SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 21 June 2023

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-34157	Vulnerability of HwWatchHealth being hijacked.Successful exploitation of this vulnerability may cause repeated pop-up windows of the app.	10.0	More Details
CVE-2019-25136	A compromised child process could have injected XBL Bindings into privileged CSS rules, resulting in arbitrary code execution and a sandbox escape. This vulnerability affects Firefox < 70.	10.0	More Details
CVE-2023-35166	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible to execute any wiki content with the right of the TipsPanel author by creating a tip UI extension. This has been patched in XWiki 15.1-rc-1 and 14.10.5.	9.9	More Details
CVE-2023-34251	Grav is a flat-file content management system. Versions prior to 1.7.42 are vulnerable to server side template injection. Remote code execution is possible by embedding malicious PHP code on the administrator screen by a user with page editing privileges. Version 1.7.42 contains a fix for this issue.	9.9	More Details
CVE-2023-29357	Microsoft SharePoint Server Elevation of Privilege Vulnerability	9.8	More Details
CVE-2023-35857	In Siren Investigate before 13.2.2, session keys remain active even after logging out.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29542	A newline in a filename could have been used to bypass the file extension security mechanisms that replace malicious file extensions such as .lnk with .download. This could have led to accidental execution of malicious code. *This bug only affects Firefox and Thunderbird on Windows. Other versions of Firefox and Thunderbird are unaffected.* This vulnerability affects Firefox < 112, Firefox ESR < 102.10, and Thunderbird < 102.10.	9.8	More Details
CVE-2023-25736	An invalid downcast from `nsHTMLDocument` to `nsIContent` could have lead to undefined behavior. This vulnerability affects Firefox < 110.	9.8	More Details
CVE-2023-32216	Memory safety bugs present in Firefox 112. 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 < 113.	9.8	More Details
CVE-2023-29531	An attacker could have caused an out of bounds memory access using WebGL APIs, leading to memory corruption and a potentially exploitable crash. *This bug only affects Firefox and Thunderbird for macOS. Other operating systems are unaffected.* This vulnerability affects Firefox < 112, Firefox ESR < 102.10, and Thunderbird < 102.10.	9.8	More Details
CVE-2023-27396	FINS (Factory Interface Network Service) is a message communication protocol, which is designed to be used in closed FA (Factory Automation) networks, and is used in FA networks composed of OMRON products. Multiple OMRON products that implement FINS protocol contain following security issues -- (1)Plaintext communication, and (2)No authentication required. When FINS messages are intercepted, the contents may be retrieved. When arbitrary FINS messages are injected, any commands may be executed on, or the system information may be retrieved from, the affected device. Affected products and versions are as follows: SYSMAC CS-series CPU Units, all versions, SYSMAC CJ-series CPU Units, all versions, SYSMAC CP-series CPU Units, all versions, SYSMAC NJ-series CPU Units, all versions, SYSMAC NX1P-series CPU Units, all versions, SYSMAC NX102-series CPU Units, all versions, and SYSMAC NX7 Database Connection CPU Units (Ver.1.16 or later)	9.8	More Details
CVE-2023-35855	A buffer overflow in Counter-Strike through 8684 allows a game server to execute arbitrary code on a remote client's machine by modifying the lservercfgfile console variable.	9.8	More Details
CVE-2023-35856	A buffer overflow in Nintendo Mario Kart Wii RMCP01, RMCE01, RMCJ01, and RMCK01 can be exploited by a game client to execute arbitrary code on a client's machine via a crafted packet.	9.8	More Details
CVE-2023-35853	In Suricata before 6.0.13, an adversary who controls an external source of Lua rules may be able to execute Lua code. This is addressed in 6.0.13 by disabling Lua unless allow-rules is true in the security lua configuration section.	9.8	More Details
CVE-2023-35839	A bypass in the component sofa-hessian of Solon before v2.3.3 allows attackers to execute arbitrary code via providing crafted payload.	9.8	More Details
CVE-2023-35813	Multiple Sitecore products allow remote code execution. This affects Experience Manager, Experience Platform, and Experience Commerce through 10.3.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2014-125106	Nanopb before 0.3.1 allows size_t overflows in pb_dec_bytes and pb_dec_string.	9.8	More Details
CVE-2023-35784	A double free or use after free could occur after SSL_clear in OpenBSD 7.2 before errata 026 and 7.3 before errata 004, and in LibreSSL before 3.6.3 and 3.7.x before 3.7.3. NOTE: OpenSSL is not affected.	9.8	More Details
CVE-2023-34416	Memory safety bugs present in Firefox 113, Firefox ESR 102.11, and Thunderbird 102.12. 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 ESR < 102.12, Firefox < 114, and Thunderbird < 102.12.	9.8	More Details
CVE-2023-34417	Memory safety bugs present in Firefox 113. 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 < 114.	9.8	More Details
CVE-2023-34659	jeecg-boot 3.5.0 and 3.5.1 have a SQL injection vulnerability the id parameter of the /jeecg-boot/jmreport/show interface.	9.8	More Details
CVE-2023-27992	The pre-authentication command injection vulnerability in the Zyxel NAS326 firmware versions prior to V5.21(AAZF.14)C0, NAS540 firmware versions prior to V5.21(AATB.11)C0, and NAS542 firmware versions prior to V5.21(ABAG.11)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands remotely by sending a crafted HTTP request.	9.8	More Details
CVE-2023-35885	CloudPanel 2 before 2.3.1 has insecure file-manager cookie authentication.	9.8	More Details
CVE-2023-34600	Adiscon LogAnalyzer v4.1.13 and before is vulnerable to SQL Injection.	9.8	More Details
CVE-2023-34541	Langchain 0.0.171 is vulnerable to Arbitrary code execution in load_prompt.	9.8	More Details
CVE-2020-21489	File Upload vulnerability in Feehicms v.2.0.8 allows a remote attacker to execute arbitrary code via the /admin/index.php?r=admin-user%2Fupdate-self component.	9.8	More Details
CVE-2020-21474	File Upload vulnerability in NucleusCMS v.3.71 allows a remote attacker to execute arbitrary code via the /nucleus/plugins/skinfiles/?dir=rsd parameter.	9.8	More Details
CVE-2020-21174	File Upload vulenrability in liufee CMS v.2.0.7.1 allows a remote attacker to execute arbitrary code via the image suffix function.	9.8	More Details
CVE-2020-20735	File Upload vulnerability in LJCMS v.4.3.R60321 allows a remote attacker to execute arbitrary code via the ljcms/index.php parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20718	File Upload vulnerability in PluckCMS v.4.7.10 dev versions allows a remote attacker to execute arbitrary code via a crafted image file to the the save_file() parameter.	9.8	More Details
CVE-2020-20703	Buffer Overflow vulnerability in VIM v.8.1.2135 allows a remote attacker to execute arbitrary code via the operand parameter.	9.8	More Details
CVE-2020-20413	SQL injection vulnerability found in WUZHICMS v.4.1.0 allows a remote attacker to execute arbitrary code via the checktitle() function in admin/content.php.	9.8	More Details
CVE-2023-35854	Zoho ManageEngine ADSelfService Plus through 6113 has an authentication bypass that can be exploited to steal the domain controller session token for identity spoofing, thereby achieving the privileges of the domain controller administrator. NOTE: the vendor's perspective is that they have "found no evidence or detail of a security vulnerability."	9.8	More Details
CVE-2023-34159	Improper permission control vulnerability in the Notepad app.Successful exploitation of the vulnerability may lead to privilege escalation, which affects availability and confidentiality.	9.8	More Details
CVE-2023-31411	A remote unprivileged attacker can modify and access configuration settings on the EventCam App due to the absence of API authentication. The lack of authentication in the API allows the attacker to potentially compromise the functionality of the EventCam App.	9.8	More Details
CVE-2023-31410	A remote unprivileged attacker can intercept the communication via e.g. Man-In-The-Middle, due to the absence of Transport Layer Security (TLS) in the SICK EventCam App. This lack of encryption in the communication channel can lead to the unauthorized disclosure of sensitive information. The attacker can exploit this weakness to eavesdrop on the communication between the EventCam App and the Client, and potentially manipulate the data being transmitted.	9.8	More Details
CVE-2023-2907	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Marksoft allows SQL Injection.This issue affects Marksoft: through Mobile:v.7.1.7 ; Login:1.4 ; API:20230605.	9.8	More Details
CVE-2023-34832	TP-Link Archer AX10(EU)_V1.2_230220 was discovered to contain a buffer overflow via the function FUN_131e8 - 0x132B4.	9.8	More Details
CVE-2023-25366	In Siglent SDS 1104X-E SDS1xx4X-E_V6.1.37R9.ADS, insecure SCPI interface discloses web password.	9.8	More Details
CVE-2023-29363	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-34548	Simple Customer Relationship Management 1.0 is vulnerable to SQL Injection via the email parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31671	PrestaShop postfinance <= 17.1.13 is vulnerable to SQL Injection via PostfinanceValidationModuleFrontController::postProcess().	9.8	More Details
CVE-2023-34095	cpdb-libs provides frontend and backend libraries for the Common Printing Dialog Backends (CPDB) project. In versions 1.0 through 2.0b4, cpdb-libs is vulnerable to buffer overflows via improper use of `scanf(3)`. cpdb-libs uses the `fscanf()` and `scanf()` functions to parse command lines and configuration files, dropping the read string components into fixed-length buffers, but does not limit the length of the strings to be read by `fscanf()` and `scanf()` causing buffer overflows when a string is longer than 1023 characters. A patch for this issue is available at commit f181bd1f14757c2ae0f17cc76dc20421a40f30b7. As all buffers have a length of 1024 characters, the patch limits the maximum string length to be read to 1023 by replacing all occurrences of `%s` with `%1023s` in all calls of the `fscanf()` and `scanf()` functions.	9.8	More Details
CVE-2023-25367	Siglent SDS 1104X-E SDS1xx4X-E_V6.1.37R9.ADS allows unfiltered user input resulting in Remote Code Execution (RCE) with SCPI interface or web server.	9.8	More Details
CVE-2023-34540	Langchain before v0.0.225 was discovered to contain a remote code execution (RCE) vulnerability in the component JiraAPIWrapper (aka the JIRA API wrapper). This vulnerability allows attackers to execute arbitrary code via crafted input. As noted in the "releases/tag" reference, a fix is available.	9.8	More Details
CVE-2023-34865	Directory traversal vulnerability in ujcms 6.0.2 allows attackers to move files via the rename feature.	9.8	More Details
CVE-2023-34756	bloofox v0.5.2.1 was discovered to contain a SQL injection vulnerability via the cid parameter at admin/index.php?mode=settings&page=charset&action=edit.	9.8	More Details
CVE-2023-34755	bloofox v0.5.2.1 was discovered to contain a SQL injection vulnerability via the userid parameter at admin/index.php?mode=user&action=edit.	9.8	More Details
CVE-2023-34754	bloofox v0.5.2.1 was discovered to contain a SQL injection vulnerability via the pid parameter at admin/index.php?mode=settings&page=plugins&action=edit.	9.8	More Details
CVE-2023-34753	bloofox v0.5.2.1 was discovered to contain a SQL injection vulnerability via the tid parameter at admin/index.php?mode=settings&page=tmpl&action=edit.	9.8	More Details
CVE-2023-34752	bloofox v0.5.2.1 was discovered to contain a SQL injection vulnerability via the lid parameter at admin/index.php?mode=settings&page=lang&action=edit.	9.8	More Details
CVE-2023-34751	bloofox v0.5.2.1 was discovered to contain a SQL injection vulnerability via the gid parameter at admin/index.php?mode=user&page=groups&action=edit.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34750	bloofox v0.5.2.1 was discovered to contain a SQL injection vulnerability via the cid parameter at admin/index.php?mode=settings&page=projects&action=edit.	9.8	More Details
CVE-2023-34747	File upload vulnerability in ujcms 6.0.2 via /api/backend/core/web-file-upload/upload.	9.8	More Details
CVE-2023-32015	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-32014	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-1329	A potential security vulnerability has been identified for certain HP multifunction printers (MFPs). The vulnerability may lead to Buffer Overflow and/or Remote Code Execution when running HP Workpath solutions on potentially affected products.	9.8	More Details
CVE-2023-30150	PrestaShop leocustomajax 1.0 and 1.0.0 are vulnerable to SQL Injection via modules/leocustomajax/leoajax.php.	9.8	More Details
CVE-2023-31746	There is a command injection vulnerability in the adslr VW2100 router with firmware version M1DV1.0. An unauthenticated attacker can exploit the vulnerability to execute system commands as the root user.	9.8	More Details
CVE-2023-34852	PublicCMS <=V4.0.202302 is vulnerable to Insecure Permissions.	9.8	More Details
CVE-2022-48472	A Huawei printer has a system command injection vulnerability. Successful exploitation could lead to remote code execution. Affected product versions include:BiSheng-WNM versions OTA-BiSheng-FW-2.0.0.211-beta,BiSheng-WNM FW 3.0.0.325,BiSheng-WNM FW 2.0.0.211.	9.8	More Details
CVE-2023-35708	In Progress MOVEit Transfer before 2021.0.8 (13.0.8), 2021.1.6 (13.1.6), 2022.0.6 (14.0.6), 2022.1.7 (14.1.7), and 2023.0.3 (15.0.3), a SQL injection vulnerability has been identified in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain unauthorized access to MOVEit Transfer's database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content. These are fixed versions of the DLL drop-in: 2020.1.10 (12.1.10), 2021.0.8 (13.0.8), 2021.1.6 (13.1.6), 2022.0.6 (14.0.6), 2022.1.7 (14.1.7), and 2023.0.3 (15.0.3).	9.8	More Details
CVE-2023-32754	Thinking Software Efence login function has insufficient validation for user input. An unauthenticated remote attacker can exploit this vulnerability to inject arbitrary SQL commands to access, modify or delete database.	9.8	More Details
CVE-2023-32753	OMICARD EDM’s file uploading function does not restrict upload of file with dangerous type. An unauthenticated remote attacker can exploit this vulnerability to upload and run arbitrary executable files to perform arbitrary system commands or disrupt service.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32752	L7 Networks InstantScan IS-8000 & InstantQoS IQ-8000's file uploading function does not restrict upload of file with dangerous type. An unauthenticated remote attacker can exploit this vulnerability to upload and run arbitrary executable files to perform arbitrary system commands or disrupt service.	9.8	More Details
CVE-2023-34800	D-Link Go-RT-AC750 revA_v101b03 was discovered to contain a command injection vulnerability via the service parameter at genacgi_main.	9.8	More Details
CVE-2023-31672	In the PrestaShop < 2.4.3 module "Length, weight or volume sell" (ailinear) there is a SQL injection vulnerability.	9.8	More Details
CVE-2023-34880	cmseasy v7.7.7.7 20230520 was discovered to contain a path traversal vulnerability via the add_action method at lib/admin/language_admin.php. This vulnerability allows attackers to execute arbitrary code and perform a local file inclusion.	9.8	More Details
CVE-2023-2686	Buffer overflow in Wi-Fi Commissioning MicriumOS example in Silicon Labs Gecko SDK v4.2.3 or earlier allows connected device to write payload onto the stack.	9.8	More Details
CVE-2023-21130	In btm_ble_periodic_adv_sync_lost of btm_ble_gap.cc, there is a possible remote code execution due to a buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-273502002	9.8	More Details
CVE-2021-0945	In _PMRCreate of the PowerVR kernel driver, a missing bounds check means it is possible to overwrite heap memory via PhysmemNewRamBackedPMR. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2021-0701	In PVRSRVBridgeSyncPrimOpCreate of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	9.8	More Details
CVE-2023-34563	netgear R6250 Firmware Version 1.0.4.48 is vulnerable to Buffer Overflow after authentication.	9.8	More Details
CVE-2023-29297	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by a Improper Neutralization of Special Elements Used in a Template Engine vulnerability that could lead to arbitrary code execution by an admin-privilege authenticated attacker. Exploitation of this issue does not require user interaction.	9.1	More Details
CVE-2023-29534	Different techniques existed to obscure the fullscreen notification in Firefox and Focus for Android. These could have led to potential user confusion and spoofing attacks. *This bug only affects Firefox and Focus for Android. Other versions of Firefox are unaffected.* This vulnerability affects Firefox for Android < 112 and Focus for Android < 112.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-34448	Grav is a flat-file content management system. Prior to version 1.7.42, the patch for CVE-2022-2073, a server-side template injection vulnerability in Grav leveraging the default `filter()` function, did not block other built-in functions exposed by Twig's Core Extension that could be used to invoke arbitrary unsafe functions, thereby allowing for remote code execution. A patch in version 1.74.2 overrides the built-in Twig `map()` and `reduce()` filter functions in `system/src/Grav/Common/Twig/Extension/GravExtension.php` to validate the argument passed to the filter in `$arrow`.	8.8	More Details
CVE-2020-21252	Cross Site Request Forgery vulnerability in Neeke HongCMS 3.0.0 allows a remote attacker to execute arbitrary code and escalate privileges via the updateusers parameter.	8.8	More Details
CVE-2023-35809	An issue was discovered in SugarCRM Enterprise before 11.0.6 and 12.x before 12.0.3. A Bean Manipulation vulnerability has been identified in the REST API. By using a crafted request, custom PHP code can be injected through the REST API because of missing input validation. Regular user privileges can be used to exploit this vulnerability. Editions other than Enterprise are also affected.	8.8	More Details
CVE-2023-35811	An issue was discovered in SugarCRM Enterprise before 11.0.6 and 12.x before 12.0.3. Two SQL Injection vectors have been identified in the REST API. By using crafted requests, custom SQL code can be injected through the REST API because of missing input validation. Regular user privileges can use used for exploitation. Editions other than Enterprise are also affected.	8.8	More Details
CVE-2023-3295	The Unlimited Elements For Elementor (Free Widgets, Addons, Templates) for WordPress is vulnerable to arbitrary file uploads due to missing file type validation of files in the file manager functionality in versions up to, and including, 1.5.66 . This makes it possible for authenticated attackers, with contributor-level permissions and above, to upload arbitrary files on the affected site's server which may make remote code execution possible. The issue was partially patched in version 1.5.66 and fully patched in 1.5.67. CVE-2023-31231 appears to be a duplicate of this issue.	8.8	More Details
CVE-2023-33131	Microsoft Outlook Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-21127	In readSampleData of NuMediaExtractor.cpp, there is a possible out of bounds write due to uninitialized data. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-275418191	8.8	More Details
CVE-2020-20067	File upload vulnerability in ebCMS v.1.1.0 allows a remote attacker to execute arbitrary code via the upload type parameter.	8.8	More Details
CVE-2023-32031	Microsoft Exchange Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-32465	Dell Power Protect Cyber Recovery, contains an Authentication Bypass vulnerability. An attacker could potentially exploit this vulnerability, leading to unauthorized admin access to the Cyber Recovery application. Exploitation may lead to complete system takeover by an attacker.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32009	Windows Collaborative Translation Framework Elevation of Privilege Vulnerability	8.8	More Details
CVE-2023-29373	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-29372	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2020-21325	An issue in WUZHI CMS v.4.1.0 allows a remote attacker to execute arbitrary code via the set_chache method of the function\common.func.php file.	8.8	More Details
CVE-2023-2359	The Slider Revolution WordPress plugin through 6.6.12 does not check for valid image files upon import, leading to an arbitrary file upload which may be escalated to Remote Code Execution in some server configurations.	8.8	More Details
CVE-2023-21115	In btm_sec_encrypt_change of btm_sec.cc, there is a possible way to downgrade the link key type due to improperly used crypto. This could lead to paired device escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-258834033	8.8	More Details
CVE-2023-21108	In sdpu_build_uuid_seq of sdp_discovery.cc, there is a possible out of bounds write due to a use after free. This could lead to remote code execution over Bluetooth, if HFP support is enabled, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-239414876	8.8	More Details
CVE-2023-30625	rudder-server is part of RudderStack, an open source Customer Data Platform (CDP). Versions of rudder-server prior to 1.3.0-rc.1 are vulnerable to SQL injection. This issue may lead to Remote Code Execution (RCE) due to the `rudder` role in PostgresSQL having superuser permissions by default. Version 1.3.0-rc.1 contains patches for this issue.	8.8	More Details
CVE-2023-34253	Grav is a flat-file content management system. Prior to version 1.7.42, the denylist introduced in commit 9d6a2d to prevent dangerous functions from being executed via injection of malicious templates was insufficient and could be easily subverted in multiple ways -- (1) using unsafe functions that are not banned, (2) using capitalised callable names, and (3) using fully-qualified names for referencing callables. Consequently, a low privileged attacker with login access to Grav Admin panel and page creation/update permissions is able to inject malicious templates to obtain remote code execution. A patch in version 1.7.42 improves the denylist.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34252	Grav is a flat-file content management system. Prior to version 1.7.42, there is a logic flaw in the `GravExtension.filterFilter()` function whereby validation against a denylist of unsafe functions is only performed when the argument passed to filter is a string. However, passing an array as a callable argument allows the validation check to be skipped. Consequently, a low privileged attacker with login access to Grav Admin panel and page creation/update permissions is able to inject malicious templates to obtain remote code execution. The vulnerability can be found in the `GravExtension.filterFilter()` function declared in `/system/src/Grav/Common/Twig/Extension/GravExtension.php`. Version 1.7.42 contains a patch for this issue. End users should also ensure that `twig.undefined_functions` and `twig.undefined_filters` properties in `/path/to/webroot/system/config/system.yaml` configuration file are set to `false` to disallow Twig from treating undefined filters/functions as PHP functions and executing them.	8.8	More Details
CVE-2023-2719	The SupportCandy WordPress plugin before 3.1.7 does not properly sanitise and escape the `id` parameter for an Agent in the REST API before using it in an SQL statement, leading to an SQL Injection exploitable by users with a role as low as Subscriber.	8.8	More Details
CVE-2023-35030	Cross-site request forgery (CSRF) vulnerability in the Layout module's SEO configuration in Liferay Portal 7.4.3.70 through 7.4.3.76, and Liferay DXP 7.4 update 70 through 76 allows remote attackers to execute arbitrary code in the scripting console via the `_com_liferay_layout_admin_web_portlet_GroupPagesPortlet_backURL` parameter.	8.8	More Details
CVE-2023-27634	Cross-Site Request Forgery (CSRF) vulnerability allows arbitrary file upload in Shingo Intrepidity plugin <= 1.5.1 versions.	8.8	More Details
CVE-2023-25434	libtiff 4.5.0 is vulnerable to Buffer Overflow via extractContigSamplesBytes() at /libtiff/tools/tiffcrop.c:3215.	8.8	More Details
CVE-2020-20726	Cross Site Request Forgery vulnerability in Gila GilaCMS v.1.11.4 allows a remote attacker to execute arbitrary code via the cm/update_rows/user parameter.	8.8	More Details
CVE-2023-29362	Remote Desktop Client Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-35808	An issue was discovered in SugarCRM Enterprise before 11.0.6 and 12.x before 12.0.3. An Unrestricted File Upload vulnerability has been identified in the Notes module. By using crafted requests, custom PHP code can be injected and executed through the Notes module because of missing input validation. Regular user privileges can be used to exploit this vulnerability. Editions other than Enterprise are also affected.	8.8	More Details
CVE-2022-46850	Auth. (author+) Broken Access Control vulnerability leading to Arbitrary File Deletion in Nabil Lemsieh Easy Media Replace plugin <= 0.1.3 versions.	8.7	More Details
CVE-2023-32274	Enphase Installer Toolkit versions 3.27.0 has hard coded credentials embedded in binary code in the Android application. An attacker can exploit this and gain access to sensitive information.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3036	An unchecked read in NTP server in github.com/cloudflare/cfnts prior to commit 783490b https://github.com/cloudflare/cfnts/commit/783490b913f05e508a492cd7b02e3c4ec2297b71 enabled a remote attacker to trigger a panic by sending an NTSAuthenticator packet with extension length longer than the packet contents.	8.6	More Details
CVE-2023-2080	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Forcepoint Cloud Security Gateway (CSG) Portal on Web Cloud Security Gateway, Email Security Cloud allows Blind SQL Injection.	8.5	More Details
CVE-2023-29360	Microsoft Streaming Service Elevation of Privilege Vulnerability	8.4	More Details
CVE-2023-2533	A Cross-Site Request Forgery (CSRF) vulnerability has been identified in PaperCut NG/MF, which, under specific conditions, could potentially enable an attacker to alter security settings or execute arbitrary code. This could be exploited if the target is an admin with a current login session. Exploiting this would typically involve the possibility of deceiving an admin into clicking a specially crafted malicious link, potentially leading to unauthorized changes.	8.4	More Details
CVE-2023-35782	The ipandlanguageredirect extension before 5.1.2 for TYPO3 allows SQL Injection.	8.2	More Details
CVE-2022-47586	Unauth. SQL Injection (SQLi) vulnerability in Themefic Ultimate Addons for Contact Form 7 plugin <= 3.1.23 versions.	8.2	More Details
CVE-2023-34154	Vulnerability of undefined permissions in HUAWEI VR screen projection.Successful exploitation of this vulnerability will cause third-party apps to create windows in an arbitrary way, consuming system resources.	8.2	More Details
CVE-2023-33243	RedTeam Pentesting discovered that the web interface of STARFACE as well as its REST API allows authentication using the SHA512 hash of the password instead of the cleartext password. While storing password hashes instead of cleartext passwords in an application's database generally has become best practice to protect users' passwords in case of a database compromise, this is rendered ineffective when allowing to authenticate using the password hash.	8.1	More Details
CVE-2023-29351	Windows Group Policy Elevation of Privilege Vulnerability	8.1	More Details
CVE-2023-3325	The CMS Commander plugin for WordPress is vulnerable to authorization bypass due to the use of an insufficiently unique cryptographic signature on the 'cmsc_add_site' function in versions up to, and including, 2.287. This makes it possible for unauthenticated attackers to the plugin to change the '_cmsc_public_key' in the plugin config, providing access to the plugin's remote control functionalities, such as creating an admin access URL, which can be used for privilege escalation. This can only be exploited if the plugin has not been configured yet, however, if combined with another arbitrary plugin installation and activation vulnerability, the impact can be severe.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35142	Jenkins Checkmarx Plugin 2022.4.3 and earlier disables SSL/TLS validation for connections to the Checkmarx server by default.	8.1	More Details
CVE-2020-21366	Cross Site Request Forgery vulnerability in GreenCMS v.2.3 allows an attacker to gain privileges via the adduser function of index.php.	8.0	More Details
CVE-2022-48330	A Huawei sound box product has an out-of-bounds write vulnerability. Attackers can exploit this vulnerability to cause buffer overflow. Affected product versions include:FLMG-10 versions FLMG-10 10.0.1.0(H100SP22C00).	8.0	More Details
CVE-2023-35141	In Jenkins 2.399 and earlier, LTS 2.387.3 and earlier, POST requests are sent in order to load the list of context actions. If part of the URL includes insufficiently escaped user-provided values, a victim may be tricked into sending a POST request to an unexpected endpoint by opening a context menu.	8.0	More Details
CVE-2023-28310	Microsoft Exchange Server Remote Code Execution Vulnerability	8.0	More Details
CVE-2023-21139	In bindPlayer of MediaControlPanel.java, there is a possible launch arbitrary activity in SysUI due to Unsafe Intent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-271845008	7.8	More Details
CVE-2022-31644	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products, which might allow arbitrary code execution, escalation of privilege, denial of service, and information disclosure.	7.8	More Details
CVE-2023-21131	In checkKeyIntentParceledCorrectly() of ActivityManagerService.java, there is a possible bypass of Parcel Mismatch mitigations due to a logic error in the code. This could lead to local escalation of privilege and the ability to launch arbitrary activities in settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-265015796	7.8	More Details
CVE-2023-24897	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-32027	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-24895	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-3001	A CWE-502: Deserialization of Untrusted Data vulnerability exists in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32026	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-30759	The driver installation package created by Printer Driver Packager NX v1.0.02 to v1.1.25 fails to detect its modification and may spawn an unexpected process with the administrative privilege. If a non-administrative user modifies the driver installation package and runs it on the target PC, an arbitrary program may be executed with the administrative privilege.	7.8	More Details
CVE-2023-32025	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-29356	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-31646	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products, which might allow arbitrary code execution, escalation of privilege, denial of service, and information disclosure.	7.8	More Details
CVE-2023-29349	Microsoft ODBC and OLE DB Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-31645	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products, which might allow arbitrary code execution, escalation of privilege, denial of service, and information disclosure.	7.8	More Details
CVE-2023-0009	A local privilege escalation (PE) vulnerability in the Palo Alto Networks GlobalProtect app on Windows enables a local user to execute programs with elevated privileges.	7.8	More Details
CVE-2023-21618	Adobe Substance 3D Designer version 12.4.1 (and earlier) is affected by an Access of Uninitialized Pointer vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-21120	In multiple functions of cdm_engine.cpp, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-258188673	7.8	More Details
CVE-2023-21135	In onCreate of NotificationAccessSettings.java, there is a possible failure to persist notifications settings due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-260570119	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21121	In onResume of AppManagementFragment.java, there is a possible way to prevent users from forgetting a previously connected VPN due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12Android ID: A-205460459	7.8	More Details
CVE-2023-21129	In getFullScreenIntentDecision of NotificationInterruptStateProviderImpl.java, there is a possible activity launch while the app is in the background due to a BAL bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-274759612	7.8	More Details
CVE-2023-21128	In various functions of AppStandbyController.java, there is a possible way to break manageability scenarios due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-272042183	7.8	More Details
CVE-2023-24032	In Zimbra Collaboration Suite through 9.0 and 8.8.15, an attacker (who has initial user access to a Zimbra server instance) can execute commands as root by passing one of JVM arguments, leading to local privilege escalation (LPE).	7.8	More Details
CVE-2023-21122	In various functions of various files, there is a possible way to bypass the DISALLOW_DEBUGGING_FEATURES restriction for tracing due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-270050191	7.8	More Details
CVE-2023-21138	In onNullBinding of CallRedirectionProcessor.java, there is a possible long lived connection due to improper input validation. This could lead to local escalation of privilege and background activity launches with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-273260090	7.8	More Details
CVE-2023-21123	In multiple functions of multiple files, there is a possible way to bypass the DISALLOW_DEBUGGING_FEATURES restriction for tracing due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-270050064	7.8	More Details
CVE-2023-29321	Adobe Animate versions 22.0.9 (and earlier) and 23.0.1 (and earlier) are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2023-21124	In run of multiple files, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-265798353	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21126	In bindOutputSwitcherAndBroadcastButton of MediaControlPanel.java, there is a possible launch arbitrary activity under SysUI due to Unsafe Intent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-271846393	7.8	More Details
CVE-2023-29326	.NET Framework Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-2847	During internal security analysis, a local privilege escalation vulnerability has been identified. On a machine with the affected ESET product installed, it was possible for a user with lower privileges due to improper privilege management to trigger actions with root privileges. ESET remedied this possible attack vector and has prepared new builds of its products that are no longer susceptible to this vulnerability.	7.8	More Details
CVE-2023-32028	Microsoft SQL OLE DB Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-32542	Out-of-bounds read vulnerability exists in TELLUS v4.0.15.0 and TELLUS Lite v4.0.15.0. Opening a specially crafted V8 file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-29365	Windows Media Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-29366	Windows Geolocation Service Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-29367	iSCSI Target WMI Provider Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-35788	An issue was discovered in fl_set_geneve_opt in net/sched/cls_flower.c in the Linux kernel before 6.3.7. It allows an out-of-bounds write in the flower classifier code via TCA_FLOWER_KEY_ENC_OPTS_GENEVE packets. This may result in denial of service or privilege escalation.	7.8	More Details
CVE-2023-32201	Stack-based buffer overflow vulnerability exists in TELLUS v4.0.15.0 and TELLUS Lite v4.0.15.0. Opening a specially crafted SIM2 file may lead to information disclosure and/or arbitrary code execution. This vulnerability is different from CVE-2023-32538 and CVE-2023-32273.	7.8	More Details
CVE-2023-29370	Windows Media Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-29371	Windows GDI Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32008	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-33133	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-32538	Stack-based buffer overflow vulnerability exists in TELLUS v4.0.15.0 and TELLUS Lite v4.0.15.0. Opening a specially crafted SIM2 file may lead to information disclosure and/or arbitrary code execution. This vulnerability is different from CVE-2023-32273 and CVE-2023-32201.	7.8	More Details
CVE-2023-2569	A CWE-787: Out-of-Bounds Write vulnerability exists that could cause local denial-of-service, elevation of privilege, and potentially kernel execution when a malicious actor with local user access crafts a script/program using an IOCTL call in the Foxboro.sys driver.	7.8	More Details
CVE-2023-32270	Access of memory location after end of buffer issue exists in TELLUS v4.0.15.0 and TELLUS Lite v4.0.15.0. Opening a specially crafted V8 file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-32273	Stack-based buffer overflow vulnerability exists in TELLUS v4.0.15.0 and TELLUS Lite v4.0.15.0. Opening a specially crafted SIM2 file may lead to information disclosure and/or arbitrary code execution. This vulnerability is different from CVE-2023-32538 and CVE-2023-32201.	7.8	More Details
CVE-2023-32288	Out-of-bounds read vulnerability exists in TELLUS v4.0.15.0 and TELLUS Lite v4.0.15.0. Opening a specially crafted SIM file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-28287	Microsoft Publisher Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-28295	Microsoft Publisher Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-32029	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-32018	Windows Hello Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-32017	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-32012	Windows Container Manager Service Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33137	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-32276	Stack-based buffer overflow vulnerability exists in TELLUS v4.0.15.0 and TELLUS Lite v4.0.15.0. Opening a specially crafted V8 file may lead to information disclosure and/or arbitrary code execution.	7.8	More Details
CVE-2023-33146	Microsoft Office Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-1049	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists that could cause execution of malicious code when an unsuspicious user loads a project file from the local filesystem into the HMI.	7.8	More Details
CVE-2023-31239	Stack-based buffer overflow vulnerability in V-Server v4.0.15.0 and V-Server Lite v4.0.15.0 and earlier allows an attacker to execute arbitrary code by having user open a specially crafted VPR file.	7.8	More Details
CVE-2023-29346	NTFS Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-34795	xlsxio v0.1.2 to v0.2.34 was discovered to contain a free of uninitialized pointer in the xlsxioread_sheetlist_close() function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted XLSX file.	7.8	More Details
CVE-2023-30905	The MC990 X and UV300 RMC component has and inadequate default configuration that could be exploited to obtain enhanced privilege.	7.8	More Details
CVE-2023-34641	KioWare for Windows through v8.33 was discovered to contain an incomplete blacklist filter for blocked dialog boxes on Windows 10. This issue can allow attackers to open a file dialog box via the function window.print() which can then be used to open an unprivileged command prompt.	7.8	More Details
CVE-2023-34642	KioWare for Windows through v8.33 was discovered to contain an incomplete blacklist filter for blocked dialog boxes on Windows 10. This issue can allow attackers to open a file dialog box via the function showDirectoryPicker() which can then be used to open an unprivileged command prompt.	7.8	More Details
CVE-2023-29358	Windows GDI Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-29359	GDI Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-25645	There is a permission and access control vulnerability in some ZTE AndroidTV STBs. Due to improper permission settings, non-privileged application can perform functions that are protected with signature/privilege-level permissions. Exploitation of this vulnerability could clear personal data and applications on the user's device, affecting device operation.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32022	Windows Server Service Security Feature Bypass Vulnerability	7.6	More Details
CVE-2023-35844	packages/backend/src/routers in Lightdash before 0.510.3 has insecure file endpoints, e.g., they allow .. directory traversal and do not ensure that an intended file extension (.csv or .png) is used.	7.5	More Details
CVE-2023-34163	Permission control vulnerability in the window management module.Successful exploitation of this vulnerability may cause features to perform abnormally.	7.5	More Details
CVE-2023-34455	snappy-java is a fast compressor/decompressor for Java. Due to use of an unchecked chunk length, an unrecoverable fatal error can occur in versions prior to 1.1.10.1. The code in the function hasNextChunk in the fileSnappyInputStream.java checks if a given stream has more chunks to read. It does that by attempting to read 4 bytes. If it wasn't possible to read the 4 bytes, the function returns false. Otherwise, if 4 bytes were available, the code treats them as the length of the next chunk. In the case that the `compressed` variable is null, a byte array is allocated with the size given by the input data. Since the code doesn't test the legality of the `chunkSize` variable, it is possible to pass a negative number (such as 0xFFFFFFFF which is -1), which will cause the code to raise a `java.lang.NegativeArraySizeException` exception. A worse case would happen when passing a huge positive value (such as 0x7FFFFFFF), which would raise the fatal `java.lang.OutOfMemoryError` error. Version 1.1.10.1 contains a patch for this issue.	7.5	More Details
CVE-2023-34166	Vulnerability of system restart triggered by abnormal callbacks passed to APIs.Successful exploitation of this vulnerability may cause the system to restart.	7.5	More Details
CVE-2023-35843	NocoDB through 0.106.0 (or 0.109.1) has a path traversal vulnerability that allows an unauthenticated attacker to access arbitrary files on the server by manipulating the path parameter of the /download route. This vulnerability could allow an attacker to access sensitive files and data on the server, including configuration files, source code, and other sensitive information.	7.5	More Details
CVE-2023-3312	A vulnerability was found in drivers/cpufreq/qcom-cpufreq-hw.c in cpufreq subsystem in the Linux Kernel. This flaw, during device unbind will lead to double release problem leading to denial of service.	7.5	More Details
CVE-2023-35848	VirtualSquare picoTCP (aka PicoTCP-NG) through 2.1 lacks certain size calculations before attempting to set a value of an mss structure member.	7.5	More Details
CVE-2023-35849	VirtualSquare picoTCP (aka PicoTCP-NG) through 2.1 does not properly check whether header sizes would result in accessing data outside of a packet.	7.5	More Details
CVE-2023-35846	VirtualSquare picoTCP (aka PicoTCP-NG) through 2.1 does not check the transport layer length in a frame before performing port filtering.	7.5	More Details
CVE-2022-32757	IBM Security Directory Suite VA 8.0.1 through 8.0.1.19 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 228510.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33168	IBM Security Directory Suite VA 8.0.1 could allow an attacker to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 228588.	7.5	More Details
CVE-2023-35847	VirtualSquare picoTCP (aka PicoTCP-NG) through 2.1 does not have an MSS lower bound (e.g., it could be zero).	7.5	More Details
CVE-2023-34155	Vulnerability of unauthorized calling on HUAWEI phones and tablets.Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2023-34162	Version update determination vulnerability in the user profile module.Successful exploitation of this vulnerability may cause repeated HMS Core updates and cause services to fail.	7.5	More Details
CVE-2023-34161	nappropriate authorization vulnerability in the SettingsProvider module.Successful exploitation of this vulnerability may cause features to perform abnormally.	7.5	More Details
CVE-2023-25747	A potential use-after-free in libaudio was fixed by disabling the AAudio backend when running on Android API below version 30. *This bug only affects Firefox for Android. Other versions of Firefox are unaffected.* This vulnerability affects Firefox for Android < 110.1.0.	7.5	More Details
CVE-2023-35790	An issue was discovered in dec_patch_dictionary.cc in libjxl before 0.8.2. An integer underflow in patch decoding can lead to a denial of service, such as an infinite loop.	7.5	More Details
CVE-2022-48486	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2023-25733	The return value from `gfx::SourceSurfaceSkia::Map()` wasn't being verified which could have potentially lead to a null pointer dereference. This vulnerability affects Firefox < 110.	7.5	More Details
CVE-2023-32214	Protocol handlers `ms-cxh` and `ms-cxh-full` could have been leveraged to trigger a denial of service. *Note: This attack only affects Windows. Other operating systems are not affected.* This vulnerability affects Firefox < 113, Firefox ESR < 102.11, and Thunderbird < 102.11.	7.5	More Details
CVE-2022-48471	There is a misinterpretation of input vulnerability in Huawei Printer. Successful exploitation of this vulnerability may cause the printer service to be abnormal.	7.5	More Details
CVE-2022-48473	There is a misinterpretation of input vulnerability in Huawei Printer. Successful exploitation of this vulnerability may cause the printer service to be abnormal.	7.5	More Details
CVE-2023-24243	CData RSB Connect v22.0.8336 was discovered to contain a Server-Side Request Forgery (SSRF).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32209	A maliciously crafted favicon could have led to an out of memory crash. This vulnerability affects Firefox < 113.	7.5	More Details
CVE-2023-30222	An information disclosure vulnerability in 4D SAS 4D Server Application v17, v18, v19 R7 and earlier allows attackers to retrieve password hashes for all users via eavesdropping.	7.5	More Details
CVE-2023-30223	A broken authentication vulnerability in 4D SAS 4D Server software v17, v18, v19 R7, and earlier allows attackers to send crafted TCP packets containing requests to perform arbitrary actions.	7.5	More Details
CVE-2023-34645	jfinal CMS 5.1.0 has an arbitrary file read vulnerability.	7.5	More Details
CVE-2023-34603	JeecgBoot up to v 3.5.1 was discovered to contain a SQL injection vulnerability via the component queryFilterTableDictInfo at org.jeecg.modules.api.controller.SystemApiController.	7.5	More Details
CVE-2023-23841	SolarWinds Serv-U is submitting an HTTP request when changing or updating the attributes for File Share or File request. Part of the URL of the request discloses sensitive data.	7.5	More Details
CVE-2023-34602	JeecgBoot up to v 3.5.1 was discovered to contain a SQL injection vulnerability via the component queryTableDictItemsByCode at org.jeecg.modules.api.controller.SystemApiController.	7.5	More Details
CVE-2022-48487	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2022-48501	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2022-48489	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2022-48490	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2022-48492	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2022-48493	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48494	Vulnerability of lax app identity verification in the pre-authorization function.Successful exploitation of this vulnerability will cause malicious apps to become pre-authorized.	7.5	More Details
CVE-2022-48496	Vulnerability of lax app identity verification in the pre-authorization function.Successful exploitation of this vulnerability will cause malicious apps to become pre-authorized.	7.5	More Details
CVE-2023-28809	Some access control products are vulnerable to a session hijacking attack because the product does not update the session ID after a user successfully logs in. To exploit the vulnerability, attackers have to request the session ID at the same time as a valid user logs in, and gain device operation permissions by forging the IP and session ID of an authenticated user.	7.5	More Details
CVE-2023-22248	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. An attacker could leverage this vulnerability to leak another user's data. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2023-21144	In doInBackground of NotificationContentInflater.java, there is a possible temporary denial or service due to long running operations. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-252766417	7.5	More Details
CVE-2022-48497	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2022-48498	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2022-48499	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2022-48500	Configuration defects in the secure OS module.Successful exploitation of this vulnerability will affect availability.	7.5	More Details
CVE-2023-35852	In Suricata before 6.0.13 (when there is an adversary who controls an external source of rules), a dataset filename, that comes from a rule, may trigger absolute or relative directory traversal, and lead to write access to a local filesystem. This is addressed in 6.0.13 by requiring allow-absolute-filenames and allow-write (in the datasets rules configuration section) if an installation requires traversal/writing in this situation.	7.5	More Details
CVE-2023-34616	An issue was discovered pbjson thru 0.4.0 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	7.5	More Details
CVE-2023-34615	An issue was discovered JSONUtil thru 5.0 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30631	Improper Input Validation vulnerability in Apache Software Foundation Apache Traffic Server. The configuration option proxy.config.http.push_method_enabled didn't function. However, by default the PUSH method is blocked in the ip_allow configuration file.This issue affects Apache Traffic Server: from 8.0.0 through 9.2.0. 8.x users should upgrade to 8.1.7 or later versions 9.x users should upgrade to 9.2.1 or later versions	7.5	More Details
CVE-2023-34612	An issue was discovered ph-json thru 9.5.5 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	7.5	More Details
CVE-2023-33933	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Software Foundation Apache Traffic Server.This issue affects Apache Traffic Server: from 8.0.0 through 9.2.0. 8.x users should upgrade to 8.1.7 or later versions 9.x users should upgrade to 9.2.1 or later versions	7.5	More Details
CVE-2023-30082	A denial of service attack might be launched against the server if an unusually lengthy password (more than 10000000 characters) is supplied using the osTicket application. This can cause the website to go down or stop responding. When a long password is entered, this procedure will consume all available CPU and memory.	7.5	More Details
CVE-2023-34000	Unauth. IDOR vulnerability leading to PII Disclosure in WooCommerce Stripe Payment Gateway plugin <= 7.4.0 versions.	7.5	More Details
CVE-2023-25369	Siglent SDS 1104X-E SDS1xx4X-E_V6.1.37R9.ADS is vulnerable to Denial of Service on the user interface triggered by malformed SCPI command.	7.5	More Details
CVE-2023-24936	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability	7.5	More Details
CVE-2023-29331	.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2023-34878	An issue was discovered in Ujcms v6.0.2 allows attackers to gain sensitive information via the dir parameter to /api/backend/core/web-file-html/download-zip.	7.5	More Details
CVE-2023-25368	Siglent SDS 1104X-E SDS1xx4X-E_V6.1.37R9.ADS is vulnerable to Incorrect Access Control. An unauthenticated attacker can overwrite firmnware.	7.5	More Details
CVE-2020-20636	SQL injection vulnerability found in Joyplus-cms v.1.6.0 allows a remote attacker to access sensitive information via the id parameter of the goodbad() function.	7.5	More Details
CVE-2023-34611	An issue was discovered mjson thru 1.4.1 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34610	An issue was discovered json-io thru 4.14.0 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	7.5	More Details
CVE-2020-20335	Buffer Overflow vulnerability in Antirez Kilo before commit 7709a04ae8520c5b04d261616098cebf742f5a23 allows a remote attacker to cause a denial of service via the editorUpdateRow function in kilo.c.	7.5	More Details
CVE-2023-32030	.NET and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2023-34609	An issue was discovered flexjson thru 3.3 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	7.5	More Details
CVE-2023-34867	Jerryscript 3.0 (commit 05dbbd1) was discovered to contain an Assertion Failure via the ecma_property_hashmap_create at jerry-core/ecma/base/ecma-property-hashmap.c.	7.5	More Details
CVE-2023-35110	An issue was discovered jjson thru 0.1.7 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	7.5	More Details
CVE-2023-34623	An issue was discovered jtidy thru r938 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	7.5	More Details
CVE-2023-34624	An issue was discovered htmlcleaner thru = 2.28 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	7.5	More Details
CVE-2023-32011	Windows iSCSI Discovery Service Denial of Service Vulnerability	7.5	More Details
CVE-2023-34617	An issue was discovered genson thru 1.6 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	7.5	More Details
CVE-2020-21486	SQL injection vulnerability in PHPOK v.5.4. allows a remote attacker to obtain sensitive information via the _userlist function in framerwork/phpok_call.php file.	7.5	More Details
CVE-2023-34620	An issue was discovered hjson thru 3.0.0 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	7.5	More Details
CVE-2022-47184	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Software Foundation Apache Traffic Server.This issue affects Apache Traffic Server: 8.0.0 to 9.2.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34868	Jerryscript 3.0 (commit 05dbbd1) was discovered to contain an Assertion Failure via the parser_parse_for_statement_start at jerry-core/parser/js/js-parser-statm.c.	7.5	More Details
CVE-2023-34614	An issue was discovered jmarsden/jsonij thru 0.5.2 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	7.5	More Details
CVE-2023-34613	An issue was discovered sojo thru 1.1.1 allows attackers to cause a denial of service or other unspecified impacts via crafted object that uses cyclic dependencies.	7.5	More Details
CVE-2023-3230	Missing Authorization in GitHub repository fossbilling/fossbilling prior to 0.5.0.	7.5	More Details
CVE-2023-33126	.NET and Visual Studio Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-33128	.NET and Visual Studio Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-33130	Microsoft SharePoint Server Spoofing Vulnerability	7.3	More Details
CVE-2023-33135	.NET and Visual Studio Elevation of Privilege Vulnerability	7.3	More Details
CVE-2023-3305	A vulnerability was found in C-DATA Web Management System up to 20230607. It has been classified as critical. This affects an unknown part of the file /cgi-bin/jumpto.php?class=user&page=config_save&isphp=1 of the component User Creation Handler. The manipulation of the argument user/newpassword leads to improper access controls. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-231801 was assigned to this vulnerability.	7.3	More Details
CVE-2023-3337	A vulnerability was found in PuneethReddyHC Online Shopping System Advanced 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/reg.php of the component Admin Registration. The manipulation leads to improper authentication. The attack can be launched remotely. The identifier VDB-232009 was assigned to this vulnerability.	7.3	More Details
CVE-2023-3306	A vulnerability was found in Ruijie RG-EW1200G EW_3.0(1)B11P204. It has been declared as critical. This vulnerability affects unknown code of the file app.09df2a9e44ab48766f5f.js of the component Admin Password Handler. The manipulation leads to improper access controls. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-231802 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34101	Contiki-NG is an operating system for internet of things devices. In version 4.8 and prior, when processing ICMP DAO packets in the `dao_input_storing` function, the Contiki-NG OS does not verify that the packet buffer is big enough to contain the bytes it needs before accessing them. Up to 16 bytes can be read out of bounds in the `dao_input_storing` function. An attacker can truncate an ICMP packet so that it does not contain enough data, leading to an out-of-bounds read on these lines. The problem has been patched in the "develop" branch of Contiki-NG, and is expected to be included in release 4.9. As a workaround, one can apply the changes in Contiki-NG pull request #2435 to patch the system.	7.3	More Details
CVE-2023-1862	Cloudflare WARP client for Windows (up to v2023.3.381.0) allowed a malicious actor to remotely access the warp-svc.exe binary due to an insufficient access control policy on an IPC Named Pipe. This would have enabled an attacker to trigger WARP connect and disconnect commands, as well as obtaining network diagnostics and application configuration from the target's device. It is important to note that in order to exploit this, a set of requirements would need to be met, such as the target's device must've been reachable on port 445, allowed authentication with NULL sessions or otherwise having knowledge of the target's credentials.	7.3	More Details
CVE-2020-20919	File upload vulnerability in Pluck CMS v.4.7.10-dev2 allows a remote attacker to execute arbitrary code and access sensitive information via the theme.php file.	7.2	More Details
CVE-2020-20491	SQL injection vulnerability in OpenCart v.2.2.00 thru 3.0.3.2 allows a remote attacker to execute arbitrary code via the Fba plugin function in upload/admin/index.php.	7.2	More Details
CVE-2023-2805	The SupportCandy WordPress plugin before 3.1.7 does not properly sanitise and escape the agents[] parameter in the set_add_agent_leaves AJAX function before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin.	7.2	More Details
CVE-2020-20918	An issue discovered in Pluck CMS v.4.7.10-dev2 allows a remote attacker to execute arbitrary php code via the hidden parameter to admin.php when editing a page.	7.2	More Details
CVE-2020-20969	File Upload vulnerability in PluckCMS v.4.7.10 allows a remote attacker to execute arbitrary code via the trashcan_restoreitem.php file.	7.2	More Details
CVE-2023-2492	The QueryWall: Plug'n Play Firewall WordPress plugin through 1.1.1 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin.	7.2	More Details
CVE-2023-2221	The WP Custom Cursors WordPress plugin before 3.2 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as Admin.	7.2	More Details
CVE-2020-21400	SQL injection vulnerability in gaozhifeng PHPMyWind v.5.6 allows a remote attacker to execute arbitrary code via the id variable in the modify function.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35810	An issue was discovered in SugarCRM Enterprise before 11.0.6 and 12.x before 12.0.3. A Second-Order PHP Object Injection vulnerability has been identified in the DocuSign module. By using crafted requests, custom PHP code can be injected and executed through the DocuSign module because of missing input validation. Admin user privileges are required to exploit this vulnerability. Editions other than Enterprise are also affected.	7.2	More Details
CVE-2022-33166	IBM Security Directory Suite VA 8.0.1 through 8.0.1.19 could allow a privileged user to upload malicious files of dangerous types that can be automatically processed within the product's environment. IBM X-Force ID: 228586.	7.2	More Details
CVE-2022-32752	IBM Security Directory Suite VA 8.0.1 through 8.0.1.19 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 228439.	7.2	More Details
CVE-2023-35775	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WP Backup Solutions WP Backup Manager plugin <= 1.13.1 versions.	7.1	More Details
CVE-2023-35772	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Alain Gonzalez Google Map Shortcode plugin <= 3.1.2 versions.	7.1	More Details
CVE-2023-27420	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Everest Themes Arya Multipurpose theme <= 1.0.5 versions.	7.1	More Details
CVE-2023-3268	An out of bounds (OOB) memory access flaw was found in the Linux kernel in relay_file_read_start_pos in kernel/relay.c in the relayfs. This flaw could allow a local attacker to crash the system or leak kernel internal information.	7.1	More Details
CVE-2023-32021	Windows SMB Witness Service Security Feature Bypass Vulnerability	7.1	More Details
CVE-2023-35884	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in EventPrime plugin <= 3.0.5 versions.	7.1	More Details
CVE-2023-21565	Azure DevOps Server Spoofing Vulnerability	7.1	More Details
CVE-2023-28175	Improper Authorization in SSH server in Bosch VMS 11.0, 11.1.0, and 11.1.1 allows a remote authenticated user to access resources within the trusted internal network via a port forwarding request.	7.1	More Details
CVE-2023-29337	NuGet Client Remote Code Execution Vulnerability	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26436	Attackers with access to the "documentconverterws" API were able to inject serialized Java objects, that were not properly checked during deserialization. Access to this API endpoint is restricted to local networks by default. Arbitrary code could be injected that is being executed when processing the request. A check has been introduced to restrict processing of legal and expected classes for this API. We now log a warning in case there are attempts to inject illegal classes. No publicly available exploits are known.	7.1	More Details
CVE-2023-24420	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Zestard Technologies Admin side data storage for Contact Form 7 plugin <= 1.1.1 versions.	7.1	More Details
CVE-2023-35098	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in John Brien WordPress NextGen GalleryView plugin <= 0.5.5 versions.	7.1	More Details
CVE-2023-35097	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Internet Marketing Dojo WP Affiliate Links plugin <= 0.1.1 versions.	7.1	More Details
CVE-2023-35826	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in cedrus_remove in drivers/staging/media/sunxi/cedrus/cedrus.c.	7.0	More Details
CVE-2023-35828	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in renesas_usb3_remove in drivers/usb/gadget/udc/renesas_usb3.c.	7.0	More Details
CVE-2023-21101	In multiple functions of WVDrmPlugin.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-258189255	7.0	More Details
CVE-2022-4149	The Netskope client service (prior to R96) on Windows runs as NT AUTHORITY\SYSTEM which writes log files to a writable directory (C:\Users\Public\netSkope) for a standard user. The files are created and written with a SYSTEM account except one file (logplaceholder) which inherits permission giving all users full access control list. Netskope client restricts access to this file by allowing only read permissions as a standard user. Whenever the Netskope client service restarts, it deletes the logplaceholder and recreates, creating a race condition, which can be exploited by a malicious local user to create the file and set ACL permissions on the file. Once the file is created by a malicious user with proper ACL permissions, all files within C:\Users\Public\netSkope\ becomes modifiable by the unprivileged user. By using Windows pseudo-symlink, these files can be pointed to other places in the system and thus malicious users will be able to elevate privileges.	7.0	More Details
CVE-2023-32010	Windows Bus Filter Driver Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-35824	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in dm1105_remove in drivers/media/pci/dm1105/dm1105.c.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35823	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in saa7134_finidev in drivers/media/pci/saa7134/saa7134-core.c.	7.0	More Details
CVE-2023-26062	A mobile network solution internal fault is found in Nokia Web Element Manager before 22 R1, in which an authenticated, unprivileged user can execute administrative functions. Exploitation is not possible from outside of mobile network solution architecture. This means that exploit is not possible from mobile network user UEs, from roaming networks, or from the Internet. Exploitation is possible only from a CSP (Communication Service Provider) mobile network solution internal BTS management network.	7.0	More Details
CVE-2023-2270	The Netskope client service running with NT\SYSTEM privileges accepts network connections from localhost to start various services and execute commands. The connection handling function of Netskope client before R100 in this service utilized a relative path to download and unzip configuration files on the machine. This relative path provided a way for local users to write arbitrary files at a location which is accessible to only higher privileged users. This can be exploited by local users to execute code with NT\SYSTEM privileges on the end machine.	7.0	More Details
CVE-2023-2570	A CWE-129: Improper Validation of Array Index vulnerability exists that could cause local denial-of-service, and potentially kernel execution when a malicious actor with local user access crafts a script/program using an unpredictable index to an IOCTL call in the Foxboro.sys driver.	7.0	More Details
CVE-2023-35829	An issue was discovered in the Linux kernel before 6.3.2. A use-after-free was found in rkvdec_remove in drivers/staging/media/rkvdec/rkvdec.c.	7.0	More Details
CVE-2023-35827	An issue was discovered in the Linux kernel through 6.3.8. A use-after-free was found in ravb_remove in drivers/net/ethernet/renesas/ravb_main.c.	7.0	More Details
CVE-2023-29364	Windows Authentication Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-29368	Windows Filtering Platform Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-31642	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products, which might allow arbitrary code execution, escalation of privilege, denial of service, and information disclosure.	7.0	More Details
CVE-2022-31641	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products, which might allow arbitrary code execution, escalation of privilege, denial of service, and information disclosure.	7.0	More Details
CVE-2022-31640	Potential vulnerabilities have been identified in the system BIOS of certain HP PC products, which might allow arbitrary code execution, escalation of privilege, denial of service, and information disclosure.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29361	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-34733	A lack of exception handling in the Volkswagen Discover Media Infotainment System Software Version 0876 allows attackers to cause a Denial of Service (DoS) via supplying crafted media files when connecting a device to the vehicle's USB plug and play feature.	6.8	More Details
CVE-2023-0837	An improper authorization check of local device settings in TeamViewer Remote between version 15.41 and 15.42.7 for Windows and macOS allows an unprivileged user to change basic local device settings even though the options were locked. This can result in unwanted changes to the configuration.	6.6	More Details
CVE-2023-33144	Visual Studio Code Spoofing Vulnerability	6.6	More Details
CVE-2023-26428	Attackers can successfully request arbitrary snippet IDs, including E-Mail signatures of other users within the same context. Signatures of other users could be read even though they are not explicitly shared. We improved permission handling when requesting snippets that are not explicitly shared with other users. No publicly available exploits are known.	6.5	More Details
CVE-2023-32032	.NET and Visual Studio Elevation of Privilege Vulnerability	6.5	More Details
CVE-2023-35882	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Team Heateor Super Socializer plugin <= 7.13.52 versions.	6.5	More Details
CVE-2023-33307	A null pointer dereference in Fortinet FortiOS before 7.2.5 and before 7.0.11, FortiProxy before 7.2.3 and before 7.0.9 allows attacker to denial of sslvpn service via specifically crafted request in network parameter.	6.5	More Details
CVE-2023-33306	A null pointer dereference in Fortinet FortiOS before 7.2.5, before 7.0.11 and before 6.4.13, FortiProxy before 7.2.4 and before 7.0.10 allows attacker to denial of sslvpn service via specifically crafted request in bookmark parameter.	6.5	More Details
CVE-2023-35862	libcoap 4.3.1 contains a buffer over-read via the function coap_parse_oscore_conf_mem at coap_oscore.c.	6.5	More Details
CVE-2023-2793	Mattermost fails to validate links on external websites when constructing a preview for a linked website, allowing an attacker to cause a denial-of-service by a linking to a specially crafted webpage in a message.	6.5	More Details
CVE-2023-33142	Microsoft SharePoint Server Elevation of Privilege Vulnerability	6.5	More Details
CVE-2023-33140	Microsoft OneNote Spoofing Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35005	In Apache Airflow, some potentially sensitive values were being shown to the user in certain situations. This vulnerability is mitigated by the fact configuration is not shown in the UI by default (only if `[webserver] expose_config` is set to `non-sensitive-only`), and not all uncensored values are actually sentitive. This issue affects Apache Airflow: from 2.5.0 before 2.6.2. Users are recommended to update to version 2.6.2 or later.	6.5	More Details
CVE-2023-34597	A vulnerability in Fibaro Motion Sensor firmware v3.4 allows attackers to cause a Denial of Service (DoS) via a crafted Z-Wave message.	6.5	More Details
CVE-2023-34660	jjeecg-boot V3.5.0 has an unauthorized arbitrary file upload in /jeecg-boot/jmreport/upload interface.	6.5	More Details
CVE-2023-33129	Microsoft SharePoint Server Denial of Service Vulnerability	6.5	More Details
CVE-2023-20885	Vulnerability in Cloud Foundry Notifications, Cloud Foundry SMB-volume release, Cloud FOundry cf-nfs-volume release.This issue affects Notifications: All versions prior to 63; SMB-volume release: All versions prior to 3.1.19; cf-nfs-volume release: 5.0.X versions prior to 5.0.27, 7.1.X versions prior to 7.1.19.	6.5	More Details
CVE-2023-32210	Documents were incorrectly assuming an ordering of principal objects when ensuring we were loading an appropriately privileged principal. In certain circumstances it might have been possible to cause a document to be loaded with a higher privileged principal than intended. This vulnerability affects Firefox < 113.	6.5	More Details
CVE-2023-24937	Windows CryptoAPI Denial of Service Vulnerability	6.5	More Details
CVE-2023-29545	Similar to CVE-2023-28163, this time when choosing 'Save Link As', suggested filenames containing environment variable names would have resolved those in the context of the current user. *This bug only affects Firefox and Thunderbird on Windows. Other versions of Firefox and Thunderbird are unaffected.* This vulnerability affects Firefox < 112, Firefox ESR < 102.10, and Thunderbird < 102.10.	6.5	More Details
CVE-2023-3229	Business Logic Errors in GitHub repository fossbilling/fossbilling prior to 0.5.0.	6.5	More Details
CVE-2023-2792	Mattermost fails to sanitize ephemeral error messages, allowing an attacker to obtain arbitrary message contents by a specially crafted /groupmsg command.	6.5	More Details
CVE-2022-48469	There is a traffic hijacking vulnerability in Huawei routers. Successful exploitation of this vulnerability can cause packets to be hijacked by attackers.	6.5	More Details
CVE-2023-29546	When recording the screen while in Private Browsing on Firefox for Android the address bar and keyboard were not hidden, potentially leaking sensitive information. *This bug only affects Firefox for Android. Other operating systems are unaffected.* This vulnerability affects Firefox for Android < 112 and Focus for Android < 112.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29369	Remote Procedure Call Runtime Denial of Service Vulnerability	6.5	More Details
CVE-2020-20502	Cross Site Request Forgery found in yzCMS v.2.0 allows a remote attacker to execute arbitrary code via the token check function.	6.5	More Details
CVE-2023-35840	_joinPath in elFinderVolumeLocalFileSystem.class.php in elFinder before 2.1.62 allows path traversal in the PHP LocalVolumeDriver connector.	6.5	More Details
CVE-2023-35147	Jenkins AWS CodeCommit Trigger Plugin 3.0.12 and earlier does not restrict the AWS SQS queue name path parameter in an HTTP endpoint, allowing attackers with Item/Read permission to obtain the contents of arbitrary files on the Jenkins controller file system.	6.5	More Details
CVE-2023-35148	A cross-site request forgery (CSRF) vulnerability in Jenkins Digital.ai App Management Publisher Plugin 2.6 and earlier allows attackers to connect to an attacker-specified URL, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2023-35776	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Beplus Sermon'e – Sermons Online plugin <= 1.0.0 versions.	6.5	More Details
CVE-2023-35149	A missing permission check in Jenkins Digital.ai App Management Publisher Plugin 2.6 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2023-34367	Windows 7 is vulnerable to a full blind TCP/IP hijacking attack. The vulnerability exists in Windows 7 (any Windows until Windows 8) and in any implementation of TCP/IP, which is vulnerable to the Idle scan attack (including many IoT devices). NOTE: The vendor considers this a low severity issue.	6.5	More Details
CVE-2023-29352	Windows Remote Desktop Security Feature Bypass Vulnerability	6.5	More Details
CVE-2023-24938	Windows CryptoAPI Denial of Service Vulnerability	6.5	More Details
CVE-2023-26013	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in WPChill Strong Testimonials plugin <= 3.0.2 versions.	6.5	More Details
CVE-2023-29289	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an XML Injection vulnerability. An attacker with low privileges can trigger a specially crafted script to a security feature bypass. Exploitation of this issue does not require user interaction.	6.5	More Details
CVE-2023-34596	A vulnerability in Aeotec WallMote Switch firmware v2.3 allows attackers to cause a Denial of Service (DoS) via a crafted Z-Wave message.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32659	SUBNET PowerSYSTEM Center versions 2020 U10 and prior contain a cross-site scripting vulnerability that may allow an attacker to inject malicious code into report header graphic files that could propagate out of the system and reach users who are subscribed to email notifications.	6.5	More Details
CVE-2023-33145	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	6.5	More Details
CVE-2023-2787	Mattermost fails to check channel membership when accessing message threads, allowing an attacker to access arbitrary posts by using the message threads API.	6.5	More Details
CVE-2023-33869	Enphase Envoy versions D7.0.88 is vulnerable to a command injection exploit that may allow an attacker to execute root commands.	6.3	More Details
CVE-2023-33132	Microsoft SharePoint Server Spoofing Vulnerability	6.3	More Details
CVE-2023-25187	An issue was discovered on NOKIA Airscale ASIKA Single RAN devices before 21B. Nokia Single RAN commissioning procedures do not change (factory-time installed) default SSH public/private key values that are specific to a network operator. As a result, the CSP internal BTS network SSH server (disabled by default) continues to apply the default SSH public/private key values. These keys don't give access to BTS, because service user authentication is username/password-based on top of SSH. Nokia factory installed default SSH keys are meant to be changed from operator-specific values during the BTS deployment commissioning phase. However, before the 21B release, BTS commissioning manuals did not provide instructions to change default SSH keys (to BTS operator-specific values). This leads to a possibility for malicious operations staff (inside a CSP network) to attempt MITM exploitation of BTS service user access, during the moments that SSH is enabled for Nokia service personnel to perform troubleshooting activities.	6.3	More Details
CVE-2023-3232	A vulnerability was found in Zhong Bang CRMEB up to 4.6.0 and classified as critical. This issue affects some unknown processing of the file /api/wechat/app_auth of the component Image Upload. The manipulation leads to deserialization. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-231503. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3233	A vulnerability was found in Zhong Bang CRMEB up to 4.6.0. It has been classified as critical. Affected is the function get_image_base64 of the file api/controller/v1/PublicController.php. The manipulation leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-231504. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-35783	The ke_search (aka Faceted Search) extension before 4.0.3, 4.1.x through 4.6.x before 4.6.6, and 5.x before 5.0.2 for TYPO3 allows XSS via indexed data.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3238	A vulnerability, which was classified as critical, has been found in OTCMS up to 6.62. This issue affects some unknown processing of the file /admin/read.php?mudi=getSignal. The manipulation of the argument signalUrl leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-231509 was assigned to this vulnerability.	6.3	More Details
CVE-2023-3237	A vulnerability classified as critical was found in OTCMS up to 6.62. This vulnerability affects unknown code. The manipulation of the argument username/password with the input admin 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-231508.	6.3	More Details
CVE-2023-3235	A vulnerability was found in mccms up to 2.6.5. It has been rated as critical. Affected by this issue is the function pic_api of the file sys/apps/controllers/admin/Comic.php. The manipulation of the argument url leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-231506 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-3310	A vulnerability, which was classified as critical, has been found in code-projects Agro-School Management System 1.0. Affected by this issue is some unknown functionality of the file loaddata.php. The manipulation of the argument subject/course leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-231806 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-3236	A vulnerability classified as critical has been found in mccms up to 2.6.5. This affects the function pic_save of the file sys/apps/controllers/admin/Comic.php. The manipulation of the argument pic leads to server-side request forgery. 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-231507.	6.3	More Details
CVE-2023-3340	A vulnerability was found in SourceCodester Online School Fees System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file ajx.php of the component GET Parameter Handler. The manipulation of the argument name_startsWith 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-232016.	6.3	More Details
CVE-2023-3307	A vulnerability was found in miniCal 1.0.0. It has been rated as critical. This issue affects some unknown processing of the file /booking/show_bookings/. The manipulation of the argument search_query 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-231803. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3274	A vulnerability classified as critical has been found in code-projects Supplier Management System 1.0. Affected is an unknown function of the file btn_functions.php of the component Picture Handler. The manipulation 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-231624.	6.3	More Details
CVE-2023-3275	A vulnerability classified as critical was found in PHPGurukul Rail Pass Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /view-pass-detail.php of the component POST Request Handler. The manipulation of the argument searchdata leads to sql injection. The attack can be launched remotely. The identifier VDB-231625 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2788	Mattermost fails to check if an admin user account active after an oauth2 flow is started, allowing an attacker with admin privileges to retain persistent access to Mattermost by obtaining an oauth2 access token while the attacker's account is deactivated.	6.2	More Details
CVE-2020-21485	Cross Site Scripting vulnerability in Alluxio v.1.8.1 allows a remote attacker to executea arbitrary code via the path parameter in the browse board component.	6.1	More Details
CVE-2023-3320	The WP Sticky Social plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.1. This is due to missing nonce validation in the ~/admin/views/admin.php file. This makes it possible for unauthenticated attackers to modify the plugin's settings and inject malicious web scripts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-3193	Cross-site scripting (XSS) vulnerability in the Layout module's SEO configuration in Liferay Portal 7.4.3.70 through 7.4.3.73, and Liferay DXP 7.4 update 70 through 73 allows remote attackers to inject arbitrary web script or HTML via the `_com_liferay_layout_admin_web_portlet_GroupPagesPortlet_backURL` parameter.	6.1	More Details
CVE-2023-35029	Open redirect vulnerability in the Layout module's SEO configuration in Liferay Portal 7.4.3.70 through 7.4.3.76, and Liferay DXP 7.4 update 70 through 76 allows remote attackers to redirect users to arbitrary external URLs via the `_com_liferay_layout_admin_web_portlet_GroupPagesPortlet_backURL` parameter.	6.1	More Details
CVE-2023-2820	An information disclosure vulnerability in the faye endpoint in Proofpoint Threat Response / Threat Response Auto-Pull (PTR/TRAP) could be used by an attacker on an adjacent network to obtain credentials to integrated services via a man-in-the-middle position or cryptanalysis of the session traffic. An attacker could use these credentials to impersonate PTR/TRAP to these services. All versions prior to 5.10.0 are affected.	6.1	More Details
CVE-2023-2779	The Social Share, Social Login and Social Comments WordPress plugin before 7.13.52 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	6.1	More Details
CVE-2023-29158	SUBNET PowerSYSTEM Center versions 2020 U10 and prior are vulnerable to replay attacks which may result in a denial-of-service condition or a loss of data integrity.	6.1	More Details
CVE-2023-24030	An open redirect vulnerability exists in the /preauth Servlet in Zimbra Collaboration Suite through 9.0 and 8.8.15. To exploit the vulnerability, an attacker would need to have obtained a valid zimbra auth token or a valid preauth token. Once the token is obtained, an attacker could redirect a user to any URL if url sanitisation is bypassed in incoming requests. NOTE: this is similar, but not identical, to CVE-2021-34807.	6.1	More Details
CVE-2023-2654	The Conditional Menus WordPress plugin before 1.2.1 does not escape a parameter before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2020-21268	Cross Site Scripting vulnerability in EasySoft ZenTao v.11.6.4 allows a remote attacker to execute arbitrary code via the lastComment parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34666	Cross-site scripting (XSS) vulnerability in Phpgurukul Cyber Cafe Management System 1.0 allows remote attackers to inject arbitrary web script or HTML via the admin username parameter.	6.1	More Details
CVE-2023-2399	The QuBot WordPress plugin before 1.1.6 doesn't filter user input on chat, leading to bad code inserted on it be reflected on the user dashboard.	6.1	More Details
CVE-2020-20725	Cross Site Scripting vulnerability in taogogo taoCMS v.2.5 beta5.1 allows remote attacker to execute arbitrary code via the name field in admin.php.	6.1	More Details
CVE-2023-34833	An arbitrary file upload vulnerability in the component /api/upload.php of ThinkAdmin v6 allows attackers to execute arbitrary code via a crafted file.	6.1	More Details
CVE-2023-34415	When choosing a site-isolated process for a document loaded from a data: URL that was the result of a redirect, Firefox would load that document in the same process as the site that issued the redirect. This bypassed the site-isolation protections against Spectre-like attacks on sites that host an "open redirect". Firefox no longer follows HTTP redirects to data: URLs. This vulnerability affects Firefox < 114.	6.1	More Details
CVE-2023-24031	An issue was discovered in Zimbra Collaboration (ZCS) 9.0 and 8.8.15. XSS can occur, via one of attributes of the webmail /h/ endpoint, to execute arbitrary JavaScript code, leading to information disclosure.	6.1	More Details
CVE-2020-20070	Cross Site Scripting vulnerability found in wkeyuan DWSurvey 1.0 allows a remote attacker to execute arbitrary code via thequltemld parameter of the qu-multi-fillblank!answers.action file.	6.1	More Details
CVE-2023-3294	Cross-site Scripting (XSS) - DOM in GitHub repository saleor/react-storefront prior to c29aab226f07ca980cc19787dcef101e11b83ef7.	6.1	More Details
CVE-2020-21052	Cross Site Scripting vulnerability in zrlog zrlog v.2.1.3 allows a remote attacker to execute arbitrary code via the nickame parameter of the /post/addComment function.	6.1	More Details
CVE-2020-21058	Cross Site Scripting vulnerability in Typora v.0.9.79 allows a remote attacker to execute arbitrary code via the mermaid sytax.	6.1	More Details
CVE-2020-22402	Cross Site Scripting (XSS) vulnerability in SOGo Web Mail before 4.3.1 allows attackers to obtain user sensitive information when a user reads an email containing malicious code.	6.1	More Details
CVE-2021-31280	An issue was discovered in tp5cms through 2017-05-25. admin.php/system/set.html has XSS via the keywords parameter.	6.1	More Details
CVE-2023-33495	Craft CMS through 4.4.9 is vulnerable to HTML Injection.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34453	snappy-java is a fast compressor/decompressor for Java. Due to unchecked multiplications, an integer overflow may occur in versions prior to 1.1.10.1, causing a fatal error. The function `shuffle(int[] input)` in the file `BitShuffle.java` receives an array of integers and applies a bit shuffle on it. It does so by multiplying the length by 4 and passing it to the natively compiled shuffle function. Since the length is not tested, the multiplication by four can cause an integer overflow and become a smaller value than the true size, or even zero or negative. In the case of a negative value, a `java.lang.NegativeArraySizeException` exception will raise, which can crash the program. In a case of a value that is zero or too small, the code that afterwards references the shuffled array will assume a bigger size of the array, which might cause exceptions such as `java.lang.ArrayIndexOutOfBoundsException`. The same issue exists also when using the `shuffle` functions that receive a double, float, long and short, each using a different multiplier that may cause the same issue. Version 1.1.10.1 contains a patch for this vulnerability.	5.9	More Details
CVE-2023-3316	A NULL pointer dereference in TIFFClose() is caused by a failure to open an output file (non-existent path or a path that requires permissions like /dev/null) while specifying zones.	5.9	More Details
CVE-2023-33213	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in gVectors Display Custom Fields – wpView plugin <= 1.3.0 versions.	5.9	More Details
CVE-2023-35779	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Seed Webs Seed Fonts plugin <= 2.3.1 versions.	5.9	More Details
CVE-2023-34454	snappy-java is a fast compressor/decompressor for Java. Due to unchecked multiplications, an integer overflow may occur in versions prior to 1.1.10.1, causing an unrecoverable fatal error. The function `compress(char[] input)` in the file `Snappy.java` receives an array of characters and compresses it. It does so by multiplying the length by 2 and passing it to the rawCompress` function. Since the length is not tested, the multiplication by two can cause an integer overflow and become negative. The rawCompress function then uses the received length and passes it to the natively compiled maxCompressedLength function, using the returned value to allocate a byte array. Since the maxCompressedLength function treats the length as an unsigned integer, it doesn't care that it is negative, and it returns a valid value, which is casted to a signed integer by the Java engine. If the result is negative, a `java.lang.NegativeArraySizeException` exception will be raised while trying to allocate the array `buf`. On the other side, if the result is positive, the `buf` array will successfully be allocated, but its size might be too small to use for the compression, causing a fatal Access Violation error. The same issue exists also when using the `compress` functions that receive double, float, int, long and short, each using a different multiplier that may cause the same issue. The issue most likely won't occur when using a byte array, since creating a byte array of size 0x80000000 (or any other negative value) is impossible in the first place. Version 1.1.10.1 contains a patch for this issue.	5.9	More Details
CVE-2023-25963	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in JoomSky JS Job Manager plugin <= 2.0.0 versions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25683	IBM PowerVM Hypervisor FW950.00 through FW950.71, FW1010.00 through FW1010.40, FW1020.00 through FW1020.20, and FW1030.00 through FW1030.11 could allow an attacker to obtain sensitive information if they gain service access to the HMC. IBM X-Force ID: 247592.	5.9	More Details
CVE-2023-26541	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Alexander Suess asMember plugin <= 1.5.4 versions.	5.9	More Details
CVE-2023-26515	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Ko Takagi Simple Slug Translate plugin <= 2.7.2 versions.	5.9	More Details
CVE-2023-25972	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in IKSWEB WordPress Старт plugin <= 3.7 versions.	5.9	More Details
CVE-2023-25974	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in psicosi448 wp2syslog plugin <= 1.0.5 versions.	5.9	More Details
CVE-2023-26527	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in WPIndeed Debug Assistant plugin <= 1.4 versions.	5.9	More Details
CVE-2023-26537	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in nicolly WP No External Links plugin <= 1.0.2 versions.	5.9	More Details
CVE-2023-35878	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Vadym K. Extra User Details plugin <= 0.5 versions.	5.9	More Details
CVE-2023-35095	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Flothemes Flo Forms – Easy Drag & Drop Form Builder plugin <= 1.0.40 versions.	5.9	More Details
CVE-2023-3228	Business Logic Errors in GitHub repository fossbilling/fossbilling prior to 0.5.0.	5.7	More Details
CVE-2023-3227	Insufficient Granularity of Access Control in GitHub repository fossbilling/fossbilling prior to 0.5.0.	5.7	More Details
CVE-2023-32020	Windows DNS Spoofing Vulnerability	5.6	More Details
CVE-2023-3022	A flaw was found in the IPv6 module of the Linux kernel. The arg.result was not used consistently in fib6_rule_lookup, sometimes holding rt6_info and other times fib6_info. This was not accounted for in other parts of the code where rt6_info was expected unconditionally, potentially leading to a kernel panic in fib6_rule_suppress.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29532	A local attacker can trick the Mozilla Maintenance Service into applying an unsigned update file by pointing the service at an update file on a malicious SMB server. The update file can be replaced after the signature check, before the use, because the write-lock requested by the service does not work on a SMB server. *Note: This attack requires local system access and only affects Windows. Other operating systems are not affected.* This vulnerability affects Firefox < 112, Firefox ESR < 102.10, and Thunderbird < 102.10.	5.5	More Details
CVE-2023-35866	In KeePassXC through 2.7.5, a local attacker can make changes to the Database security settings, including master password and second-factor authentication, within an authenticated KeePassXC Database session, without the need to authenticate these changes by entering the password and/or second-factor authentication to confirm changes. NOTE: the vendor's position is "asking the user for their password prior to making any changes to the database settings adds no additional protection against a local attacker."	5.5	More Details
CVE-2023-3220	An issue was discovered in the Linux kernel through 6.1-rc8. dpu_crtc_atomic_check in drivers/gpu/drm/msm/disp/dpu1/dpu_crtc.c lacks check of the return value of kzalloc() and will cause the NULL Pointer Dereference.	5.5	More Details
CVE-2023-21141	In several functions of several files, there is a possible way to access developer mode traces due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-262244249	5.5	More Details
CVE-2023-32016	Windows Installer Information Disclosure Vulnerability	5.5	More Details
CVE-2023-21137	In several methods of JobStore.java, uncaught exceptions in job map parsing could lead to local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-246541702	5.5	More Details
CVE-2023-21142	In multiple files, there is a possible way to access traces in the dev mode due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-262243665	5.5	More Details
CVE-2023-21143	In multiple functions of multiple files, there is a possible way to make the device unusable due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-268193777	5.5	More Details
CVE-2023-3276	A vulnerability, which was classified as problematic, has been found in Dromara HuTool up to 5.8.19. Affected by this issue is the function readBySax of the file XmlUtil.java of the component XML Parsing Module. The manipulation leads to xml external entity reference. The exploit has been disclosed to the public and may be used. VDB-231626 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-21569	Azure DevOps Server Spoofing Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21105	In multiple functions of ChooserActivity.java, there is a possible cross-user media read due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261036568	5.5	More Details
CVE-2023-26965	loadImage() in tools/tiffcrop.c in LibTIFF through 4.5.0 has a heap-based use after free via a crafted TIFF image.	5.5	More Details
CVE-2023-2976	Use of Java's default temporary directory for file creation in `FileBackedOutputStream` in Google Guava versions 1.0 to 31.1 on Unix systems and Android Ice Cream Sandwich allows other users and apps on the machine with access to the default Java temporary directory to be able to access the files created by the class. Even though the security vulnerability is fixed in version 32.0.0, we recommend using version 32.0.1 as version 32.0.0 breaks some functionality under Windows.	5.5	More Details
CVE-2023-34824	fdkaac before 1.0.5 was discovered to contain a heap buffer overflow in caf_info function in caf_reader.c.	5.5	More Details
CVE-2023-34823	fdkaac before 1.0.5 was discovered to contain a stack overflow in read_callback function in src/main.c.	5.5	More Details
CVE-2023-33139	Visual Studio Information Disclosure Vulnerability	5.5	More Details
CVE-2023-21136	In multiple functions of JobStore.java, there is a possible way to cause a crash on startup due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-246542285	5.5	More Details
CVE-2023-35789	An issue was discovered in the C AMQP client library (aka rabbitmq-c) through 0.13.0 for RabbitMQ. Credentials can only be entered on the command line (e.g., for amqp-publish or amqp-consume) and are thus visible to local attackers by listing a process and its arguments.	5.5	More Details
CVE-2023-30903	HP-UX could be exploited locally to create a Denial of Service (DoS) when any physical interface is configured with IPv6/inet6.	5.5	More Details
CVE-2023-29353	Sysinternals Process Monitor for Windows Denial of Service Vulnerability	5.5	More Details
CVE-2023-3308	A vulnerability classified as problematic has been found in whaleal IceFrog 1.1.8. Affected is an unknown function of the component Aviator Template Engine. The manipulation leads to deserialization. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-231804.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34474	A heap-based buffer overflow issue was discovered in ImageMagick's ReadTIM2ImageData() function in coders/tim2.c. A local attacker could trick the user in opening specially crafted file, triggering an out-of-bounds read error, allowing an application to crash, resulting in a denial of service.	5.5	More Details
CVE-2023-3195	A stack-based buffer overflow issue was found in ImageMagick's coders/tiff.c. This flaw allows an attacker to trick the user into opening a specially crafted malicious tiff file, causing an application to crash, resulting in a denial of service.	5.5	More Details
CVE-2023-34475	A heap use after free issue was discovered in ImageMagick's ReplaceXmpValue() function in MagickCore/profile.c. An attacker could trick user to open a specially crafted file to convert, triggering an heap-use-after-free write error, allowing an application to crash, resulting in a denial of service.	5.5	More Details
CVE-2023-30904	A security vulnerability in HPE Insight Remote Support may result in the local disclosure of privileged LDAP information.	5.5	More Details
CVE-2023-34797	Broken access control in the Registration page (/Registration.aspx) of Termenos CWX v8.5.6 allows attackers to access sensitive information.	5.4	More Details
CVE-2023-33438	A stored Cross-site scripting (XSS) vulnerability in Wolters Kluwer TeamMate+ 35.0.11.0 allows remote attackers to inject arbitrary web script or HTML.	5.4	More Details
CVE-2023-34565	Netbox 3.5.1 is vulnerable to Cross Site Scripting (XSS) in the "Create Wireless LAN Groups" function.	5.4	More Details
CVE-2023-2899	The Google Map Shortcode WordPress plugin through 3.1.2 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admin	5.4	More Details
CVE-2023-29322	Adobe Experience Manager versions 6.5.16.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2023-34452	Grav is a flat-file content management system. In versions 1.7.42 and prior, the "/forgot_password" page has a self-reflected cross-site scripting vulnerability that can be exploited by injecting a script into the "email" parameter of the request. While this vulnerability can potentially allow an attacker to execute arbitrary code on the user's browser, the impact is limited as it requires user interaction to trigger the vulnerability. As of time of publication, a patch is not available. Server-side validation should be implemented to prevent this vulnerability.	5.4	More Details
CVE-2023-34373	Cross-Site Request Forgery (CSRF) vulnerability in Dylan James Zephyr Project Manager plugin <= 3.3.93 versions.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29307	Adobe Experience Manager versions 6.5.16.0 (and earlier) is affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction.	5.4	More Details
CVE-2023-29304	Adobe Experience Manager versions 6.5.16.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2023-29302	Adobe Experience Manager versions 6.5.16.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2023-25450	Cross-Site Request Forgery (CSRF) vulnerability in GiveWP GiveWP – Donation Plugin and Fundraising Platform plugin <= 2.25.1 versions.	5.4	More Details
CVE-2023-34845	Bludit v3.14.1 was discovered to contain an arbitrary file upload vulnerability in the component /admin/new-content. This vulnerability allows attackers to execute arbitrary web scripts or HTML via uploading a crafted SVG file. NOTE: the product's security model is that users are trusted by the administrator to insert arbitrary content (users cannot create their own accounts through self-registration).	5.4	More Details
CVE-2023-33515	SoftExpert Excellence Suite 2.1.9 is vulnerable to Cross Site Scripting (XSS) via query screens.	5.4	More Details
CVE-2023-35145	Jenkins Sonargraph Integration Plugin 5.0.1 and earlier does not escape the file path and the project name for the Log file field form validation, resulting in a stored cross-site scripting vulnerability exploitable by attackers with Item/Configure permission.	5.4	More Details
CVE-2023-35146	Jenkins Template Workflows Plugin 41.v32d86a_313b_4a and earlier does not escape names of jobs used as buildings blocks for Template Workflow Job, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to create jobs.	5.4	More Details
CVE-2020-21246	Cross Site Scripting vulnerability in YiiCMS v.1.0 allows a remote attacker to execute arbitrary code via the news function.	5.4	More Details
CVE-2023-30453	The Teamlead Reminder plugin through 2.6.5 for Jira allows persistent XSS via the message parameter.	5.4	More Details
CVE-2023-35143	Jenkins Maven Repository Server Plugin 1.10 and earlier does not escape the versions of build artifacts on the Build Artifacts As Maven Repository page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control maven project versions in `pom.xml`.	5.4	More Details
CVE-2023-35144	Jenkins Maven Repository Server Plugin 1.10 and earlier does not escape project and build display names on the Build Artifacts As Maven Repository page, resulting in a stored cross-site scripting (XSS) vulnerability.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0368	The Responsive Tabs For WPBakery Page Builder (formerly Visual Composer) WordPress plugin through 1.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-0489	The SlideOnline WordPress plugin through 1.2.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2023-0010	A reflected cross-site scripting (XSS) vulnerability in the Captive Portal feature of Palo Alto Networks PAN-OS software can allow a JavaScript payload to be executed in the context of an authenticated Captive Portal user's browser when they click on a specifically crafted link.	5.4	More Details
CVE-2022-48488	Vulnerability of bypassing the default desktop security controls.Successful exploitation of this vulnerability may cause unauthorized modifications to the desktop.	5.3	More Details
CVE-2023-34160	Vulnerability of spoofing trustlists of Huawei desktop.Successful exploitation of this vulnerability can cause third-party apps to hide app icons on the desktop to prevent them from being uninstalled.	5.3	More Details
CVE-2023-34459	OpenZeppelin Contracts is a library for smart contract development. Starting in version 4.7.0 and prior to version 4.9.2, when the `verifyMultiProof`, `verifyMultiProofCalldata`, `procesprocessMultiProof`, or `processMultiProofCalldat` functions are in use, it is possible to construct merkle trees that allow forging a valid multiproof for an arbitrary set of leaves. A contract may be vulnerable if it uses multiproofs for verification and the merkle tree that is processed includes a node with value 0 at depth 1 (just under the root). This could happen inadvertedly for balanced trees with 3 leaves or less, if the leaves are not hashed. This could happen deliberately if a malicious tree builder includes such a node in the tree. A contract is not vulnerable if it uses single-leaf proving (`verify`, `verifyCalldata`, `processProof`, or `processProofCalldata`), or if it uses multiproofs with a known tree that has hashed leaves. Standard merkle trees produced or validated with the @openzeppelin/merkle-tree library are safe. The problem has been patched in version 4.9.2. Some workarounds are available. For those using multiproofs: When constructing merkle trees hash the leaves and do not insert empty nodes in your trees. Using the @openzeppelin/merkle-tree package eliminates this issue. Do not accept user-provided merkle roots without reconstructing at least the first level of the tree. Verify the merkle tree structure by reconstructing it from the leaves.	5.3	More Details
CVE-2023-34167	Vulnerability of spoofing trustlists of Huawei desktop.Successful exploitation of this vulnerability can cause third-party apps to hide app icons on the desktop to prevent them from being uninstalled.	5.3	More Details
CVE-2023-29287	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Information Exposure vulnerability that could lead to a security feature bypass. An attacker could leverage this vulnerability to leak minor user data. Exploitation of this issue does not require user interaction..	5.3	More Details
CVE-2023-32208	Service workers could reveal script base URL due to dynamic `import()`. This vulnerability affects Firefox < 113.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48491	Vulnerability of missing authentication on certain HUAWEI phones.Successful exploitation of this vulnerability can lead to ads and other windows to display at any time.	5.3	More Details
CVE-2022-48495	Vulnerability of unauthorized access to foreground app information.Successful exploitation of this vulnerability may cause foreground app information to be obtained.	5.3	More Details
CVE-2023-34165	Unauthorized access vulnerability in the Save for later feature provided by AI Touch.Successful exploitation of this vulnerability may cause third-party apps to forge a URI for unauthorized access with zero permissions.	5.3	More Details
CVE-2023-34156	Vulnerability of services denied by early fingerprint APIs on HarmonyOS products.Successful exploitation of this vulnerability may cause services to be denied.	5.3	More Details
CVE-2022-33163	IBM Security Directory Suite VA 8.0.1 specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors. IBM X-Force ID: 228571.	5.3	More Details
CVE-2023-1999	There exists a use after free/double free in libwebp. An attacker can use the ApplyFiltersAndEncode() function and loop through to free best.bw and assign best = trial pointer. The second loop will then return 0 because of an Out of memory error in VP8 encoder, the pointer is still assigned to trial and the AddressSanitizer will attempt a double free.	5.3	More Details
CVE-2023-2683	A memory leak in the EFR32 Bluetooth LE stack 5.1.0 through 5.1.1 allows an attacker to send an invalid pairing message and cause future legitimate connection attempts to fail. A reset of the device immediately clears the error.	5.3	More Details
CVE-2022-33159	IBM Security Directory Suite VA 8.0.1 through 8.0.1.19 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 228567.	5.3	More Details
CVE-2023-32013	Windows Hyper-V Denial of Service Vulnerability	5.3	More Details
CVE-2023-29355	DHCP Server Service Information Disclosure Vulnerability	5.3	More Details
CVE-2023-34158	Vulnerability of spoofing trustlists of Huawei desktop.Successful exploitation of this vulnerability can cause third-party apps to hide app icons on the desktop to prevent them from being uninstalled.	5.3	More Details
CVE-2023-34449	ink! is an embedded domain specific language to write smart contracts in Rust for blockchains built on the Substrate framework. Starting in version 4.0.0 and prior to version 4.2.1, the return value when using delegate call mechanics, either through `CallBuilder::delegate` or `ink_env::invoke_contract_delegate`, is decoded incorrectly. This bug was related to the mechanics around decoding a call's return buffer, which was changed as part of pull request 1450. Since this feature was only released in ink! 4.0.0, no previous versions are affected. Users who have an ink! 4.x series contract should upgrade to 4.2.1 to receive a patch.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2751	The Upload Resume WordPress plugin through 1.2.0 does not validate the captcha parameter when uploading a resume via the resume_upload_form shortcode, allowing unauthenticated visitors to upload arbitrary media files to the site.	5.3	More Details
CVE-2023-29290	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. An attacker could leverage this vulnerability to bypass a minor functionality. Exploitation of this issue does not require user interaction.	5.3	More Details
CVE-2023-25186	An issue was discovered on NOKIA Airscale ASIKA Single RAN devices before 21B. If/when CSP (as a BTS administrator) removes security hardenings from a Nokia Single RAN BTS baseband unit, a directory path traversal in the Nokia BTS baseband unit diagnostic tool AaShell (which is by default disabled) provides access to the BTS baseband unit internal filesystem from the mobile network solution internal BTS management network.	5.1	More Details
CVE-2023-25188	An issue was discovered on NOKIA Airscale ASIKA Single RAN devices before 21B. If/when CSP (as a BTS administrator) removes security hardenings from the Nokia Single RAN BTS baseband unit, the BTS baseband unit diagnostic tool AaShell (which is by default disabled) allows unauthenticated access from the mobile network solution internal BTS management network to the BTS embedded Linux operating-system level.	5.1	More Details
CVE-2023-26435	It was possible to call filesystem and network references using the local LibreOffice instance using manipulated ODT documents. Attackers could discover restricted network topology and services as well as including local files with read permissions of the open-xchange system user. This was limited to specific file-types, like images. We have improved existing content filters and validators to avoid including any local resources. No publicly available exploits are known.	5.0	More Details
CVE-2023-26431	IPv4-mapped IPv6 addresses did not get recognized as "local" by the code and a connection attempt is made. Attackers with access to user accounts could use this to bypass existing deny-list functionality and trigger requests to restricted network infrastructure to gain insight about topology and running services. We now respect possible IPV4-mapped IPv6 addresses when checking if contained in a deny-list. No publicly available exploits are known.	5.0	More Details
CVE-2023-29291	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. An admin-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require user interaction.	4.9	More Details
CVE-2023-29292	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. An admin-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require user interaction.	4.9	More Details
CVE-2023-32229	Due to an error in the software interface to the secure element chip on Bosch IP cameras of family CPP13 and CPP14, the chip can be permanently damaged when enabling the Stream security option (signing of the video stream) with option MD5, SHA-1 or SHA-256.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-20697	Cross Site Scripting vulnerability in khodakhah NodCMS v.3.0 allows a remote attacker to execute arbitrary code and gain access to senstivie information via a crafted script to the address parameter.	4.8	More Details
CVE-2023-34657	A stored cross-site scripting (XSS) vulnerability in Eyoucms v1.6.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the web_recordnum parameter.	4.8	More Details
CVE-2023-2812	The Ultimate Dashboard WordPress plugin before 3.7.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-2811	The AI ChatBot WordPress plugin before 4.5.6 does not sanitise and escape numerous of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks to all admin when setting chatbot and all client when using chatbot	4.8	More Details
CVE-2023-2742	The AI ChatBot WordPress plugin before 4.5.5 does not sanitize and escape its settings, allowing high-privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2023-2684	The File Renaming on Upload WordPress plugin before 2.5.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-3293	Cross-site Scripting (XSS) - Stored in GitHub repository salesagility/suitecrm-core prior to 8.3.0.	4.8	More Details
CVE-2023-2401	The QuBot WordPress plugin before 1.1.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-2527	The Integration for Contact Form 7 and Zoho CRM, Bigin WordPress plugin before 1.2.4 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	4.8	More Details
CVE-2023-2600	The Custom Base Terms WordPress plugin before 1.0.3 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-32019	Windows Kernel Information Disclosure Vulnerability	4.7	More Details
CVE-2023-21095	In canStartSystemGesture of RecentsAnimationDeviceState.java, there is a possible partial lockscreen bypass due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12L Android-13Android ID: A-242704576	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35116	jackson-databind through 2.15.2 allows attackers to cause a denial of service or other unspecified impact via a crafted object that uses cyclic dependencies. NOTE: the vendor's perspective is that this is not a valid vulnerability report, because the steps of constructing a cyclic data structure and trying to serialize it cannot be achieved by an external attacker.	4.7	More Details
CVE-2023-34461	PyBB is an open source bulletin board. A manual code review of the PyBB bulletin board server has revealed that a vulnerability could have been exploited in which users could submit any type of HTML tag, and have said tag run. For example, a malicious `<a>` that looks like ```xss``` could have been used to run code through JavaScript on the client side. The problem has been patched as of commit `5defd92`, and users are advised to upgrade. Attackers do need posting privilege in order to exploit this vulnerability. This vulnerability is present within the 0.1.0 release, and users are advised to upgrade to 0.1.1. Users unable to upgrade may be able to work around the attack by either; Removing the ability to create posts, removing the `|safe` tag from the Jinja2 template titled "post.html" in templates or by adding manual validation of links in the post creation section.	4.6	More Details
CVE-2022-22307	IBM Security Guardium 11.3, 11.4, and 11.5 could allow a local user to obtain elevated privileges due to incorrect authorization checks. IBM X-Force ID: 216753.	4.4	More Details
CVE-2023-3201	The MStore API plugin for WordPress is vulnerable to Cross-Site Request Forgery due to missing nonce validation on the mstore_update_new_order_title function. This makes it possible for unauthenticated attackers to update new order title via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-3203	The MStore API plugin for WordPress is vulnerable to Cross-Site Request Forgery due to missing nonce validation on the mstore_update_limit_product function. This makes it possible for unauthenticated attackers to update limit the number of product per category to use cache data in home screen via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-28810	Some access control/intercom products have unauthorized modification of device network configuration vulnerabilities. Attackers can modify device network configuration by sending specific data packets to the vulnerable interface within the same local network.	4.3	More Details
CVE-2023-34149	Allocation of Resources Without Limits or Throttling vulnerability in Apache Software Foundation Apache Struts.This issue affects Apache Struts: through 2.5.30, through 6.1.2. Upgrade to Struts 2.5.31 or 6.1.2.1 or greater.	4.3	More Details
CVE-2023-2783	Mattermost Apps Framework fails to verify that a secret provided in the incoming webhook request allowing an attacker to modify the contents of the post sent by the Apps.	4.3	More Details
CVE-2023-2831	Mattermost fails to unescape Markdown strings in a memory-efficient way, allowing an attacker to cause a Denial of Service by sending a message containing a large number of escaped characters.	4.3	More Details
CVE-2023-2786	Mattermost fails to properly check the permissions when executing commands allowing a member with no permissions to post a message in a channel to actually post it by executing channel commands.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2791	When creating a playbook run via the /dialog API, Mattermost fails to validate all parameters, allowing an authenticated attacker to edit an arbitrary channel post.	4.3	More Details
CVE-2023-2785	Mattermost fails to properly truncate the postgres error log message of a search query failure allowing an attacker to cause the creation of large log files which can result in Denial of Service	4.3	More Details
CVE-2023-3234	A vulnerability was found in Zhong Bang CRMEB up to 4.6.0. It has been declared as problematic. Affected by this vulnerability is the function put_image of the file api/controller/v1/PublicController.php. The manipulation leads to deserialization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-231505 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-29288	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A privileged attacker could leverage this vulnerability to modify a minor functionality of another user's data. Exploitation of this issue does not require user interaction.	4.3	More Details
CVE-2023-26434	When adding an external mail account, processing of POP3 "capabilities" responses are not limited to plausible sizes. Attacker with access to a rogue POP3 service could trigger requests that lead to excessive resource usage and eventually service unavailability. We now limit accepted POP3 server response to reasonable length/size. No publicly available exploits are known.	4.3	More Details
CVE-2023-26433	When adding an external mail account, processing of IMAP "capabilities" responses are not limited to plausible sizes. Attacker with access to a rogue IMAP service could trigger requests that lead to excessive resource usage and eventually service unavailability. We now limit accepted IMAP server response to reasonable length/size. No publicly available exploits are known.	4.3	More Details
CVE-2023-25449	Cross-Site Request Forgery (CSRF) vulnerability in Oliver Seidel, Bastian Germann cformsII plugin <= 15.0.4 versions.	4.3	More Details
CVE-2023-34626	Piwigo 13.7.0 is vulnerable to SQL Injection via the "Users" function.	4.3	More Details
CVE-2023-25055	Cross-Site Request Forgery (CSRF) vulnerability in Amit Agarwal Google XML Sitemap for Videos plugin <= 2.6.1 versions.	4.3	More Details
CVE-2023-29294	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by a Business Logic Errors vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass a minor functionality. Exploitation of this issue does not require user interaction.	4.3	More Details
CVE-2023-29295	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass a minor functionality. Exploitation of this issue does not require user interaction.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26432	When adding an external mail account, processing of SMTP "capabilities" responses are not limited to plausible sizes. Attacker with access to a rogue SMTP service could trigger requests that lead to excessive resource usage and eventually service unavailability. We now limit accepted SMTP server response to reasonable length/size. No publicly available exploits are known.	4.3	More Details
CVE-2023-23802	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes HT Easy GA4 (Google Analytics 4) plugin <= 1.0.6 versions.	4.3	More Details
CVE-2023-34396	Allocation of Resources Without Limits or Throttling vulnerability in Apache Software Foundation Apache Struts.This issue affects Apache Struts: through 2.5.30, through 6.1.2. Upgrade to Struts 2.5.31 or 6.1.2.1 or greater	4.3	More Details
CVE-2023-29296	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to modify a minor functionality of another user's data. Exploitation of this issue does not require user interaction.	4.3	More Details
CVE-2023-3315	Missing permission checks in Jenkins Team Concert Plugin 2.4.1 and earlier allow attackers with Overall/Read permission to check for the existence of an attacker-specified file path on the Jenkins controller file system.	4.3	More Details
CVE-2023-3198	The MStore API plugin for WordPress is vulnerable to Cross-Site Request Forgery due to missing nonce validation on the mstore_update_status_order_message function. This makes it possible for unauthenticated attackers to update status order message via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-2819	A stored cross-site scripting vulnerability in the Sources UI in Proofpoint Threat Response/ Threat Response Auto Pull (PTR/TRAP) could allow an authenticated administrator on an adjacent network to replace the image file with an arbitrary MIME type. This could result in arbitrary javascript code execution in an admin context. All versions prior to 5.10.0 are affected.	4.3	More Details
CVE-2023-3200	The MStore API plugin for WordPress is vulnerable to Cross-Site Request Forgery due to missing nonce validation on the mstore_update_new_order_message function. This makes it possible for unauthenticated attackers to update new order message via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-2784	Mattermost fails to verify if the requestor is a sysadmin or not, before allowing `install` requests to the Apps allowing a regular user send install requests to the Apps.	4.2	More Details
CVE-2023-25185	An issue was discovered on NOKIA Airscale ASIKA Single RAN devices before 21B. A mobile network solution internal fault was found in Nokia Single RAN software releases. Certain software processes in the BTS internal software design have unnecessarily high privileges to BTS embedded operating system (OS) resources.	3.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3040	A debug function in the lua-resty-json package, up to commit id 3ef9492bd3a44d9e51301d6adc3cd1789c8f534a (merged in PR #14) contained an out of bounds access bug that could have allowed an attacker to launch a DoS if the function was used to parse untrusted input data. It is important to note that because this debug function was only used in tests and demos, it was not exploitable in a normal environment.	3.7	More Details
CVE-2023-3189	A vulnerability, which was classified as problematic, was found in SourceCodester Online School Fees System 1.0. This affects an unknown part of the file /paysystem/branch.php of the component POST Parameter Handler. The manipulation of the argument branch leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-231501 was assigned to this vulnerability.	3.5	More Details
CVE-2023-3318	A vulnerability was found in SourceCodester Resort Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation of the argument page leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-231937 was assigned to this vulnerability.	3.5	More Details
CVE-2023-26429	Control characters were not removed when exporting user feedback content. This allowed attackers to include unexpected content via user feedback and potentially break the exported data structure. We now drop all control characters that are not whitespace character during the export. No publicly available exploits are known.	3.5	More Details
CVE-2023-3309	A vulnerability classified as problematic was found in SourceCodester Resort Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file ?page=rooms of the component Manage Room Page. The manipulation of the argument Cottage Number leads to cross site scripting. The attack can be launched remotely. The identifier VDB-231805 was assigned to this vulnerability.	3.5	More Details
CVE-2023-3241	A vulnerability was found in OTCMS up to 6.62 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/read.php?mudi=announContent. The manipulation of the argument url leads to path traversal. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-231512.	3.5	More Details
CVE-2023-3240	A vulnerability has been found in OTCMS up to 6.62 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file usersNews_deal.php. The manipulation of the argument file leads to path traversal: '../filedir'. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-231511.	3.5	More Details
CVE-2023-3239	A vulnerability, which was classified as problematic, was found in OTCMS up to 6.62. Affected is an unknown function of the file admin/readDeal.php?mudi=readQrCode. The manipulation of the argument img leads to path traversal: '../filedir'. The exploit has been disclosed to the public and may be used. VDB-231510 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-2431	A security issue was discovered in Kubelet that allows pods to bypass the seccomp profile enforcement. Pods that use localhost type for seccomp profile but specify an empty profile field, are affected by this issue. In this scenario, this vulnerability allows the pod to run in unconfined (seccomp disabled) mode. This bug affects Kubelet.	3.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34242	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to version 1.13.4, when Gateway API is enabled in Cilium, the absence of a check on the namespace in which a ReferenceGrant is created could result in Cilium unintentionally gaining visibility of secrets (including certificates) and services across namespaces. An attacker on an affected cluster can leverage this issue to use cluster secrets that should not be visible to them, or communicate with services that they should not have access to. Gateway API functionality is disabled by default. This vulnerability is fixed in Cilium release 1.13.4. As a workaround, restrict the creation of `ReferenceGrant` resources to admin users by using Kubernetes RBAC.	3.4	More Details
CVE-2023-3291	Heap-based Buffer Overflow in GitHub repository gpac/gpac prior to 2.2.2.	3.3	More Details
CVE-2023-26427	Default permissions for a properties file were too permissive. Local system users could read potentially sensitive information. We updated the default permissions for noreply.properties set during package installation. No publicly available exploits are known.	3.2	More Details
CVE-2023-2797	Mattermost fails to sanitize code permalinks, allowing an attacker to preview code from private repositories by posting a specially crafted permalink on a channel.	3.1	More Details
CVE-2023-3231	A vulnerability has been found in UJCMS up to 6.0.2 and classified as problematic. This vulnerability affects unknown code of the component ZIP Package Handler. The manipulation of the argument dir leads to information disclosure. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. Upgrading to version 7.0.0 is able to address this issue. It is recommended to upgrade the affected component. VDB-231502 is the identifier assigned to this vulnerability.	3.1	More Details
CVE-2023-34414	The error page for sites with invalid TLS certificates was missing the activation-delay Firefox uses to protect prompts and permission dialogs from attacks that exploit human response time delays. If a malicious page elicited user clicks in precise locations immediately before navigating to a site with a certificate error and made the renderer extremely busy at the same time, it could create a gap between when the error page was loaded and when the display actually refreshed. With the right timing the elicited clicks could land in that gap and activate the button that overrides the certificate error for that site. This vulnerability affects Firefox ESR < 102.12, Firefox < 114, and Thunderbird < 102.12.	3.1	More Details
CVE-2023-2747	The initialization vector (IV) used by the secure engine (SE) for encrypting data stored in the SE flash memory is uninitialized.	3.1	More Details
CVE-2023-32024	Microsoft Power Apps Spoofing Vulnerability	3.0	More Details
CVE-2023-2400	Improper deletion of resource in the user management feature in Devolutions Server 2023.1.8 and earlier allows an administrator to view users vaults of deleted users via database access.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29293	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An admin privileged attacker could leverage this vulnerability to impact the availability of a user's minor feature. Exploitation of this issue does not require user interaction.	2.7	More Details
CVE-2022-48506	A flawed pseudorandom number generator in Dominion Voting Systems ImageCast Precinct (ICP and ICP2) and ImageCast Evolution (ICE) scanners allows anyone to determine the order in which ballots were cast from public ballot-level data, allowing deanonymization of voted ballots, in several types of scenarios. This issue was observed for use of the following versions of Democracy Suite: 5.2, 5.4-NM, 5.5, 5.5-A, 5.5-B, 5.5-C, 5.5-D, 5.7-A, 5.10, 5.10A, 5.15. NOTE: the Democracy Suite 5.17 EAC Certificate of Conformance mentions "Improved pseudo random number algorithm," which may be relevant.	2.4	More Details
CVE-2023-3311	A vulnerability, which was classified as problematic, was found in PuneethReddyHC online-shopping-system-advanced 1.0. This affects an unknown part of the file addsuppliers.php. The manipulation of the argument First name 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-231807.	2.4	More Details
CVE-2023-34585	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-4284	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-2918	Rejected reason: Duplicate Assignment.	N/A	More Details
CVE-2023-35825	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-3141. Reason: This candidate is a reservation duplicate of CVE-2023-3141. Notes: All CVE users should reference CVE-2023-3141 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details