configured on the vManage. An attacker could exploit this vulnerability by sending a crafted HTTP request to a reachable vManage on port 9200. A successful exploit could allow the attacker to view the Elasticsearch database content. There are workarounds that address this vulnerability.	7.5	More Details
CVE-2023-41307	Memory overwriting vulnerability in the security module. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2023-41309	Permission control vulnerability in the MediaPlaybackController module. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2023-41305	Vulnerability of 5G messages being sent without being encrypted in a VPN environment in the SMS message module. Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details
CVE-2023-40407	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14. A remote attacker may be able to cause a denial-of-service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4882	DOS vulnerability that could allow an attacker to register a new VNF (Virtual Network Function) value. This action could trigger the args_assets() function defined in the arg-log.php file, which would then execute the args-abort.c file, causing the service to crash.	7.5	More Details
CVE-2023-4883	Invalid pointer release vulnerability. Exploitation of this vulnerability could allow an attacker to interrupt the correct operation of the service by sending a specially crafted json string to the VNF (Virtual Network Function), and triggering the ogs_sbi_message_free function, which could cause a service outage.	7.5	More Details
CVE-2023-39375	SiberianCMS - CWE-274: Improper Handling of Insufficient Privileges	7.5	More Details
CVE-2023-3223	A flaw was found in undertow. Servlets annotated with @MultipartConfig may cause an OutOfMemoryError due to large multipart content. This may allow unauthorized users to cause remote Denial of Service (DoS) attack. If the server uses fileSizeThreshold to limit the file size, it's possible to bypass the limit by setting the file name in the request to null.	7.5	More Details
CVE-2023-41308	Screenshot vulnerability in the input module. Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details
CVE-2023-5170	In canvas rendering, a compromised content process could have caused a surface to change unexpectedly, leading to a memory leak of a privileged process. This memory leak could be used to effect a sandbox escape if the correct data was leaked. This vulnerability affects Firefox < 118.	7.4	More Details
CVE-2023-26145	This affects versions of the package pydash before 6.0.0. A number of pydash methods such as pydash.objects.invoke() and pydash.collections.invoke_map() accept dotted paths (Deep Path Strings) to target a nested Python object, relative to the original source object. These paths can be used to target internal class attributes and dict items, to retrieve, modify or invoke nested Python objects. **Note:** The pydash.objects.invoke() method is vulnerable to Command Injection when the following prerequisites are satisfied: 1) The source object (argument 1) is not a built-in object such as list/dict (otherwise, the __init__.__globals__ path is not accessible) 2) The attacker has control over argument 2 (the path string) and argument 3 (the argument to pass to the invoked method) The pydash.collections.invoke_map() method is also vulnerable, but is harder to exploit as the attacker does not have direct control over the argument to be passed to the invoked function.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0456	A flaw was found in APICast, when 3Scale's OIDC module does not properly evaluate the response to a mismatched token from a separate realm. This could allow a separate realm to be accessible to an attacker, permitting access to unauthorized information.	7.4	More Details
CVE-2023-40375	Integrated application server for IBM i 7.2, 7.3, 7.4, and 7.5 contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain root access to the host operating system. IBM X-Force ID: 263580.	7.4	More Details
CVE-2023-22382	Weak configuration in Automotive while VM is processing a listener request from TEE.	7.4	More Details
CVE-2023-32458	Dell AppSync, versions 4.4.0.0 to 4.6.0.0 including Service Pack releases, contains an improper access control vulnerability in Embedded Service Enabler component. A local malicious user could potentially exploit this vulnerability during installation leading to a privilege escalation.	7.3	More Details
CVE-2023-39377	SiberianCMS - CWE-434: Unrestricted Upload of File with Dangerous Type - A malicious user with administrative privileges may be able to upload a dangerous filetype via an unspecified method	7.2	More Details
CVE-2023-43657	discourse-encrypt is a plugin that provides a secure communication channel through Discourse. Improper escaping of encrypted topic titles could lead to a cross site scripting (XSS) issue when a site has content security policy (CSP) headers disabled. Having CSP disabled is a non-default configuration, and having it disabled with discourse-encrypt installed will result in a warning in the Discourse admin dashboard. This has been fixed in commit `9c75810af9` which is included in the latest version of the discourse-encrypt plugin. Users are advised to upgrade. Users unable to upgrade should ensure that CSP headers are enabled and properly configured.	7.2	More Details
CVE-2023-20254	A vulnerability in the session management system of the Cisco Catalyst SD-WAN Manager multi-tenant feature could allow an authenticated, remote attacker to access another tenant that is being managed by the same Cisco Catalyst SD-WAN Manager instance. This vulnerability requires the multi-tenant feature to be enabled. This vulnerability is due to insufficient user session management within the Cisco Catalyst SD-WAN Manager system. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain unauthorized access to information about another tenant, make configuration changes, or possibly take a tenant offline causing a denial of service condition.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33972	Scylladb is a NoSQL data store using the seastar framework, compatible with Apache Cassandra. Authenticated users who are authorized to create tables in a keyspace can escalate their privileges to access a table in the same keyspace, even if they don't have permissions for that table. This issue has not yet been patched. A workaround to address this issue is to disable CREATE privileges on a keyspace, and create new tables on behalf of other users.	7.2	More Details
CVE-2023-4817	This vulnerability allows an authenticated attacker to upload malicious files by bypassing the restrictions of the upload functionality, compromising the entire device.	7.2	More Details
CVE-2023-44047	Sourcecodester Toll Tax Management System v1 is vulnerable to SQL Injection.	7.2	More Details
CVE-2023-44044	Super Store Finder v3.6 and below was discovered to contain a SQL injection vulnerability via the Search parameter at /admin/stores.php.	7.2	More Details
CVE-2023-40219	Welcart e-Commerce versions 2.7 to 2.8.21 allows a user with editor or higher privilege to upload an arbitrary file to an unauthorized directory.	7.2	More Details
CVE-2023-40664	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in RedNao Donations Made Easy – Smart Donations plugin <= 4.0.12 versions.	7.1	More Details
CVE-2023-30472	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in MyThemeShop URL Shortener by MyThemeShop plugin <= 1.0.17 versions.	7.1	More Details
CVE-2023-40663	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Rextheme WP VR plugin <= 8.3.4 versions.	7.1	More Details
CVE-2023-41658	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution Photo Gallery Slideshow & Masonry Tiled Gallery plugin <= 1.0.13 versions.	7.1	More Details
CVE-2023-41662	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Ulf Benjaminsson WP-dTree plugin <= 4.4.5 versions.	7.1	More Details
CVE-2023-39308	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in UserFeedback Team User Feedback plugin <= 1.0.7 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30471	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Cornel Raiu WP Search Analytics plugin <= 1.4.7 versions.	7.1	More Details
CVE-2023-40333	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Qode Interactive Bridge Core plugin <= 3.0.9 versions.	7.1	More Details
CVE-2023-40330	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Milan Petrovic GD Security Headers plugin <= 1.6.1 versions.	7.1	More Details
CVE-2023-40667	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Lasso Simple URLs plugin <= 117 versions.	7.1	More Details
CVE-2023-41238	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in UltimatelySocial Social Media Share Buttons & Social Sharing Icons plugin <= 2.8.3 versions.	7.1	More Details
CVE-2023-41237	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Everest Themes Arya Multipurpose Pro theme <= 1.0.8 versions.	7.1	More Details
CVE-2023-41236	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Happy addons Happy Elementor Addons Pro plugin <= 2.8.0 versions.	7.1	More Details
CVE-2023-41235	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Everest Themes Everest News Pro theme <= 1.1.7 versions.	7.1	More Details
CVE-2023-30493	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Themefic Ultimate Addons for Contact Form 7 plugin <= 3.2.0 versions.	7.1	More Details
CVE-2023-20253	A vulnerability in the command line interface (cli) management interface of Cisco SD-WAN vManage could allow an authenticated, local attacker to bypass authorization and allow the attacker to roll back the configuration on vManage controllers and edge router device. This vulnerability is due to improper access control in the cli-management interface of an affected system. An attacker with low-privilege (read only) access to the cli could exploit this vulnerability by sending a request to roll back the configuration on for other controller and devices managed by an affected system. A successful exploit could allow the attacker to to roll back the configuration on for other controller and devices managed by an affected system.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27616	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in David F. Carr RSVPMaker plugin <= 10.6.6 versions.	7.1	More Details
CVE-2023-40454	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Ventura 13.6, tvOS 17, iOS 16.7 and iPadOS 16.7, macOS Monterey 12.7, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to delete files for which it does not have permission.	7.1	More Details
CVE-2023-4264	Potential buffer overflow vulnerabilities n the Zephyr Bluetooth subsystem.	7.1	More Details
CVE-2023-41653	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Beplus Sermon'e – Sermons Online plugin <= 1.0.0 versions.	7.1	More Details
CVE-2023-40452	The issue was addressed with improved bounds checks. This issue is fixed in macOS Ventura 13.6, tvOS 17, macOS Monterey 12.7, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to overwrite arbitrary files.	7.1	More Details
CVE-2023-41692	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Hennessey Digital Attorney theme <= 3 theme.	7.1	More Details
CVE-2023-44474	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in MD Jakir Hosen Tiger Forms – Drag and Drop Form Builder plugin <= 2.0.0 versions.	7.1	More Details
CVE-2023-41663	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Giovambattista Fazioli WP Bannerize Pro plugin <= 1.6.9 versions.	7.1	More Details
CVE-2023-28490	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Estatik Estatik Mortgage Calculator plugin <= 2.0.7 versions.	7.1	More Details
CVE-2023-44244	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in FooPlugins FooGallery plugin <= 2.2.44 versions.	7.1	More Details
CVE-2023-41691	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Pensopay WooCommerce PensoPay plugin <= 6.3.1 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44144	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Dreamfox Payment gateway per Product for WooCommerce plugin <= 3.2.7 versions.	7.1	More Details
CVE-2023-44245	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Leap Contractor Contact Form Website to Workflow Tool plugin <= 4.0.0 versions.	7.1	More Details
CVE-2023-41861	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Restrict plugin <= 2.2.4 versions.	7.1	More Details
CVE-2023-41856	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in ClickToTweet.Com Click To Tweet plugin <= 2.0.14 versions.	7.1	More Details
CVE-2023-42820	JumpServer is an open source bastion host. This vulnerability is due to exposing the random number seed to the API, potentially allowing the randomly generated verification codes to be replayed, which could lead to password resets. If MFA is enabled users are not affect. Users not using local authentication are also not affected. Users are advised to upgrade to either version 2.28.19 or to 3.6.5. There are no known workarounds or this issue.	7.0	More Details
CVE-2023-5184	Two potential signed to unsigned conversion errors and buffer overflow vulnerabilities at the following locations in the Zephyr IPM drivers.	7.0	More Details
CVE-2023-41333	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. An attacker with the ability to create or modify CiliumNetworkPolicy objects in a particular namespace is able to affect traffic on an entire Cilium cluster, potentially bypassing policy enforcement in other namespaces. By using a crafted `endpointSelector` that uses the `DoesNotExist` operator on the `reserved:init` label, the attacker can create policies that bypass namespace restrictions and affect the entire Cilium cluster. This includes potentially allowing or denying all traffic. This attack requires API server access, as described in the Kubernetes API Server Attacker section of the Cilium Threat Model. This issue has been resolved in Cilium versions 1.14.2, 1.13.7, and 1.12.14. As a workaround an admission webhook can be used to prevent the use of `endpointSelectors` that use the `DoesNotExist` operator on the `reserved:init` label in CiliumNetworkPolicies.	6.9	More Details
CVE-2023-43125	BIG-IP APM clients may send IP traffic outside of the VPN tunnel. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40048	In WS_FTP Server version prior to 8.8.2, the WS_FTP Server Manager interface was missing cross-site request forgery (CSRF) protection on a POST transaction corresponding to a WS_FTP Server administrative function.	6.8	More Details
CVE-2023-23958	Symantec Protection Engine, prior to 9.1.0, may be susceptible to a Hash Leak vulnerability.	6.8	More Details
CVE-2023-32823	In rpmb , there is a possible memory corruption due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07912966; Issue ID: ALPS07912966.	6.7	More Details
CVE-2023-32824	In rpmb , there is a possible double free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07912966; Issue ID: ALPS07912961.	6.7	More Details
CVE-2023-32826	In camera middleware, there is a possible out of bounds write due to a missing input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07993539; Issue ID: ALPS07993544.	6.7	More Details
CVE-2023-32822	In ftm, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07994229; Issue ID: ALPS07994229.	6.7	More Details
CVE-2023-4886	A sensitive information exposure vulnerability was found in foreman. Contents of tomcat's server.xml file, which contain passwords to candlepin's keystore and truststore, were found to be world readable.	6.7	More Details
CVE-2023-34043	VMware Aria Operations contains a local privilege escalation vulnerability. A malicious actor with administrative access to the local system can escalate privileges to 'root'.	6.7	More Details
CVE-2023-22384	Memory Corruption in VR Service while sending data using Fast Message Queue (FMQ).	6.7	More Details
CVE-2023-32821	In video, there is a possible out of bounds write due to a permissions bypass. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08013430; Issue ID: ALPS08013433.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0828	Cross-site Scripting (XSS) vulnerability in Syslog Section of Pandora FMS allows attacker to cause that users cookie value will be transferred to the attackers users server. This issue affects Pandora FMS v767 version and prior versions on all platforms.	6.7	More Details
CVE-2023-24518	A Cross-site Request Forgery (CSRF) vulnerability in Pandora FMS allows an attacker to force authenticated users to send a request to a web application they are currently authenticated against. This issue affects Pandora FMS version 767 and earlier versions on all platforms.	6.7	More Details
CVE-2023-32828	In vpu, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767817; Issue ID: ALPS07767817.	6.7	More Details
CVE-2023-32827	In camera middleware, there is a possible out of bounds write due to a missing input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07993539; Issue ID: ALPS07993539.	6.7	More Details
CVE-2023-32830	In TVAPI, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: DTV03802522; Issue ID: DTV03802522.	6.7	More Details
CVE-2023-32829	In apusys, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07713478; Issue ID: ALPS07713478.	6.7	More Details
CVE-2023-28539	Memory corruption in WLAN Host when the firmware invokes multiple WMI Service Available command.	6.6	More Details
CVE-2023-20109	A vulnerability in the Cisco Group Encrypted Transport VPN (GET VPN) feature of Cisco IOS Software and Cisco IOS XE Software could allow an authenticated, remote attacker who has administrative control of either a group member or a key server to execute arbitrary code on an affected device or cause the device to crash. This vulnerability is due to insufficient validation of attributes in the Group Domain of Interpretation (GDOI) and G-IKEv2 protocols of the GET VPN feature. An attacker could exploit this vulnerability by either compromising an installed key server or modifying the configuration of a group member to point to a key server that is controlled by the attacker. A successful exploit could allow the attacker to execute arbitrary code and gain full control of the affected system or cause the affected system to reload, resulting in a denial of service (DoS) condition. For more information, see the Details ["#details"] section of this advisory.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40669	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in twinpictures, baden03 Collapse-O-Matic plugin <= 1.8.5.5 versions.	6.5	More Details
CVE-2023-4884	An attacker could send an HTTP request to an Open5GS endpoint and retrieve the information stored on the device due to the lack of Authentication.	6.5	More Details
CVE-2023-28372	A flaw exists in FlashBlade Purity (OE) Version 4.1.0 whereby a user with privileges to extend an object’s retention period can affect the availability of the object lock.	6.5	More Details
CVE-2023-41847	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WEN Solutions Notice Bar plugin <= 3.1.0 versions.	6.5	More Details
CVE-2023-26150	Versions of the package asyncua before 0.9.96 are vulnerable to Improper Authentication such that it is possible to access Address Space without encryption and authentication. **Note:** This issue is a result of missing checks for services that require an active session.	6.5	More Details
CVE-2023-3335	Insertion of Sensitive Information into Log File vulnerability in Hitachi Ops Center Administrator on Linux allows local users to gain sensitive information.This issue affects Hitachi Ops Center Administrator: before 10.9.3-00.	6.5	More Details
CVE-2023-38873	The commit 3730880 (April 2023) and v.0.9-beta1 of gugoan Economizzer is vulnerable to Clickjacking. Clickjacking, also known as a "UI redress attack", is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.	6.5	More Details
CVE-2023-39376	SiberianCMS - CWE-284 Improper Access Control Authorized user may disable a security feature over the network	6.5	More Details
CVE-2023-4929	All firmware versions of the NPort 5000 Series are affected by an improper validation of integrity check vulnerability. This vulnerability results from insufficient checks on firmware updates or upgrades, potentially allowing malicious users to manipulate the firmware and gain control of devices.	6.5	More Details
CVE-2023-43323	mooSocial 3.1.8 is vulnerable to external service interaction on post function. When executed, the server sends a HTTP and DNS request to external server. The Parameters effected are multiple - messageText, data[wall_photo], data[userShareVideo] and data[userShareLink].	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44145	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in jesweb.Dev Anchor Episodes Index (Spotify for Podcasters) plugin <= 2.1.7 versions.	6.5	More Details
CVE-2023-40420	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.6, tvOS 17, iOS 16.7 and iPadOS 16.7, macOS Monterey 12.7, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. Processing web content may lead to a denial-of-service.	6.5	More Details
CVE-2023-44477	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Boxy Studio Cooked plugin <= 1.7.13 versions.	6.5	More Details
CVE-2023-42461	GLPI stands for Gestionnaire Libre de Parc Informatique is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. The ITIL actors input field from the Ticket form can be used to perform a SQL injection. Users are advised to upgrade to version 10.0.10. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2023-40605	Auth. (contributor) Cross-Site Scripting (XSS) vulnerability in 93digital Typing Effect plugin <= 1.3.6 versions.	6.5	More Details
CVE-2023-40441	A resource exhaustion issue was addressed with improved input validation. This issue is fixed in iOS 17 and iPadOS 17, macOS Sonoma 14. Processing web content may lead to a denial-of-service.	6.5	More Details
CVE-2023-4885	Man in the Middle vulnerability, which could allow an attacker to intercept VNF (Virtual Network Function) communications resulting in the exposure of sensitive information.	6.5	More Details
CVE-2023-32572	A flaw exists in FlashArray Purity wherein under limited circumstances, an array administrator can alter the retention lock of a pgroup and disable pgroup SafeMode protection.	6.5	More Details
CVE-2023-40403	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.6, tvOS 17, iOS 16.7 and iPadOS 16.7, macOS Monterey 12.7, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. Processing web content may disclose sensitive information.	6.5	More Details
CVE-2023-39233	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. Processing web content may disclose sensitive information.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5171	During Ion compilation, a Garbage Collection could have resulted in a use-after-free condition, allowing an attacker to write two NUL bytes, and cause a potentially exploitable crash. This vulnerability affects Firefox < 118, Firefox ESR < 115.3, and Thunderbird < 115.3.	6.5	More Details
CVE-2023-44264	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Arrow Plugins The Awesome Feed – Custom Feed plugin <= 2.2.5 versions.	6.5	More Details
CVE-2023-4100	Allows an attacker to perform XSS attacks stored on certain resources. Exploiting this vulnerability can lead to a DoS condition, among other actions.	6.5	More Details
CVE-2023-41687	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Irina Sokolovskaya Goods Catalog plugin <= 2.4.1 versions.	6.5	More Details
CVE-2023-32791	Cross-Site Request Forgery (CSRF) vulnerability in NXLog Manager 5.6.5633 version. This vulnerability allows an attacker to manipulate and delete user accounts within the platform by sending a specifically crafted query to the server. The vulnerability is based on the lack of proper validation of the origin of incoming requests.	6.5	More Details
CVE-2023-41666	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Stockdio Stock Quotes List plugin <= 2.9.9 versions.	6.5	More Details
CVE-2023-32792	Cross-Site Request Forgery (CSRF) vulnerability in NXLog Manager 5.6.5633 version. This vulnerability allows an attacker to eliminate roles within the platform by sending a specifically crafted query to the server. The vulnerability is based on the absence of proper validation of the origin of incoming requests.	6.5	More Details
CVE-2023-44160	Sensitive information manipulation due to cross-site request forgery. The following products are affected: Acronis Cyber Protect 15 (Linux, Windows) before build 35979.	6.5	More Details
CVE-2023-44161	Sensitive information manipulation due to cross-site request forgery. The following products are affected: Acronis Cyber Protect 15 (Linux, Windows) before build 35979.	6.5	More Details
CVE-2023-43836	There is a SQL injection vulnerability in the Jizhicms 2.4.9 backend, which users can use to obtain database information	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40201	Cross-Site Request Forgery (CSRF) vulnerability in FuturioWP Futurio Extra plugin <= 1.8.4 versions leads to activation of arbitrary plugin.	6.5	More Details
CVE-2023-42508	JFrog Artifactory prior to version 7.66.0 is vulnerable to specific endpoint abuse with a specially crafted payload, which can lead to unauthenticated users being able to send emails with manipulated email body.	6.5	More Details
CVE-2023-5353	Improper Access Control in GitHub repository salesagility/suitecrm prior to 7.14.1.	6.5	More Details
CVE-2023-5169	A compromised content process could have provided malicious data in a `PathRecording` resulting in an out-of-bounds write, leading to a potentially exploitable crash in a privileged process. This vulnerability affects Firefox < 118, Firefox ESR < 115.3, and Thunderbird < 115.3.	6.5	More Details
CVE-2023-41728	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rescue Themes Rescue Shortcodes allows Stored XSS.This issue affects Rescue Shortcodes: from n/a through 2.5.	6.5	More Details
CVE-2023-5192	Excessive Data Query Operations in a Large Data Table in GitHub repository pimcore/demo prior to 10.3.0.	6.5	More Details
CVE-2023-5195	Mattermost fails to properly validate the permissions when soft deleting a team allowing a team member to soft delete other teams that they are not part of	6.5	More Details
CVE-2023-41797	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Gold Plugins Locations plugin <= 4.0 versions.	6.5	More Details
CVE-2023-27628	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Webvitaly Sitekit plugin <= 1.3 versions.	6.5	More Details
CVE-2023-44242	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in 2J Slideshow Team Slideshow, Image Slider by 2J plugin <= 1.3.54 versions.	6.5	More Details
CVE-2023-3413	An issue has been discovered in GitLab affecting all versions starting from 16.2 before 16.2.8, all versions starting from 16.3 before 16.3.5, all versions starting from 16.4 before 16.4.1. It was possible to read the source code of a project through a fork created before changing visibility to only project members.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30961	Palantir Gotham was found to be vulnerable to a bug where under certain circumstances, the frontend could have applied an incorrect classification to a newly created property or link.	6.5	More Details
CVE-2023-5196	Mattermost fails to enforce character limits in all possible notification props allowing an attacker to send a really long value for a notification_prop resulting in the server consuming an abnormal quantity of computing resources and possibly becoming temporarily unavailable for its users.	6.5	More Details
CVE-2023-5233	The Font Awesome Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'fawesome' shortcode in versions up to, and including, 5.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5230	The TM WooCommerce Compare & Wishlist plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'tm_woo_wishlist_table' shortcode in versions up to, and including, 1.1.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5161	The Modal Window plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 5.3.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-44174	Online Movie Ticket Booking System v1.0 is vulnerable to an authenticated Stored Cross-Site Scripting vulnerability.	6.4	More Details
CVE-2023-5135	The Simple Cloudflare Turnstile plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'gravity-simple-turnstile' shortcode in versions up to, and including, 1.23.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5232	The Font Awesome More Icons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'icon' shortcode in versions up to, and including, 3.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-43655	Composer is a dependency manager for PHP. Users publishing a composer.phar to a public web-accessible server where the composer.phar can be executed as a php file may be subject to a remote code execution vulnerability if PHP also has `register_argc_argv` enabled in php.ini. Versions 2.6.4, 2.2.22 and 1.10.27 patch this vulnerability. Users are advised to upgrade. Users unable to upgrade should make sure `register_argc_argv` is disabled in php.ini, and avoid publishing composer.phar to the web as this is not best practice.	6.4	More Details
CVE-2023-5334	The WP Responsive header image slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'sp_responsiveslider' shortcode in versions up to, and including, 3.2.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5295	The Blog Filter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'vivafbcomment' shortcode in versions up to, and including, 1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5162	The Options for Twenty Seventeen plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'social-links' shortcode in versions up to, and including, 2.5.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5278	A vulnerability, which was classified as critical, was found in SourceCodester Engineers Online Portal 1.0. Affected is an unknown function of the file login.php. The manipulation of the argument username/password leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-240906 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5266	A vulnerability, which was classified as critical, was found in DedeBIZ 6.2. This affects an unknown part of the file /src/admin/tags_main.php. The manipulation of the argument ids leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-240879.	6.3	More Details
CVE-2023-5279	A vulnerability has been found in SourceCodester Engineers Online Portal 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file my_classmates.php. The manipulation of the argument teacher_class_student_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-240907.	6.3	More Details
CVE-2023-5280	A vulnerability was found in SourceCodester Engineers Online Portal 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file my_students.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-240908.	6.3	More Details
CVE-2023-5281	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been classified as critical. This affects an unknown part of the file remove_inbox_message.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-240909 was assigned to this vulnerability.	6.3	More Details
CVE-2023-5268	A vulnerability was found in DedeBIZ 6.2 and classified as critical. This issue affects some unknown processing of the file /src/admin/makehtml_taglist_action.php. The manipulation of the argument mktime leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-240881 was assigned to this vulnerability.	6.3	More Details
CVE-2023-5282	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been declared as critical. This vulnerability affects unknown code of the file seed_message_student.php. The manipulation of the argument teacher_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-240910 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-5260	A vulnerability, which was classified as critical, has been found in SourceCodester Simple Membership System 1.0. This issue affects some unknown processing of the file group_validator.php. The manipulation of the argument club_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-240869 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5262	A vulnerability has been found in OpenRapid RapidCMS 1.3.1 and classified as critical. Affected by this vulnerability is the function isImg of the file /admin/config/uploadicon.php. The manipulation of the argument fileName leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-240871.	6.3	More Details
CVE-2023-5264	A vulnerability classified as critical was found in huakecms 3.0. Affected by this vulnerability is an unknown functionality of the file /admin/cms_content.php. The manipulation of the argument cid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-240877 was assigned to this vulnerability.	6.3	More Details
CVE-2023-5283	A vulnerability was found in SourceCodester Engineers Online Portal 1.0. It has been rated as critical. This issue affects some unknown processing of the file teacher_signup.php. The manipulation of the argument firstname/lastname leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-240911.	6.3	More Details
CVE-2023-5263	A vulnerability was found in ZZZCMS 2.1.7 and classified as critical. Affected by this issue is the function restore of the file /admin/save.php of the component Database Backup File Handler. The manipulation leads to permission issues. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-240872.	6.3	More Details
CVE-2023-5284	A vulnerability classified as critical has been found in SourceCodester Engineers Online Portal 1.0. Affected is an unknown function of the file upload_save_student.php. The manipulation of the argument uploaded_file leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-240912.	6.3	More Details
CVE-2023-5258	A vulnerability classified as critical has been found in OpenRapid RapidCMS 1.3.1. This affects an unknown part of the file /resource/addgood.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-240867.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5285	A vulnerability classified as critical was found in Tongda OA 2017. Affected by this vulnerability is an unknown functionality of the file general/hr/recruit/recruitment/delete.php. The manipulation of the argument RECRUITMENT_ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-240913 was assigned to this vulnerability.	6.3	More Details
CVE-2023-43663	PrestaShop is an Open Source e-commerce web application. In affected versions any module can be disabled or uninstalled from back office, even with low user right. This allows low privileged users to disable portions of a shops functionality. Commit `ce1f6708` addresses this issue and is included in version 8.1.2. Users are advised to upgrade. There are no known workarounds for this issue.	6.3	More Details
CVE-2015-10124	A vulnerability was found in Most Popular Posts Widget Plugin up to 0.8 on WordPress. It has been classified as critical. Affected is the function add_views/show_views of the file functions.php. The manipulation leads to sql injection. It is possible to launch the attack remotely. Upgrading to version 0.9 is able to address this issue. The patch is identified as a99667d11ac8d320006909387b100e9a8b5c12e1. It is recommended to upgrade the affected component. VDB-241026 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-42486	Fortect - CWE-428: Unquoted Search Path or Element, may be used by local user to elevate privileges.	6.3	More Details
CVE-2023-5276	A vulnerability classified as critical was found in SourceCodester Engineers Online Portal 1.0. This vulnerability affects unknown code of the file downloadable_student.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The identifier of this vulnerability is VDB-240904.	6.3	More Details
CVE-2023-32671	A stored XSS vulnerability has been found on BuddyBoss Platform affecting version 2.2.9. This vulnerability allows an attacker to store a malicious javascript payload via POST request when sending an invitation.	6.3	More Details
CVE-2023-5277	A vulnerability, which was classified as critical, has been found in SourceCodester Engineers Online Portal 1.0. This issue affects some unknown processing of the file student_avatar.php. The manipulation of the argument change leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-240905 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4260	Potential off-by-one buffer overflow vulnerability in the Zephyr fuse file system.	6.3	More Details
CVE-2023-5300	A vulnerability classified as critical has been found in TTSPlanning up to 20230925. This affects an unknown part. The manipulation of the argument uid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-240939.	6.3	More Details
CVE-2023-27435	Cross-Site Request Forgery (CSRF) vulnerability in Sami Ahmed Siddiqui HTTP Auth plugin <= 0.3.2 versions.	6.3	More Details
CVE-2023-5223	A vulnerability, which was classified as critical, has been found in HimitZH HOJ up to 4.6-9a65e3f. This issue affects some unknown processing of the component Topic Handler. The manipulation leads to sandbox issue. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-240365 was assigned to this vulnerability.	6.3	More Details
CVE-2023-5328	A vulnerability classified as critical has been found in SATO CL4NX-J Plus 1.13.2-u455_r2. This affects an unknown part of the component Cookie Handler. The manipulation with the input auth=user,level1,settings; web=true leads to improper authentication. Access to the local network is required for this attack. The exploit has been disclosed to the public and may be used. The identifier VDB-241029 was assigned to this vulnerability.	6.3	More Details
CVE-2023-5326	A vulnerability was found in SATO CL4NX-J Plus 1.13.2-u455_r2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component WebConfig. The manipulation leads to improper authentication. The attack needs to be done within the local network. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-241027.	6.3	More Details
CVE-2023-5222	A vulnerability classified as critical was found in Viessmann Vitogate 300 up to 2.1.3.0. This vulnerability affects the function isValidUser of the file /cgi-bin/vitogate.cgi of the component Web Management Interface. The manipulation leads to use of hard-coded password. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-240364. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-40307	An attacker with standard privileges on macOS when requesting administrator privileges from the application can submit input which causes a buffer overflow resulting in a crash of the application. This could make the application unavailable and allow reading or modification of data.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26149	Versions of the package quill-mention before 4.0.0 are vulnerable to Cross-site Scripting (XSS) due to improper user-input sanitization, via the renderList function. **Note:** If the mentions list is sourced from unsafe (user-sourced) data, this might allow an injection attack when a Quill user hits @.	6.1	More Details
CVE-2023-40519	A cross-site scripting (XSS) vulnerability in the bpk-common/auth/login/index.html login portal in Broadpeak Centralized Accounts Management Auth Agent 01.01.00.19219575_ee9195b0, 01.01.01.30097902_fd999e76, and 00.12.01.9565588_1254b459 allows remote attackers to inject arbitrary web script or HTML via the disconnectMessage parameter.	6.1	More Details
CVE-2023-28571	Information disclosure in WLAN HOST while processing the WLAN scan descriptor list during roaming scan.	6.1	More Details
CVE-2023-5323	Cross-site Scripting (XSS) - Generic in GitHub repository dolibarr/dolibarr prior to 18.0.	6.1	More Details
CVE-2023-43484	Cross-site scripting vulnerability in Item List page of Welcart e-Commerce versions 2.7 to 2.8.21 allows a remote unauthenticated attacker to inject an arbitrary script.	6.1	More Details
CVE-2023-44123	The vulnerability is the use of implicit PendingIntents with the PendingIntent.FLAG_MUTABLE set that leads to theft and/or (over-)write of arbitrary files with system privilege in the Bluetooth ("com.lge.bluetoothsetting") app. The attacker's app, if it had access to app notifications, could intercept them and redirect them to its activity, before making it grant access permissions to content providers with the `android:grantUriPermissions="true"` flag.	6.1	More Details
CVE-2023-44012	Cross Site Scripting vulnerability in mojoPortal v.2.7.0.0 allows a remote attacker to execute arbitrary code via the helpkey parameter in the Help.aspx component.	6.1	More Details
CVE-2023-5316	Cross-site Scripting (XSS) - DOM in GitHub repository thorsten/phpmyfaq prior to 3.1.18.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44124	The vulnerability is to theft of arbitrary files with system privilege in the Screen recording ("com.lge.gametools.gamerecorder") app in the "com/lge/gametools/gamerecorder/settings/ProfilePreferenceFragment.java" file. The main problem is that the app launches implicit intents that can be intercepted by third-party apps installed on the same device. They also can return arbitrary data that will be passed to the "onActivityResult()" method. The Screen recording app saves contents of arbitrary URIs to SD card which is a world-readable storage.	6.1	More Details
CVE-2023-26146	All versions of the package ithewei/libhv are vulnerable to Cross-site Scripting (XSS) such that when a file with a name containing a malicious payload is served by the application, the filename is displayed without proper sanitization when it is rendered.	6.1	More Details
CVE-2023-44125	The vulnerability is the use of implicit PendingIntents without the PendingIntent.FLAG_IMMUTABLE set that leads to theft and/or (over-)write of arbitrary files with system privilege in the Personalized service ("com.lge.abba") app. The attacker's app, if it had access to app notifications, could intercept them and redirect them to its activity, before making it grant access permissions to content providers with the `android:grantUriPermissions="true"` flag.	6.1	More Details
CVE-2023-20251	A vulnerability in the memory buffer of Cisco Wireless LAN Controller (WLC) AireOS Software could allow an unauthenticated, adjacent attacker to cause memory leaks that could eventually lead to a device reboot. This vulnerability is due to memory leaks caused by multiple clients connecting under specific conditions. An attacker could exploit this vulnerability by causing multiple wireless clients to attempt to connect to an access point (AP) on an affected device. A successful exploit could allow the attacker to cause the affected device to reboot after a significant amount of time, resulting in a denial of service (DoS) condition.	6.1	More Details
CVE-2023-5320	Cross-site Scripting (XSS) - DOM in GitHub repository thorsten/phpmyfaq prior to 3.1.18.	6.1	More Details
CVE-2023-41233	Cross-site scripting vulnerability in Item List page registration process of Welcart e-Commerce versions 2.7 to 2.8.21 allows a remote unauthenticated attacker to inject an arbitrary script.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20202	A vulnerability in the Wireless Network Control daemon (wncd) of Cisco IOS XE Software for Wireless LAN Controllers could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper memory management. An attacker could exploit this vulnerability by sending a series of network requests to an affected device. A successful exploit could allow the attacker to cause the wncd process to consume available memory and eventually cause the device to reload, resulting in a DoS condition.	6.1	More Details
CVE-2023-44043	A reflected cross-site scripting (XSS) vulnerability in /install/index.php of Black Cat CMS 1.4.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Website title parameter.	6.1	More Details
CVE-2023-44122	The vulnerability is to theft of arbitrary files with system privilege in the LockScreenSettings ("com.lge.lockscreensettings") app in the "com/lge/lockscreensettings/dynamicwallpaper/MyCategoryGuideActivity.java" file. The main problem is that the app launches implicit intents that can be intercepted by third-party apps installed on the same device. They also can return arbitrary data that will be passed to the "onActivityResult()" method. The LockScreenSettings app copies the received file to the "/data/shared/dw/mycategory/wallpaper_01.png" path and then changes the file access mode to world-readable and world-writable.	6.1	More Details
CVE-2023-43263	A Cross-site scripting (XSS) vulnerability in Froala Editor v.4.1.1 allows attackers to execute arbitrary code via the Markdown component.	6.1	More Details
CVE-2023-43614	Cross-site scripting vulnerability in Order Data Edit page of Welcart e-Commerce versions 2.7 to 2.8.21 allows a remote unauthenticated attacker to inject an arbitrary script.	6.1	More Details
CVE-2023-41447	Cross Site Scripting vulnerability in phpkobo AjaxNewTicker v.1.0.5 allows a remote attacker to execute arbitrary code via a crafted payload to the subcmd parameter in the index.php component.	6.1	More Details
CVE-2023-41446	Cross Site Scripting vulnerability in phpkobo AjaxNewTicker v.1.0.5 allows a remote attacker to execute arbitrary code via a crafted script to the title parameter in the index.php component.	6.1	More Details
CVE-2023-41962	Cross-site scripting vulnerability in Credit Card Payment Setup page of Welcart e-Commerce versions 2.7 to 2.8.21 allows a remote unauthenticated attacker to inject an arbitrary script in the page.	6.1	More Details
CVE-2023-43233	A stored cross-site scripting (XSS) vulnerability in the cms/content/edit component of YZNCMS v1.3.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the title parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5244	Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 2.0.	6.1	More Details
CVE-2023-41453	Cross Site Scripting vulnerability in phpkobo AjaxNewTicker v.1.0.5 allows a remote attacker to execute arbitrary code via a crafted payload to the cmd parameter in the index.php component.	6.1	More Details
CVE-2023-41448	Cross Site Scripting vulnerability in phpkobo AjaxNewTicker v.1.0.5 allows a remote attacker to execute arbitrary code via a crafted payload to the ID parameter in the index.php component.	6.1	More Details
CVE-2023-41445	Cross Site Scripting vulnerability in phpkobo AjaxNewTicker v.1.0.5 allows a remote attacker to execute arbitrary code via a crafted payload to the index.php component.	6.1	More Details
CVE-2023-41451	Cross Site Scripting vulnerability in phpkobo AjaxNewTicker v.1.0.5 allows a remote attacker to execute arbitrary code via a crafted payload to the txt parameter in the index.php component.	6.1	More Details
CVE-2023-25483	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Ankit Agarwal, Priyanshu Mittal Easy Coming Soon plugin <= 2.3 versions.	5.9	More Details
CVE-2023-44266	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Jewel Theme WP Adminify plugin <= 3.1.6 versions.	5.9	More Details
CVE-2023-41733	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in YYDevelopment Back To The Top Button plugin <= 2.1.5 versions.	5.9	More Details
CVE-2023-41731	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in I Thirteen Web Solution WordPress publish post email notification plugin <= 1.0.2.2 versions.	5.9	More Details
CVE-2023-44265	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Popup contact form plugin <= 7.1 versions.	5.9	More Details
CVE-2023-28790	Auth. (editor+) Stored Cross-Site Scripting (XSS) vulnerability in Brett Shumaker Simple Staff List plugin <= 2.2.3 versions.	5.9	More Details
CVE-2023-41655	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Andreas Heigl authLdap plugin <= 2.5.9 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43645	OpenFGA is an authorization/permission engine built for developers and inspired by Google Zanzibar. OpenFGA is vulnerable to a denial of service attack when certain Check calls are executed against authorization models that contain circular relationship definitions. When the call is made, it's possible for the server to exhaust resources and die. Users are advised to upgrade to v1.3.2 and update any offending models. There are no known workarounds for this vulnerability. Note that for models which contained cycles or a relation definition that has the relation itself in its evaluation path, checks and queries that require evaluation will no longer be evaluated on v1.3.2+ and will return errors instead. Users who do not have cyclic models are unaffected.	5.9	More Details
CVE-2023-41657	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Groundhogg Inc. HollerBox plugin <= 2.3.2 versions.	5.9	More Details
CVE-2023-41661	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in PressPage Entertainment Inc. Smarty for WordPress plugin <= 3.1.35 versions.	5.9	More Details
CVE-2023-41729	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in SendPress Newsletters plugin <= 1.22.3.31 versions.	5.9	More Details
CVE-2023-3024	Forcing the Bluetooth LE stack to segment 'prepare write response' packets can lead to an out-of-bounds memory access.	5.9	More Details
CVE-2023-44239	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Jobin Jose WWM Social Share On Image Hover plugin <= 2.2 versions.	5.9	More Details
CVE-2023-40604	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Jes Madsen Cookies by JM plugin <= 1.0 versions.	5.9	More Details
CVE-2023-41242	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Hassan Ali Snap Pixel plugin <= 1.5.7 versions.	5.9	More Details
CVE-2023-27622	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Abel Ruiz GuruWalk Affiliates plugin <= 1.0.0 versions.	5.9	More Details
CVE-2023-44479	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Jim Krill WP Jump Menu plugin <= 3.6.4 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41859	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Ashok Rane Order Delivery Date for WP e-Commerce plugin <= 1.2 versions.	5.9	More Details
CVE-2023-41855	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Regpacks Regpack plugin <= 0.1 versions.	5.9	More Details
CVE-2023-41800	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in UniConsent UniConsent CMP for GDPR CPRA GPP TCF plugin <= 1.4.2 versions.	5.9	More Details
CVE-2023-44262	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Renzo Johnson Blocks plugin <= 1.6.41 versions.	5.9	More Details
CVE-2023-40665	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Pdfcrowd Save as Image plugin by Pdfcrowd plugin <= 2.16.0 versions.	5.9	More Details
CVE-2023-40668	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Pdfcrowd Save as PDF plugin by Pdfcrowd plugin <= 2.16.0 versions.	5.9	More Details
CVE-2023-40675	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in PluginOps Landing Page Builder plugin <= 1.5.1.2 versions.	5.9	More Details
CVE-2023-40676	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Jason Crouse, VeronaLabs Slimstat Analytics plugin <= 5.0.8 versions.	5.9	More Details
CVE-2023-40677	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Vertical marquee plugin <= 7.1 versions.	5.9	More Details
CVE-2023-4129	Dell Data Protection Central, version 19.9, contains an Inadequate Encryption Strength Vulnerability. An unauthenticated network attacker could potentially exploit this vulnerability, allowing an attacker to recover plaintext from a block of ciphertext.	5.9	More Details
CVE-2023-44263	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Riyaz Social Metrics plugin <= 2.2 versions.	5.9	More Details
CVE-2023-41737	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPGens Swifty Bar, sticky bar by WPGens plugin <= 1.2.10 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27617	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in David F. Carr RSVPMaker plugin <= 10.6.6 versions.	5.9	More Details
CVE-2023-41241	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in SureCart WordPress Ecommerce For Creating Fast Online Stores plugin <= 2.5.0 versions.	5.9	More Details
CVE-2023-41734	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in nigauri Insert Estimated Reading Time plugin <= 1.2 versions.	5.9	More Details
CVE-2023-44228	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Onclick show popup plugin <= 8.1 versions.	5.9	More Details
CVE-2023-44230	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Popup contact form plugin <= 7.1 versions.	5.9	More Details
CVE-2023-41736	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gopi Ramasamy Email posts to subscribers plugin <= 6.2 versions.	5.9	More Details
CVE-2023-20176	A vulnerability in the networking component of Cisco access point (AP) software could allow an unauthenticated, remote attacker to cause a temporary disruption of service. This vulnerability is due to overuse of AP resources. An attacker could exploit this vulnerability by connecting to an AP on an affected device as a wireless client and sending a high rate of traffic over an extended period of time. A successful exploit could allow the attacker to cause the Datagram TLS (DTLS) session to tear down and reset, causing a denial of service (DoS) condition.	5.8	More Details
CVE-2023-0809	In Mosquitto before 2.0.16, excessive memory is allocated based on malicious initial packets that are not CONNECT packets.	5.8	More Details
CVE-2023-3592	In Mosquitto before 2.0.16, a memory leak occurs when clients send v5 CONNECT packets with a will message that contains invalid property types.	5.8	More Details
CVE-2023-41860	Unauth. Cross-Site Scripting (XSS) vulnerability in TravelMap plugin <= 1.0.1 versions.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43627	Path traversal vulnerability in ACERA 1320 firmware ver.01.26 and earlier, and ACERA 1310 firmware ver.01.26 and earlier allows a network-adjacent authenticated attacker to alter critical information such as system files by sending a specially crafted request. They are affected when running in ST(Standalone) mode.	5.7	More Details
CVE-2023-43656	matrix-hookshot is a Matrix bot for connecting to external services like GitHub, GitLab, JIRA, and more. Instances that have enabled transformation functions (those that have `generic.allowJsTransformationFunctions` in their config), may be vulnerable to an attack where it is possible to break out of the `vm2` sandbox and as a result Hookshot will be vulnerable to this. This problem is only likely to affect users who have allowed untrusted users to apply their own transformation functions. If you have only enabled a limited set of trusted users, this threat is reduced (though not eliminated). Version 4.5.0 and above of hookshot include a new sandbox library which should better protect users. Users are advised to upgrade. Users unable to upgrade should disable `generic.allowJsTransformationFunctions` in the config.	5.6	More Details
CVE-2023-5298	A vulnerability was found in Tongda OA 2017. It has been rated as critical. Affected by this issue is some unknown functionality of the file general/hr/recruit/requirements/delete.php. The manipulation of the argument REQUIREMENTS_ID leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. VDB-240938 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-23495	A permissions issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sonoma 14. An app may be able to access sensitive user data.	5.5	More Details
CVE-2023-42132	FD Application Apr. 2022 Edition (Version 9.01) and earlier improperly restricts XML external entity references (XXE). By processing a specially crafted XML file, arbitrary files on the system may be read by an attacker.	5.5	More Details
CVE-2023-4211	A local non-privileged user can make improper GPU memory processing operations to gain access to already freed memory.	5.5	More Details
CVE-2023-5321	Missing Authorization in GitHub repository hamza417/inure prior to build94.	5.5	More Details
CVE-2023-40402	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14. An app may be able to access sensitive user data.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5272	A vulnerability classified as critical has been found in SourceCodester Best Courier Management System 1.0. This affects an unknown part of the file edit_parcel.php of the component GET Parameter Handler. The manipulation of the argument id leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-240885 was assigned to this vulnerability.	5.5	More Details
CVE-2023-41070	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.6, iOS 16.7 and iPadOS 16.7, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to access sensitive data logged when a user shares a link.	5.5	More Details
CVE-2023-40428	The issue was addressed with improved handling of caches. This issue is fixed in iOS 17 and iPadOS 17. An app may be able to access sensitive user data.	5.5	More Details
CVE-2023-40429	A permissions issue was addressed with improved validation. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10, macOS Sonoma 14. An app may be able to access sensitive user data.	5.5	More Details
CVE-2023-40435	This issue was addressed by enabling hardened runtime. This issue is fixed in Xcode 15. An app may be able to access App Store credentials.	5.5	More Details
CVE-2023-40450	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may bypass Gatekeeper checks.	5.5	More Details
CVE-2023-40541	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in macOS Sonoma 14. A shortcut may output sensitive user data without consent.	5.5	More Details
CVE-2023-4066	A flaw was found in Red Hat's AMQ Broker, which stores certain passwords in a secret security-properties-prop-module, defined in ActivemqArtemisSecurity CR; however, they are shown in plaintext in the StatefulSet details yaml of AMQ Broker.	5.5	More Details
CVE-2023-5271	A vulnerability was found in SourceCodester Best Courier Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file edit_parcel.php. The manipulation of the argument email leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-240884.	5.5	More Details
CVE-2023-41067	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. An app may bypass Gatekeeper checks.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41073	An authorization issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.6, tvOS 17, iOS 16.7 and iPadOS 16.7, macOS Monterey 12.7, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to access protected user data.	5.5	More Details
CVE-2023-40424	The issue was addressed with improved checks. This issue is fixed in iOS 17 and iPadOS 17, watchOS 10, macOS Sonoma 14. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2023-41078	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14. An app may be able to bypass certain Privacy preferences.	5.5	More Details
CVE-2023-41079	The issue was addressed with improved permissions logic. This issue is fixed in macOS Sonoma 14. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2023-41232	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Monterey 12.7, iOS 17 and iPadOS 17, macOS Ventura 13.6, iOS 16.7 and iPadOS 16.7. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2023-4065	A flaw was found in Red Hat AMQ Broker Operator, where it displayed a password defined in ActiveMQArtemisAddress CR, shown in plain text in the Operator Log. This flaw allows an authenticated local attacker to access information outside of their permissions.	5.5	More Details
CVE-2023-41968	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Ventura 13.6, tvOS 17, macOS Monterey 12.7, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to read arbitrary files.	5.5	More Details
CVE-2023-41980	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2023-41986	The issue was addressed with improved checks. This issue is fixed in iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2023-41996	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.6. Apps that fail verification checks may still launch.	5.5	More Details
CVE-2023-40426	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14. An app may be able to bypass certain Privacy preferences.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41066	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14. An app may be able to unexpectedly leak a user's credentials from secure text fields.	5.5	More Details
CVE-2023-40422	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14. An app may be able to cause a denial-of-service.	5.5	More Details
CVE-2023-38596	The issue was addressed with improved handling of protocols. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10, macOS Sonoma 14. An app may fail to enforce App Transport Security.	5.5	More Details
CVE-2023-40418	An authentication issue was addressed with improved state management. This issue is fixed in watchOS 10. An Apple Watch Ultra may not lock when using the Depth app.	5.5	More Details
CVE-2023-5265	A vulnerability, which was classified as critical, has been found in Tongda OA 2017. Affected by this issue is some unknown functionality of the file general/hr/manage/staff_transfer/delete.php. The manipulation of the argument TRANSFER_ID leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. VDB-240878 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-5267	A vulnerability has been found in Tongda OA 2017 and classified as critical. This vulnerability affects unknown code of the file general/hr/recruit/hr_pool/delete.php. The manipulation of the argument EXPERT_ID leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-240880.	5.5	More Details
CVE-2023-5261	A vulnerability, which was classified as critical, was found in Tongda OA 2017. Affected is an unknown function of the file general/hr/manage/staff_title_evaluation/delete.php. The manipulation of the argument EVALUATION_ID leads to sql injection. The exploit has been disclosed to the public and may be used. Upgrading to version 11.10 is able to address this issue. It is recommended to upgrade the affected component. VDB-240870 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-43898	Nothings stb 2.28 was discovered to contain a Null Pointer Dereference via the function stbi__convert_format. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted pic file.	5.5	More Details
CVE-2023-37605	Weak Exception Handling vulnerability in baramundi software GmbH EMM Agent 23.1.50 and before allows an attacker to cause a denial of service via a crafted request to the password parameter.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32421	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14. An app may be able to observe unprotected user data.	5.5	More Details
CVE-2023-5269	A vulnerability was found in SourceCodester Best Courier Management System 1.0. It has been classified as critical. Affected is an unknown function of the file parcel_list.php of the component GET Parameter Handler. The manipulation of the argument s leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-240882 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-32361	The issue was addressed with improved handling of caches. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10, macOS Sonoma 14. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2023-5270	A vulnerability was found in SourceCodester Best Courier Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file view_parcel.php. The manipulation of the argument id leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-240883.	5.5	More Details
CVE-2023-40391	The issue was addressed with improved memory handling. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, macOS Sonoma 14, Xcode 15. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2023-40406	The issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.7, macOS Ventura 13.6, macOS Sonoma 14. An app may be able to read arbitrary files.	5.5	More Details
CVE-2023-40399	The issue was addressed with improved memory handling. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10, macOS Sonoma 14. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2023-40410	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.6, tvOS 17, macOS Monterey 12.7, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to disclose kernel memory.	5.5	More Details
CVE-2023-25463	Cross-Site Request Forgery (CSRF) vulnerability in Gopi Ramasamy WP tell a friend popup form plugin <= 7.1 versions.	5.4	More Details
CVE-2023-5112	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "specials_type_name[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43952	SSCMS 7.2.2 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Material Management component.	5.4	More Details
CVE-2023-5351	Cross-site Scripting (XSS) - Stored in GitHub repository salesagility/suitecrm prior to 7.14.1.	5.4	More Details
CVE-2023-32669	Authorization bypass vulnerability in BuddyBoss 2.2.9 version, the exploitation of which could allow an authenticated user to access and rename other users' albums. This vulnerability can be exploited by changing the album identification (id).	5.4	More Details
CVE-2023-40210	Cross-Site Request Forgery (CSRF) vulnerability in Sean Barton (Tortoise IT) SB Child List plugin <= 4.5 versions.	5.4	More Details
CVE-2023-5111	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "featured_type_name[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-39989	Cross-Site Request Forgery (CSRF) vulnerability in 99robots Header Footer Code Manager plugin <= 1.1.34 versions.	5.4	More Details
CVE-2023-39923	Cross-Site Request Forgery (CSRF) vulnerability in RadiusTheme The Post Grid plugin <= 7.2.7 versions.	5.4	More Details
CVE-2023-39165	Cross-Site Request Forgery (CSRF) vulnerability in Fetch Designs Sign-up Sheets plugin <= 2.2.8 versions.	5.4	More Details
CVE-2023-2830	Cross-Site Request Forgery (CSRF) vulnerability in Trustindex.Io WP Testimonials plugin <= 1.4.2 versions.	5.4	More Details
CVE-2023-38396	Cross-Site Request Forgery (CSRF) vulnerability in Alain Gonzalez plugin <= 3.1.2 versions.	5.4	More Details
CVE-2023-38381	Cross-Site Request Forgery (CSRF) vulnerability in Cyle Conoly WP-FlyBox plugin <= 6.46 versions.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40009	Cross-Site Request Forgery (CSRF) vulnerability in ThimPress WP Pipes plugin <= 1.4.0 versions.	5.4	More Details
CVE-2023-40198	Cross-Site Request Forgery (CSRF) vulnerability in Antsanchez Easy Cookie Law plugin <= 3.1 versions.	5.4	More Details
CVE-2023-40199	Cross-Site Request Forgery (CSRF) vulnerability in CRUDLab WP Like Button plugin <= 1.7.0 versions.	5.4	More Details
CVE-2022-46841	Cross-Site Request Forgery (CSRF) vulnerability in Soflyy Oxygen Builder plugin <= 4.4 versions.	5.4	More Details
CVE-2023-43951	SSCMS 7.2.2 was discovered to contain a cross-site scripting (XSS) vulnerability via the Column Management component.	5.4	More Details
CVE-2023-37996	Cross-Site Request Forgery (CSRF) vulnerability in GTmetrix GTmetrix for WordPress plugin <= 0.4.7 versions.	5.4	More Details
CVE-2023-37992	Cross-Site Request Forgery (CSRF) vulnerability in PressPage Entertainment Inc. Smarty for WordPress plugin <= 3.1.35 versions.	5.4	More Details
CVE-2023-40202	Cross-Site Request Forgery (CSRF) vulnerability in Hannes Etzelstorfer // codemiq WP HTML Mail plugin <= 3.4.1 versions.	5.4	More Details
CVE-2023-43734	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "name" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43267	A cross-site scripting (XSS) vulnerability in the publish article function of emlog pro v2.1.14 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the title field.	5.4	More Details
CVE-2023-43297	An issue in animal-art-lab v13.6.1 allows attackers to send crafted notifications via leakage of the channel access token.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39429	Cross-site scripting vulnerability in FURUNO SYSTEMS wireless LAN access point devices allows an authenticated user to inject an arbitrary script via a crafted configuration. Affected products and versions are as follows: ACERA 1210 firmware ver.02.36 and earlier, ACERA 1150i firmware ver.01.35 and earlier, ACERA 1150w firmware ver.01.35 and earlier, ACERA 1110 firmware ver.01.76 and earlier, ACERA 1020 firmware ver.01.86 and earlier, ACERA 1010 firmware ver.01.86 and earlier, ACERA 950 firmware ver.01.60 and earlier, ACERA 850F firmware ver.01.60 and earlier, ACERA 900 firmware ver.02.54 and earlier, ACERA 850M firmware ver.02.06 and earlier, ACERA 810 firmware ver.03.74 and earlier, and ACERA 800ST firmware ver.07.35 and earlier. They are affected when running in ST(Standalone) mode.	5.4	More Details
CVE-2023-32091	Cross-Site Request Forgery (CSRF) vulnerability in POEditor plugin <= 0.9.4 versions.	5.4	More Details
CVE-2023-40558	Cross-Site Request Forgery (CSRF) vulnerability in eMarket Design YouTube Video Gallery by YouTube Showcase plugin <= 3.3.5 versions.	5.4	More Details
CVE-2023-41693	Cross-Site Request Forgery (CSRF) vulnerability in edward_plainview MyCryptoCheckout plugin <= 2.125 versions.	5.4	More Details
CVE-2023-43735	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "formats_titles[7]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43953	SSCMS 7.2.2 was discovered to contain a cross-site scripting (XSS) vulnerability via the Content Management component.	5.4	More Details
CVE-2023-43733	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "company_address" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43708	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "configuration_title[1] (MODULE_PAYMENT_SAGE_PAY_SERVER_TEXT_TITLE)" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43876	A Cross-Site Scripting (XSS) vulnerability in installation of October v.3.4.16 allows an attacker to execute arbitrary web scripts via a crafted payload injected into the dbhost field.	5.4	More Details
CVE-2023-43878	Rite CMS 3.0 has Multiple Cross-Site scripting (XSS) vulnerabilities that allow attackers to execute arbitrary code via a crafted payload into the Main Menu Items in the Administration Menu.	5.4	More Details
CVE-2023-43884	A Cross-site scripting (XSS) vulnerability in Reference ID from the panel Transactions, of Subrion v4.2.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into 'Reference ID' parameter.	5.4	More Details
CVE-2023-44173	Online Movie Ticket Booking System v1.0 is vulnerable to an authenticated Reflected Cross-Site Scripting vulnerability.	5.4	More Details
CVE-2023-26148	All versions of the package ithewei/libhv are vulnerable to CRLF Injection when untrusted user input is used to set request headers. An attacker can add the \r\n (carriage return line feeds) characters and inject additional headers in the request sent.	5.4	More Details
CVE-2023-3115	An issue has been discovered in GitLab EE affecting all versions affecting all versions from 11.11 prior to 16.2.8, 16.3 prior to 16.3.5, and 16.4 prior to 16.4.1. Single Sign On restrictions were not correctly enforced for indirect project members accessing public members-only project repositories.	5.4	More Details
CVE-2023-3914	A business logic error in GitLab EE affecting all versions prior to 16.2.8, 16.3 prior to 16.3.5, and 16.4 prior to 16.4.1 allows access to internal projects. A service account is not deleted when a namespace is deleted, allowing access to internal projects.	5.4	More Details
CVE-2023-43944	A Stored Cross Site Scripting (XSS) vulnerability was found in SourceCodester Task Management System 1.0. It allows attackers to execute arbitrary code via parameter field in index.php?page=project_list.	5.4	More Details
CVE-2023-5317	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.18.	5.4	More Details
CVE-2023-5319	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.18.	5.4	More Details
CVE-2023-43702	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "tracking_number" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43703	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "product_info[][name]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43704	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "title" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43705	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "translation_value[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43706	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "email_templates_key" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43874	Multiple Cross Site Scripting (XSS) vulnerability in e017 CMS v.2.3.2 allows a local attacker to execute arbitrary code via a crafted script to the Copyright and Author fields in the Meta & Custom Tags Menu.	5.4	More Details
CVE-2023-43873	A Cross Site Scripting (XSS) vulnerability in e017 CMS v.2.3.2 allows a local attacker to execute arbitrary code via a crafted script to the Name filed in the Manage Menu.	5.4	More Details
CVE-2023-43872	A File upload vulnerability in CMSmadesimple v.2.2.18 allows a local attacker to upload a pdf file with hidden Cross Site Scripting (XSS).	5.4	More Details
CVE-2023-43857	Dreamer CMS v4.1.3 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the component /admin/u/toIndex.	5.4	More Details
CVE-2023-40417	A window management issue was addressed with improved state management. This issue is fixed in Safari 17, iOS 17 and iPadOS 17, watchOS 10, macOS Sonoma 14. Visiting a website that frames malicious content may lead to UI spoofing.	5.4	More Details
CVE-2023-41904	Zoho ManageEngine ADManager Plus before 7203 allows 2FA bypass (for AuthToken generation) in REST APIs.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43232	A stored cross-site scripting (XSS) vulnerability in the Website column management function of DedeBIZ v6.2.11 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the title parameter.	5.4	More Details
CVE-2023-43331	A cross-site scripting (XSS) vulnerability in the Add User function of Small CRM v3.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field.	5.4	More Details
CVE-2023-43828	A Cross-site scripting (XSS) vulnerability in /panel/languages/ of Subrion v4.2.1 allow attackers to execute arbitrary web scripts or HTML via a crafted payload injected into 'Title' parameter.	5.4	More Details
CVE-2023-43830	A Cross-site scripting (XSS) vulnerability in /panel/configuration/financial/ of Subrion v4.2.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into several fields: 'Minimum deposit', 'Maximum deposit' and/or 'Maximum balance'.	5.4	More Details
CVE-2023-44042	A stored cross-site scripting (XSS) vulnerability in /settings/index.php of Black Cat CMS 1.4.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Website header parameter.	5.4	More Details
CVE-2023-43732	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "tax_class_title" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-44207	Stored cross-site scripting (XSS) vulnerability in protection plan name. The following products are affected: Acronis Cyber Protect 15 (Linux, Windows) before build 35979.	5.4	More Details
CVE-2023-44048	Sourcecodester Expense Tracker App v1 is vulnerable to Cross Site Scripting (XSS) via add category.	5.4	More Details
CVE-2023-42818	JumpServer is an open source bastion host. When users enable MFA and use a public key for authentication, the Koko SSH server does not verify the corresponding SSH private key. An attacker could exploit a vulnerability by utilizing a disclosed public key to attempt brute-force authentication against the SSH service This issue has been patched in versions 3.6.5 and 3.5.6. Users are advised to upgrade. There are no known workarounds for this issue.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43191	SpringbootCMS 1.0 foreground message can be embedded malicious code saved in the database. When users browse the comments, these malicious codes embedded in the HTML will be executed, and the user's browser will be controlled by the attacker, so as to achieve the special purpose of the attacker, such as cookie theft	5.4	More Details
CVE-2023-44275	OPNsense before 23.7.5 allows XSS via the index.php column_count parameter to the Lobby Dashboard.	5.4	More Details
CVE-2023-44276	OPNsense before 23.7.5 allows XSS via the index.php sequence parameter to the Lobby Dashboard.	5.4	More Details
CVE-2023-43707	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "CatalogsPageDescriptionForm[1][name] " parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43871	A File upload vulnerability in WBCE v.1.6.1 allows a local attacker to upload a pdf file with hidden Cross Site Scripting (XSS).	5.4	More Details
CVE-2023-43709	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "configuration_title[1](MODULE)" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43728	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "stock_delivery_terms_text[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43724	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "derb6zmklgtjuhh2cn5chn2qjbm2stgmfa4.oastify.comscription[1][name]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43722	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "orders_status_groups_name[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43725	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "orders_products_status_name_long[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43721	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "PACKING_SLIPS_SUMMARY_TITLE[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43715	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "ENTRY_FIRST_NAME_MIN_LENGTH_TITLE[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43710	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "configuration_title[1][MODULE_SHIPPING_PERCENT_TEXT_TITLE]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43720	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "BILLING_GENDER_TITLE[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43726	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "orders_products_status_manual_name_long[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43719	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "SHIPPING_GENDER_TITLE[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43727	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "stock_indication_text[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43729	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "xsell_type_name[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43730	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "countries_name[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43712	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "access_levels_name" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43718	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "MSEARCH_ENABLE_TITLE[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43713	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability, which allows attackers to inject JS via the "title" parameter, in the "/admin/admin-menu/add-submit" endpoint, which can lead to unauthorized execution of scripts in a user's web browser.	5.4	More Details
CVE-2023-43717	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "MSEARCH_HIGHLIGHT_ENABLE_TITLE[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43731	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "zone_name" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43714	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "SKIP_CART_PAGE_TITLE[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43716	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "MAX_DISPLAY_NEW_PRODUCTS_TITLE[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43711	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "admin_firstname" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details
CVE-2023-43723	Os Commerce is currently susceptible to a Cross-Site Scripting (XSS) vulnerability. This vulnerability allows attackers to inject JS through the "orders_status_name[1]" parameter, potentially leading to unauthorized execution of scripts within a user's web browser.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47187	There is a file upload XSS vulnerability in Generex CS141 below 2.06 version. The web application allows file uploading, making it possible to upload a file with HTML content. When HTML files are allowed, XSS payload can be injected into the uploaded file.	5.3	More Details
CVE-2023-5215	A flaw was found in libnbd. A server can reply with a block size larger than 2^63 (the NBD spec states the size is a 64-bit unsigned value). This issue could lead to an application crash or other unintended behavior for NBD clients that doesn't treat the return value of the nbd_get_size() function correctly.	5.3	More Details
CVE-2023-26151	Versions of the package asyncua before 0.9.96 are vulnerable to Denial of Service (DoS) such that an attacker can send a malformed packet and as a result, the server will enter into an infinite loop and consume excessive memory.	5.3	More Details
CVE-2023-3967	Allocation of Resources Without Limits or Throttling vulnerability in Hitachi Ops Center Common Services on Linux allows DoS.This issue affects Hitachi Ops Center Common Services: before 10.9.3-00.	5.3	More Details
CVE-2023-4565	Broadcast permission control vulnerability in the framework module. Successful exploitation of this vulnerability may cause the hotspot feature to be unavailable.	5.3	More Details
CVE-2023-38871	The commit 3730880 (April 2023) and v.0.9-beta1 of gugoan Economizzer has a user enumeration vulnerability in the login and forgot password functionalities. The app reacts differently when a user or email address is valid, and when it's not. This may allow an attacker to determine whether a user or email address is valid, or brute force valid usernames and email addresses.	5.3	More Details
CVE-2023-43124	BIG-IP APM clients may send IP traffic outside of the VPN tunnel. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	5.3	More Details
CVE-2023-44216	PVRIC (PowerVR Image Compression) on Imagination 2018 and later GPU devices offers software-transparent compression that enables cross-origin pixel-stealing attacks against feTurbulence and feBlend in the SVG Filter specification, aka a GPU.zip issue. For example, attackers can sometimes accurately determine text contained on a web page from one origin if they control a resource from a different origin.	5.3	More Details
CVE-2023-44205	Sensitive information disclosure due to improper authorization. The following products are affected: Acronis Cyber Protect 15 (Linux, Windows) before build 35979.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47892	All versions of NetMan 204 could allow an unauthenticated remote attacker to read a file (config.cgi) containing sensitive information, like credentials.	5.3	More Details
CVE-2023-42460	Vyper is a Pythonic Smart Contract Language for the EVM. The `_abi_decode()` function does not validate input when it is nested in an expression. Uses of `_abi_decode()` can be constructed which allow for bounds checking to be bypassed resulting in incorrect results. This issue has not yet been fixed, but a fix is expected in release `0.3.10`. Users are advised to reference pull request #3626.	5.3	More Details
CVE-2023-41888	GLPI stands for Gestionnaire Libre de Parc Informatique is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. The lack of path filtering on the GLPI URL may allow an attacker to transmit a malicious URL of login page that can be used to attempt a phishing attack on user credentials. Users are advised to upgrade to version 10.0.10. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2023-41323	GLPI stands for Gestionnaire Libre de Parc Informatique is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. An unauthenticated user can enumerate users logins. Users are advised to upgrade to version 10.0.10. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2023-41312	Permission control vulnerability in the audio module. Successful exploitation of this vulnerability may cause several apps to be activated automatically.	5.3	More Details
CVE-2023-41311	Permission control vulnerability in the audio module. Successful exploitation of this vulnerability may cause an app to be activated automatically.	5.3	More Details
CVE-2023-2544	Authorization bypass vulnerability in UPV PEIX, affecting the component "pdf_curri_new.php". Through a POST request, an authenticated user could change the ID parameter to retrieve all the stored information of other registered users.	5.3	More Details
CVE-2023-40049	In WS_FTP Server version prior to 8.8.2, an unauthenticated user could enumerate files under the 'WebServiceHost' directory listing.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36851	A Missing Authentication for Critical Function vulnerability in Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause limited impact to the file system integrity. With a specific request to webauth_operation.php that doesn't require authentication, an attacker is able to upload and download arbitrary files via J-Web, leading to a loss of integrity or confidentiality, which may allow chaining to other vulnerabilities. This issue affects Juniper Networks Junos OS on SRX Series: * 21.2 versions prior to 21.2R3-S8; * 21.4 versions prior to 21.4R3-S6; * 22.1 versions prior to 22.1R3-S5; * 22.2 versions prior to 22.2R3-S3; * 22.3 versions prior to 22.3R3-S2; * 22.4 versions prior to 22,4R2-S2, 22.4R3; * 23.2 versions prior to 23.2R1-S2, 23.2R2.	5.3	More Details
CVE-2023-43044	IBM License Metric Tool 9.2 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 266893.	5.3	More Details
CVE-2023-20262	A vulnerability in the SSH service of Cisco Catalyst SD-WAN Manager could allow an unauthenticated, remote attacker to cause a process crash, resulting in a DoS condition for SSH access only. This vulnerability does not prevent the system from continuing to function, and web UI access is not affected. This vulnerability is due to insufficient resource management when an affected system is in an error condition. An attacker could exploit this vulnerability by sending malicious traffic to the affected system. A successful exploit could allow the attacker to cause the SSH process to crash and restart, resulting in a DoS condition for the SSH service.	5.3	More Details
CVE-2023-3770	Incorrect validation vulnerability of the data entered, allowing an attacker with access to the network on which the affected device is located to use the discovery port protocol (1925/UDP) to obtain device-specific information without the need for authentication.	5.3	More Details
CVE-2023-26147	All versions of the package ithewei/libhv are vulnerable to HTTP Response Splitting when untrusted user input is used to build headers values. An attacker can add the \r\n (carriage return line feeds) characters to end the HTTP response headers and inject malicious content, like for example additional headers or new response body, leading to a potential XSS vulnerability.	5.3	More Details
CVE-2023-5313	A vulnerability classified as problematic was found in phpkobo Ajax Poll Script 3.18. Affected by this vulnerability is an unknown functionality of the file ajax-poll.php of the component Poll Handler. The manipulation leads to improper enforcement of a single, unique action. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-240949 was assigned to this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44463	An issue was discovered in pretix before 2023.7.1. Incorrect parsing of configuration files causes the application to trust unchecked X-Forwarded-For headers even though it has not been configured to do so. This can lead to IP address spoofing by users of the application.	5.3	More Details
CVE-2023-44270	An issue was discovered in PostCSS before 8.4.31. The vulnerability affects linters using PostCSS to parse external untrusted CSS. An attacker can prepare CSS in such a way that it will contains parts parsed by PostCSS as a CSS comment. After processing by PostCSS, it will be included in the PostCSS output in CSS nodes (rules, properties) despite being included in a comment.	5.3	More Details
CVE-2023-40026	Argo CD is a declarative continuous deployment framework for Kubernetes. In Argo CD versions prior to 2.3 (starting at least in v0.1.0, but likely in any version using Helm before 2.3), using a specifically-crafted Helm file could reference external Helm charts handled by the same repo-server to leak values, or files from the referenced Helm Chart. This was possible because Helm paths were predictable. The vulnerability worked by adding a Helm chart that referenced Helm resources from predictable paths. Because the paths of Helm charts were predictable and available on an instance of repo-server, it was possible to reference and then render the values and resources from other existing Helm charts regardless of permissions. While generally, secrets are not stored in these files, it was nevertheless possible to reference any values from these charts. This issue was fixed in Argo CD 2.3 and subsequent versions by randomizing Helm paths. User's still using Argo CD 2.3 or below are advised to update to a supported version. If this is not possible, disabling Helm chart rendering, or using an additional repo-server for each Helm chart would prevent possible exploitation.	5.0	More Details
CVE-2023-44128	he vulnerability is to delete arbitrary files in LGInstallService ("com.lge.lginstallservies") app. The app contains the exported "com.lge.lginstallservies.InstallService" service that exposes an AIDL interface. All its "installPackage*" methods are finally calling the "installPackageVerify()" method that performs signature validation after the delete file method. An attacker can control conditions so this security check is never performed and an attacker-controlled file is deleted.	5.0	More Details
CVE-2023-44121	The vulnerability is an intent redirection in LG ThinQ Service ("com.lge.lms2") in the "com/lge/lms/things/ui/notification/NotificationManager.java" file. This vulnerability could be exploited by a third-party app installed on an LG device by sending a broadcast with the action "com.lge.lms.things.notification.ACTION". Additionally, this vulnerability is very dangerous because LG ThinQ Service is a system app (having android:sharedUserId="android.uid.system" setting). Intent redirection in this app leads to accessing arbitrary not exported activities of absolutely all apps.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5193	Mattermost fails to properly check permissions when retrieving a post allowing for a System Role with the permission to manage channels to read the posts of a DM conversation.	4.9	More Details
CVE-2023-43493	SQL injection vulnerability in Item List page of Welcart e-Commerce versions 2.7 to 2.8.21 allows a user with author or higher privilege to obtain sensitive information.	4.9	More Details
CVE-2023-41321	GLPI stands for Gestionnaire Libre de Parc Informatique is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. An API user can enumerate sensitive fields values on resources on which he has read access. Users are advised to upgrade to version 10.0.10. There are no known workarounds for this vulnerability.	4.9	More Details
CVE-2023-41322	GLPI stands for Gestionnaire Libre de Parc Informatique is a Free Asset and IT Management Software package, that provides ITIL Service Desk features, licenses tracking and software auditing. A user with write access to another user can make requests to change the latter's password and then take control of their account. Users are advised to upgrade to version 10.0.10. There are no known work around for this vulnerability.	4.9	More Details
CVE-2023-43879	Rite CMS 3.0 has a Cross-Site scripting (XSS) vulnerability that allows attackers to execute arbitrary code via a crafted payload into the Global Content Blocks in the Administration Menu.	4.8	More Details
CVE-2023-43660	Warpgate is a smart SSH, HTTPS and MySQL bastion host for Linux that doesn't need special client apps. The SSH key verification for a user can be bypassed by sending an SSH key offer without a signature. This allows bypassing authentication under following conditions: 1. The attacker knows the username and a valid target name 2. The attacked knows the user's public key and 3. Only SSH public key authentication is required for the user account. This issue has been addressed in version 0.8.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.8	More Details
CVE-2023-5322	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DAR-7000 up to 20151231. It has been rated as critical. Affected by this issue is some unknown functionality of the file /sysmanage/edit_manageadmin.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-240992. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5293	A vulnerability, which was classified as critical, was found in ECshop 4.1.5. Affected is an unknown function of the file /admin/leancloud.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-240924.	4.7	More Details
CVE-2023-0833	A flaw was found in Red Hat's AMQ-Streams, which ships a version of the OKHttp component with an information disclosure flaw via an exception triggered by a header containing an illegal value. This issue could allow an authenticated attacker to access information outside of their regular permissions.	4.7	More Details
CVE-2023-41979	A race condition was addressed with improved locking. This issue is fixed in macOS Sonoma 14. An app may be able to modify protected parts of the file system.	4.7	More Details
CVE-2023-43775	Denial-of-service vulnerability in the web server of the Eaton SMP Gateway allows attacker to potentially force an unexpected restart of the automation platform, impacting the availability of the product. In rare situations, the issue could cause the SMP device to restart in Safe Mode or Max Safe Mode. When in Max Safe Mode, the product is not vulnerable anymore.	4.7	More Details
CVE-2023-4732	A flaw was found in pfn_swap_entry_to_page in memory management subsystem in the Linux Kernel. In this flaw, an attacker with a local user privilege may cause a denial of service problem due to a BUG statement referencing pmd_t x.	4.7	More Details
CVE-2023-20268	A vulnerability in the packet processing functionality of Cisco access point (AP) software could allow an unauthenticated, adjacent attacker to exhaust resources on an affected device. This vulnerability is due to insufficient management of resources when handling certain types of traffic. An attacker could exploit this vulnerability by sending a series of specific wireless packets to an affected device. A successful exploit could allow the attacker to consume resources on an affected device. A sustained attack could lead to the disruption of the Control and Provisioning of Wireless Access Points (CAPWAP) tunnel and intermittent loss of wireless client traffic.	4.7	More Details
CVE-2023-5294	A vulnerability has been found in ECshop 4.1.1 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/order.php. The manipulation of the argument goods_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-240925 was assigned to this vulnerability.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5221	A vulnerability classified as critical has been found in ForU CMS. This affects an unknown part of the file /install/index.php. The manipulation of the argument db_name leads to code injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The associated identifier of this vulnerability is VDB-240363. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2023-34970	A local non-privileged user can make improper GPU processing operations to access a limited amount outside of buffer bounds or to exploit a software race condition. If the system’s memory is carefully prepared by the user, then this in turn could give them access to already freed memory	4.7	More Details
CVE-2023-41911	Samsung Mobile Processor Exynos 2200 allows a GPU Double Free (issue 1 of 2).	4.7	More Details
CVE-2023-33200	A local non-privileged user can make improper GPU processing operations to exploit a software race condition. If the system’s memory is carefully prepared by the user, then this in turn could give them access to already freed memory.	4.7	More Details
CVE-2023-4564	This vulnerability could allow an attacker to store a malicious JavaScript payload in the broadcast message parameter within the admin panel.	4.7	More Details
CVE-2023-3196	This vulnerability could allow an attacker to store a malicious JavaScript payload in the login footer and login page description parameters within the administration panel.	4.7	More Details
CVE-2023-5301	A vulnerability classified as critical was found in DedeCMS 5.7.111. This vulnerability affects the function AddMyAddon of the file album_add.php. The manipulation of the argument albumUploadFiles leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-240940.	4.7	More Details
CVE-2023-32790	Cross-Site Scripting (XSS) vulnerability in NXLog Manager 5.6.5633 version. This vulnerability allows an attacker to inject a malicious JavaScript payload into the 'Full Name' field during a user edit, due to improper sanitization of the input parameter.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41878	MeterSphere is a one-stop open source continuous testing platform, covering functions such as test tracking, interface testing, UI testing and performance testing. The Selenium VNC config used in Metersphere is using a weak password by default, attackers can login to vnc and obtain high permissions. This issue has been addressed in version 2.10.7 LTS. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.6	More Details
CVE-2023-42822	xrdp is an open source remote desktop protocol server. Access to the font glyphs in xrdp_painter.c is not bounds-checked . Since some of this data is controllable by the user, this can result in an out-of-bounds read within the xrdp executable. The vulnerability allows an out-of-bounds read within a potentially privileged process. On non-Debian platforms, xrdp tends to run as root. Potentially an out-of-bounds write can follow the out-of-bounds read. There is no denial-of-service impact, providing xrdp is running in forking mode. This issue has been addressed in release 0.9.23.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.6	More Details
CVE-2023-28373	A flaw exists in FlashArray Purity whereby an array administrator by configuring an external key manager can affect the availability of data on the system including snapshots protected by SafeMode.	4.4	More Details
CVE-2023-5255	For certificates that utilize the auto-renew feature in Puppet Server, a flaw exists which prevents the certificates from being revoked.	4.4	More Details
CVE-2023-4423	The WP Event Manager – Events Calendar, Registrations, Sell Tickets with WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 3.1.37.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2023-41981	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.6, tvOS 17, iOS 16.7 and iPadOS 16.7, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations.	4.4	More Details
CVE-2023-42756	A flaw was found in the Netfilter subsystem of the Linux kernel. A race condition between IPSET_CMD_ADD and IPSET_CMD_SWAP can lead to a kernel panic due to the invocation of `__ip_set_put` on a wrong `set`. This issue may allow a local user to crash the system.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32819	In display, there is a possible information disclosure due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07993705; Issue ID: ALPS08014138.	4.4	More Details
CVE-2023-40388	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14. Safari may save photos to an unprotected location.	4.3	More Details
CVE-2023-41244	Cross-Site Request Forgery (CSRF) vulnerability in Buildfail Localize Remote Images plugin <= 1.0.9 versions.	4.3	More Details
CVE-2023-39158	Cross-Site Request Forgery (CSRF) vulnerability in theDotstore Banner Management For WooCommerce plugin <= 2.4.2 versions.	4.3	More Details
CVE-2023-40532	Path traversal vulnerability in Welcart e-Commerce versions 2.7 to 2.8.21 allows a user with author or higher privilege to obtain partial information of the files on the web server.	4.3	More Details
CVE-2023-40212	Cross-Site Request Forgery (CSRF) vulnerability in theDotstore Product Attachment for WooCommerce plugin <= 2.1.8 versions.	4.3	More Details
CVE-2023-5296	A vulnerability was found in Xinhu RockOA 1.1/2.3.2/15.X3amdi and classified as problematic. Affected by this issue is some unknown functionality of the file api.php?m=reimplat&a=index of the component Password Handler. The manipulation leads to weak password recovery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-240926 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2023-5324	A vulnerability has been found in eeroOS up to 6.16.4-11 and classified as critical. This vulnerability affects unknown code of the component Ethernet Interface. The manipulation leads to denial of service. The attack needs to be approached within the local network. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-241024.	4.3	More Details
CVE-2023-39917	Cross-Site Request Forgery (CSRF) vulnerability in Photo Gallery Team Photo Gallery by Ays – Responsive Image Gallery plugin <= 5.2.6 versions.	4.3	More Details
CVE-2023-39159	Cross-Site Request Forgery (CSRF) vulnerability in theDotstore Fraud Prevention For Woocommerce plugin <= 2.1.5 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25989	Cross-Site Request Forgery (CSRF) vulnerability in Meks Video Importer, Meks Time Ago, Meks ThemeForest Smart Widget, Meks Smart Author Widget, Meks Audio Player, Meks Easy Maps, Meks Easy Photo Feed Widget, Meks Simple Flickr Widget, Meks Easy Ads Widget, Meks Smart Social Widget plugins leading to dismiss or the popup.	4.3	More Details
CVE-2023-38398	Cross-Site Request Forgery (CSRF) vulnerability in Taboola plugin <= 2.0.1 versions.	4.3	More Details
CVE-2023-2358	Hitachi Vantara Pentaho Business Analytics Server prior to versions 9.5.0.0 and 9.3.0.4, including 8.3.x.x, saves passwords of the Hadoop Copy Files step in plaintext.	4.3	More Details
CVE-2023-38390	Cross-Site Request Forgery (CSRF) vulnerability in Anshul Labs Mobile Address Bar Changer plugin <= 3.0 versions.	4.3	More Details
CVE-2023-37991	Cross-Site Request Forgery (CSRF) vulnerability in Monchito.Net WP Emoji One plugin <= 0.6.0 versions.	4.3	More Details
CVE-2023-43664	PrestaShop is an Open Source e-commerce web application. In the Prestashop Back office interface, an employee can list all modules without any access rights: method `ajaxProcessGetPossibleHookingListForModule` doesn't check access rights. This issue has been addressed in commit `15bd281c` which is included in version 8.1.2. Users are advised to upgrade. There are no known workaround for this issue.	4.3	More Details
CVE-2023-35984	The issue was addressed with improved checks. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10, macOS Sonoma 14. An attacker in physical proximity can cause a limited out of bounds write.	4.3	More Details
CVE-2023-0989	An information disclosure issue in GitLab CE/EE affecting all versions starting from 13.11 prior to 16.2.8, 16.3 prior to 16.3.5, and 16.4 prior to 16.4.1 allows an attacker to extract non-protected CI/CD variables by tricking a user to visit a fork with a malicious CI/CD configuration.	4.3	More Details
CVE-2023-3917	Denial of Service in pipelines affecting all versions of Gitlab EE and CE prior to 16.2.8, 16.3 prior to 16.3.5, and 16.4 prior to 16.4.1 allows attacker to cause pipelines to fail.	4.3	More Details
CVE-2023-3920	An issue has been discovered in GitLab affecting all versions starting from 11.2 before 16.2.8, all versions starting from 16.3 before 16.3.5, all versions starting from 16.4 before 16.4.1. It was possible that a maintainer to create a fork relationship between existing projects contrary to the documentation.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44469	A Server-Side Request Forgery issue in the OpenID Connect Issuer in LemonLDAP::NG before 2.17.1 allows authenticated remote attackers to send GET requests to arbitrary URLs through the request_uri authorization parameter. This is similar to CVE-2020-10770.	4.3	More Details
CVE-2023-5198	An issue has been discovered in GitLab affecting all versions prior to 16.2.7, all versions starting from 16.3 before 16.3.5, and all versions starting from 16.4 before 16.4.1. It was possible for a removed project member to write to protected branches using deploy keys.	4.3	More Details
CVE-2023-5329	A vulnerability classified as problematic was found in Field Logic DataCube4 up to 20231001. This vulnerability affects unknown code of the file /api/ of the component Web API. The manipulation leads to improper authentication. The exploit has been disclosed to the public and may be used. VDB-241030 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2023-20179	A vulnerability in the web-based management interface of Cisco Catalyst SD-WAN Manager, formerly Cisco SD-WAN vManage, could allow an authenticated, remote attacker to inject HTML content. This vulnerability is due to improper validation of user-supplied data in element fields. An attacker could exploit this vulnerability by submitting malicious content within requests and persuading a user to view a page that contains injected content. A successful exploit could allow the attacker to modify pages within the web-based management interface, possibly leading to further browser-based attacks against users of the application.	4.3	More Details
CVE-2023-37891	Cross-Site Request Forgery (CSRF) vulnerability in OptiMonk OptiMonk: Popups, Personalization & A/B Testing plugin <= 2.0.4 versions.	4.3	More Details
CVE-2023-4532	An issue has been discovered in GitLab affecting all versions starting from 16.2 before 16.2.8, all versions starting from 16.3 before 16.3.5, all versions starting from 16.4 before 16.4.1. Users were capable of linking CI/CD jobs of private projects which they are not a member of.	4.3	More Details
CVE-2023-37990	Cross-Site Request Forgery (CSRF) vulnerability in Mike Perelink Pro plugin <= 2.1.4 versions.	4.3	More Details
CVE-2023-37998	Cross-Site Request Forgery (CSRF) vulnerability in Saas Disabler allows Cross Site Request Forgery.This issue affects Disabler: from n/a through 3.0.3.	4.3	More Details
CVE-2023-5160	Mattermost fails to check the Show Full Name option at the /api/v4/teams/TEAM_ID/top/team_members endpoint allowing a member to get the full name of another user even if the Show Full Name option was disabled	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3775	A Vault Enterprise Sentinel Role Governing Policy created by an operator to restrict access to resources in one namespace can be applied to requests outside in another non-descendant namespace, potentially resulting in denial of service. Fixed in Vault Enterprise 1.15.0, 1.14.4, 1.13.8.	4.2	More Details
CVE-2023-30959	In Apollo change requests, comments added by users could contain a javascript URI link that when rendered will result in an XSS that require user interaction.	4.1	More Details
CVE-2023-5159	Mattermost fails to properly verify the permissions when managing/updating a bot allowing a User Manager role with user edit permissions to manage/update bots.	3.8	More Details
CVE-2023-41306	Vulnerability of mutex management in the bone voice ID trusted application (TA) module. Successful exploitation of this vulnerability may cause the bone voice ID feature to be unavailable.	3.7	More Details
CVE-2023-5297	A vulnerability was found in Xinhu RockOA 2.3.2. It has been classified as problematic. This affects the function start of the file task.php?m=syslrunt&a=beifen. The manipulation leads to exposure of backup file to an unauthorized control sphere. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-240927.	3.7	More Details
CVE-2023-38872	An Insecure Direct Object Reference (IDOR) vulnerability in gugoan Economizzer commit 3730880 (April 2023) and v.0.9-beta1 allows any unauthenticated attacker to access cash book entry attachments of any other user, if they know the Id of the attachment.	3.7	More Details
CVE-2023-41335	Synapse is an open-source Matrix homeserver written and maintained by the Matrix.org Foundation. When users update their passwords, the new credentials may be briefly held in the server database. While this doesn't grant the server any added capabilities—it already learns the users' passwords as part of the authentication process—it does disrupt the expectation that passwords won't be stored in the database. As a result, these passwords could inadvertently be captured in database backups for a longer duration. These temporarily stored passwords are automatically erased after a 48-hour window. This issue has been addressed in version 1.93.0. Users are advised to upgrade. There are no known workarounds for this issue.	3.7	More Details
CVE-2023-44126	The vulnerability is that the Call management ("com.android.server.telecom") app patched by LG sends a lot of LG-owned implicit broadcasts that disclose sensitive data to all third-party apps installed on the same device. Those intents include data such as call states, durations, called numbers, contacts info, etc.	3.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44129	The vulnerability is that the Messaging ("com.android.mms") app patched by LG forwards attacker-controlled intents back to the attacker in the exported "com.android.mms.ui.QClipIntentReceiverActivity" activity. The attacker can abuse this functionality by launching this activity and then sending a broadcast with the "com.lge.message.action.QCLIP" action. The attacker can send, e.g., their own data/clipdata and set Intent.FLAG_GRANT_* flags. After the attacker received that intent in the "onActivityResult()" method, they would have access to arbitrary content providers that have the `android:grantUriPermissions="true"` flag set.	3.6	More Details
CVE-2023-44127	he vulnerability is that the Call management ("com.android.server.telecom") app patched by LG launches implicit intents that disclose sensitive data to all third-party apps installed on the same device. Those intents include data such as contact details and phone numbers.	3.6	More Details
CVE-2023-41332	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. In Cilium clusters where Cilium's Layer 7 proxy has been disabled, creating workloads with `policy.cilium.io/proxy-visibility` annotations (in Cilium >= v1.13) or `io.cilium.proxy-visibility` annotations (in Cilium <= v1.12) causes the Cilium agent to segfault on the node to which the workload is assigned. Existing traffic on the affected node will continue to flow, but the Cilium agent on the node will not able to process changes to workloads running on the node. This will also prevent workloads from being able to start on the affected node. The denial of service will be limited to the node on which the workload is scheduled, however an attacker may be able to schedule workloads on the node of their choosing, which could lead to targeted attacks. This issue has been resolved in Cilium versions 1.14.2, 1.13.7, and 1.12.14. Users unable to upgrade can avoid this denial of service attack by enabling the Layer 7 proxy.	3.5	More Details
CVE-2023-3906	An input validation issue in the asset proxy in GitLab EE, affecting all versions from 12.3 prior to 16.2.8, 16.3 prior to 16.3.5, and 16.4 prior to 16.4.1, allowed an authenticated attacker to craft image urls which bypass the asset proxy.	3.5	More Details
CVE-2023-5273	A vulnerability classified as problematic was found in SourceCodester Best Courier Management System 1.0. This vulnerability affects unknown code of the file manage_parcel_status.php. The manipulation of the argument id leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-240886 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-5257	A vulnerability was found in WhiteHSBG JNDIExploit 1.4 on Windows. It has been rated as problematic. Affected by this issue is the function handleFileRequest of the file src/main/java/com/feihong/ldap/HTTPServer.java. The manipulation leads to path traversal. The exploit has been disclosed to the public and may be used. VDB-240866 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5286	A vulnerability, which was classified as problematic, has been found in SourceCodester Expense Tracker App v1. Affected by this issue is some unknown functionality of the file add_category.php of the component Category Handler. The manipulation of the argument category_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-240914 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-5305	A vulnerability was found in Online Banquet Booking System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /mail.php of the component Contact Us Page. The manipulation of the argument message leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-240944.	3.5	More Details
CVE-2023-5302	A vulnerability, which was classified as problematic, has been found in SourceCodester Best Courier Management System 1.0. This issue affects some unknown processing of the component Manage Account Page. The manipulation of the argument First Name leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-240941 was assigned to this vulnerability.	3.5	More Details
CVE-2023-5304	A vulnerability has been found in Online Banquet Booking System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /book-services.php of the component Service Booking. The manipulation of the argument message leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-240943.	3.5	More Details
CVE-2023-5327	A vulnerability was found in SATO CL4NX-J Plus 1.13.2-u455_r2. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /rest/dir/. The manipulation of the argument full leads to path traversal. The attack needs to be initiated within the local network. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-241028.	3.5	More Details
CVE-2023-5303	A vulnerability, which was classified as problematic, was found in Online Banquet Booking System 1.0. Affected is an unknown function of the file /view-booking-detail.php of the component Account Detail Handler. The manipulation of the argument username leads to cross site scripting. It is possible to launch the attack remotely. VDB-240942 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-37448	A lock screen issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14. A user may be able to view restricted content from the lock screen.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40384	A permissions issue was addressed with improved redaction of sensitive information. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to read sensitive location information.	3.3	More Details
CVE-2023-40386	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14. An app may be able to access Notes attachments.	3.3	More Details
CVE-2023-40395	The issue was addressed with improved handling of caches. This issue is fixed in tvOS 17, iOS 16.7 and iPadOS 16.7, macOS Monterey 12.7, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to access contacts.	3.3	More Details
CVE-2023-40427	The issue was addressed with improved handling of caches. This issue is fixed in macOS Ventura 13.6, tvOS 17, macOS Monterey 12.7, watchOS 10, iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to read sensitive location information.	3.3	More Details
CVE-2023-35990	The issue was addressed with improved checks. This issue is fixed in iOS 17 and iPadOS 17, watchOS 10, iOS 16.7 and iPadOS 16.7, macOS Sonoma 14. An app may be able to identify what other apps a user has installed.	3.3	More Details
CVE-2023-40434	A configuration issue was addressed with additional restrictions. This issue is fixed in iOS 17 and iPadOS 17, macOS Sonoma 14. An app may be able to access a user's Photos Library.	3.3	More Details
CVE-2023-40456	The issue was addressed with improved checks. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10. An app may be able to access edited photos saved to a temporary directory.	3.3	More Details
CVE-2023-40520	The issue was addressed with improved checks. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10. An app may be able to access edited photos saved to a temporary directory.	3.3	More Details
CVE-2023-41310	Keep-alive vulnerability in the sticky broadcast mechanism. Successful exploitation of this vulnerability may cause malicious apps to run continuously in the background.	3.3	More Details
CVE-2023-29497	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Sonoma 14. An app may be able to access calendar data saved to a temporary directory.	3.3	More Details
CVE-2023-41065	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in tvOS 17, iOS 17 and iPadOS 17, watchOS 10, macOS Sonoma 14. An app may be able to read sensitive location information.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2233	An improper authorization issue has been discovered in GitLab CE/EE affecting all versions starting from 11.8 before 16.2.8, all versions starting from 16.3 before 16.3.5 and all versions starting from 16.4 before 16.4.1. It allows a project reporter to leak the owner's Sentry instance projects.	3.1	More Details
CVE-2023-3979	An issue has been discovered in GitLab affecting all versions starting from 10.6 before 16.2.8, all versions starting from 16.3 before 16.3.5, all versions starting from 16.4 before 16.4.1. It was possible that upstream members to collaborate with you on your branch get permission to write to the merge request’s source branch.	3.1	More Details
CVE-2023-42453	Synapse is an open-source Matrix homeserver written and maintained by the Matrix.org Foundation. Users were able to forge read receipts for any event (if they knew the room ID and event ID). Note that the users were not able to view the events, but simply mark it as read. This could be confusing as clients will show the event as read by the user, even if they are not in the room. This issue has been patched in version 1.93.0. Users are advised to upgrade. There are no known workarounds for this issue.	3.1	More Details
CVE-2023-3922	An issue has been discovered in GitLab affecting all versions starting from 8.15 before 16.2.8, all versions starting from 16.3 before 16.3.5, all versions starting from 16.4 before 16.4.1. It was possible to hijack some links and buttons on the GitLab UI to a malicious page.	3.0	More Details
CVE-2023-5259	A vulnerability classified as problematic was found in ForU CMS. This vulnerability affects unknown code of the file /admin/cms_admin.php. The manipulation of the argument del leads to denial of service. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The identifier of this vulnerability is VDB-240868.	2.7	More Details
CVE-2023-5194	Mattermost fails to properly validate permissions when demoting and deactivating a user allowing for a system/user manager to demote / deactivate another manager	2.7	More Details
CVE-2023-5287	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as problematic, was found in BEECMS 4.0. This affects an unknown part of the file /admin/admin_content_tag.php?action=save_content. The manipulation of the argument tag leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-240915. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4506	The Active Directory Integration / LDAP Integration plugin for WordPress is vulnerable to LDAP Passback in versions up to, and including, 4.1.10. This is due to insufficient validation when changing the LDAP server. This makes it possible for authenticated attackers, with administrative access and above, to change the LDAP server and retrieve the credentials for the original LDAP server.	2.2	More Details
CVE-2023-4505	The Staff / Employee Business Directory for Active Directory plugin for WordPress is vulnerable to LDAP Passback in versions up to, and including, 1.2.3. This is due to insufficient validation when changing the LDAP server. This makes it possible for authenticated attackers, with administrative access and above, to change the LDAP server and retrieve the credentials for the original LDAP server.	2.2	More Details
CVE-2023-2222	Rejected reason: This was deemed not a security vulnerability by upstream.	N/A	More Details
CVE-2023-4262	Rejected reason: User data field is not attacker controlled	N/A	More Details
CVE-2023-39195	Rejected reason: CVE-2023-39195 was found to be a duplicate of CVE-2023-42755. Please see https://access.redhat.com/security/cve/CVE-2023-42755 for more information.	N/A	More Details
CVE-2023-44165	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-44168	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-40744	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The CNA or individual who requested this candidate did not associate it with any vulnerability during 2023. Notes: none.	N/A	More Details
CVE-2023-5290	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2023-44167	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details