SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 08 November 2023

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-42802	GLPI is a free asset and IT management software package. Starting in version 10.0.7 and prior to version 10.0.10, an unverified object instantiation allows one to upload malicious PHP files to unwanted directories. Depending on web server configuration and available system libraries, malicious PHP files can then be executed through a web server request. Version 10.0.10 fixes this issue. As a workaround, remove write access on `/ajax` and `/front` files to the web server.	10.0	More Details
CVE-2023-25960	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Zendrop Zendrop – Global Dropshipping zendrop-dropshipping-and-fulfillment allows SQL Injection.This issue affects Zendrop – Global Dropshipping: from n/a through 1.0.0.	10.0	More Details
CVE-2023-46731	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki doesn't properly escape the section URL parameter that is used in the code for displaying administration sections. This allows any user with read access to the document `XWiki.AdminSheet` (by default, everyone including unauthenticated users) to execute code including Groovy code. This impacts the confidentiality, integrity and availability of the whole XWiki instance. This vulnerability has been patched in XWiki 14.10.14, 15.6 RC1 and 15.5.1. Users are advised to upgrade. Users unablr to upgrade may apply the fix in commit `fec8e0e53f9` manually. Alternatively, to protect against attacks from unauthenticated users, view right for guests can be removed from this document (it is only needed for space and wiki admins).	10.0	More Details
CVE-2023-4699	Missing Authentication for Critical Function vulnerability in Mitsubishi Electric Corporation MELSEC-F Series CPU modules, MELSEC iQ-F Series, MELSEC iQ-R series CPU modules, MELSEC iQ-R series, MELSEC iQ-L series, MELSEC Q series, MELSEC-L series, Mitsubishi Electric CNC M800V/M80V series, Mitsubishi Electric CNC M800/M80/E80 series and Mitsubishi Electric CNC M700V/M70V/E70 series allows a remote unauthenticated attacker to execute arbitrary commands by sending specific packets to the affected products. This could lead to disclose or tamper with information by reading or writing control programs, or cause a denial-of-service (DoS) condition on the products by resetting the memory contents of the products to factory settings or resetting the products remotely.	10.0	More Details
CVE-2023-5964	The 1E-Exchange-DisplayMessageinstruction that is part of the End-User Interaction product pack available on the 1E Exchange does not properly validate the Caption or Message parameters, which allows for a specially crafted input to perform arbitrary code execution with SYSTEM permissions. This instruction only runs on Windows clients. To remediate this issue DELETE the instruction “Show dialogue with caption %Caption% and message %Message%” from the list of instructions in the Settings UI, and replace it with the new instruction 1E-Exchange-ShowNotification instruction available in the updated End-User Interaction product pack. The new instruction should show as “Show %Type% type notification with header %Header% and message %Message%” with a version of 7.1 or above.	9.9	More Details
CVE-2023-45163	The 1E-Exchange-CommandLinePing instruction that is part of the Network product pack available on the 1E Exchange does not properly validate the input parameter, which allows for a specially crafted input to perform arbitrary code execution with SYSTEM permissions. This instruction only runs on Windows clients. To remediate this issue download the updated Network product pack from the 1E Exchange and update the 1E-Exchange-CommandLinePing instruction to v18.1 by uploading it through the 1E Platform instruction upload UI	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45161	The 1E-Exchange-URLResponseTime instruction that is part of the Network product pack available on the 1E Exchange does not properly validate the URL parameter, which allows for a specially crafted input to perform arbitrary code execution with SYSTEM permissions. This instruction only runs on Windows clients. To remediate this issue download the updated Network product pack from the 1E Exchange and update the 1E-Exchange-URLResponseTime instruction to v20.1 by uploading it through the 1E Platform instruction upload UI	9.9	More Details
CVE-2023-46404	PCRS <= 3.11 (d0de1e) “Questions” page and “Code editor” page are vulnerable to remote code execution (RCE) by escaping Python sandboxing.	9.9	More Details
CVE-2023-46243	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions it's possible for a user to execute any content with the right of an existing document's content author, provided the user have edit right on it. A crafted URL of the form ` /xwiki/bin/edit//?content=%7B%7Bgroovy%7D%7Dprintln%28%22Hello+from+Groovy%21%22%29%7B%7B%2Fgroovy%7D%7D&xpage=view` can be used to execute arbitrary groovy code on the server. This vulnerability has been patched in XWiki versions 14.10.6 and 15.2RC1. Users are advised to update. There are no known workarounds for this issue.	9.9	More Details
CVE-2023-20048	A vulnerability in the web services interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute certain unauthorized configuration commands on a Firepower Threat Defense (FTD) device that is managed by the FMC Software. This vulnerability is due to insufficient authorization of configuration commands that are sent through the web service interface. An attacker could exploit this vulnerability by authenticating to the FMC web services interface and sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to execute certain configuration commands on the targeted FTD device. To successfully exploit this vulnerability, an attacker would need valid credentials on the FMC Software.	9.9	More Details
CVE-2022-46849	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Weblizar Coming Soon Page – Responsive Coming Soon & Maintenance Mode allows SQL Injection.This issue affects Coming Soon Page – Responsive Coming Soon & Maintenance Mode: from n/a through 1.5.9.	9.8	More Details
CVE-2023-40609	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Aiyaz, maheshpatel Contact form 7 Custom validation allows SQL Injection.This issue affects Contact form 7 Custom validation: from n/a through 1.1.3.	9.8	More Details
CVE-2023-45657	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in POSIMYTH Nexter allows SQL Injection.This issue affects Nexter: from n/a through 2.0.3.	9.8	More Details
CVE-2023-45074	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Page Visit Counter Advanced Page Visit Counter – Most Wanted Analytics Plugin for WordPress allows SQL Injection.This issue affects Advanced Page Visit Counter – Most Wanted Analytics Plugin for WordPress: from n/a through 7.1.1.	9.8	More Details
CVE-2023-45069	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Video Gallery by Total-Soft Video Gallery – Best WordPress YouTube Gallery Plugin allows SQL Injection.This issue affects Video Gallery – Best WordPress YouTube Gallery Plugin: from n/a through 2.1.3.	9.8	More Details
CVE-2023-45055	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in InspireUI MStore API allows SQL Injection.This issue affects MStore API: from n/a through 4.0.6.	9.8	More Details
CVE-2023-45046	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pressference Pressference Exporter allows SQL Injection.This issue affects Pressference Exporter: from n/a through 1.0.3.	9.8	More Details
CVE-2023-45001	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Castos Seriously Simple Stats allows SQL Injection.This issue affects Seriously Simple Stats: from n/a through 1.5.0.	9.8	More Details
CVE-2023-41685	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ilGhera Woocommerce Support System allows SQL Injection.This issue affects Woocommerce Support System: from n/a through 1.2.1.	9.8	More Details
CVE-2023-35911	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Creative Solutions Contact Form Generator : Creative form builder for WordPress allows SQL Injection.This issue affects Contact Form Generator : Creative form builder for WordPress: from n/a through 2.6.0.	9.8	More Details
CVE-2023-40207	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RedNao Donations Made Easy – Smart Donations allows SQL Injection.This issue affects Donations Made Easy – Smart Donations: from n/a through 4.0.12.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38382	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Daniel Söderström / Sidney van de Stouwe Subscribe to Category allows SQL Injection.This issue affects Subscribe to Category: from n/a through 2.7.4.	9.8	More Details
CVE-2023-5777	Weintek EasyBuilder Pro contains a vulnerability that, even when the private key is immediately deleted after the crash report transmission is finished, the private key is exposed to the public, which could result in obtaining remote control of the crash report server.	9.8	More Details
CVE-2023-33924	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Felix Welberg SIS Handball allows SQL Injection.This issue affects SIS Handball: from n/a through 1.0.45.	9.8	More Details
CVE-2023-28748	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in biztechc Copy or Move Comments allows SQL Injection.This issue affects Copy or Move Comments: from n/a through 5.0.4.	9.8	More Details
CVE-2023-27605	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Sajjad Hossain WP Reroute Email allows SQL Injection.This issue affects WP Reroute Email: from n/a through 1.4.6.	9.8	More Details
CVE-2022-47432	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Kemal YAZICI - PluginPress Shortcode IMDB allows SQL Injection.This issue affects Shortcode IMDB: from n/a through 6.0.8.	9.8	More Details
CVE-2022-47430	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Weblizar The School Management – Education & Learning Management allows SQL Injection.This issue affects The School Management – Education & Learning Management: from n/a through 4.1.	9.8	More Details
CVE-2022-47428	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WpDevArt Booking calendar, Appointment Booking System allows SQL Injection.This issue affects Booking calendar, Appointment Booking System: from n/a through 3.2.7.	9.8	More Details
CVE-2022-47420	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Online ADA Accessibility Suite by Online ADA allows SQL Injection.This issue affects Accessibility Suite by Online ADA: from n/a through 4.12.	9.8	More Details
CVE-2022-46860	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in KaizenCoders Short URL allows SQL Injection.This issue affects Short URL: from n/a through 1.6.4.	9.8	More Details
CVE-2022-45373	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Jason Crouse, VeronaLabs Slimstat Analytics allows SQL Injection.This issue affects Slimstat Analytics: from n/a through 5.0.4.	9.8	More Details
CVE-2023-2675	Improper Restriction of Excessive Authentication Attempts in GitHub repository linagora/twake prior to 2023.Q1.1223.	9.8	More Details
CVE-2023-5601	The WooCommerce Ninja Forms Product Add-ons WordPress plugin before 1.7.1 does not validate the file to be uploaded, allowing any unauthenticated users to upload arbitrary files to the server, leading to RCE.	9.8	More Details
CVE-2022-45360	Improper Neutralization of Formula Elements in a CSV File vulnerability in Scott Reilly Commenter Emails.This issue affects Commenter Emails: from n/a through 2.6.1.	9.8	More Details
CVE-2023-46793	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'day' parameter in the 'register()' function of the functions.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-46789	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'filename' attribute of the 'pic1' multipart parameter of the functions.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-46788	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'id' parameter in the 'uploadphoto()' function of the functions.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-46787	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'username' parameter of the auth/auth.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46785	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'id' parameter of the partner_preference.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-46679	Online Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txt_uname_email' parameter of the index.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-46677	Online Job Portal v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'txt_uname' parameter of the sign-up.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2022-46809	Improper Neutralization of Formula Elements in a CSV File vulnerability in WPDeveloper ReviewX – Multi-criteria Rating & Reviews for WooCommerce.This issue affects ReviewX – Multi-criteria Rating & Reviews for WooCommerce: from n/a through 1.6.7.	9.8	More Details
CVE-2022-46803	Improper Neutralization of Formula Elements in a CSV File vulnerability in Noptin Newsletter Simple Newsletter Plugin – Noptin.This issue affects Simple Newsletter Plugin – Noptin: from n/a through 1.9.5.	9.8	More Details
CVE-2022-46801	Improper Neutralization of Formula Elements in a CSV File vulnerability in Paul Ryley Site Reviews.This issue affects Site Reviews: from n/a through 6.2.0.	9.8	More Details
CVE-2022-45810	Improper Neutralization of Formula Elements in a CSV File vulnerability in Icegram Icegram Express – Email Marketing, Newsletters and Automation for WordPress & WooCommerce.This issue affects Icegram Express – Email Marketing, Newsletters and Automation for WordPress & WooCommerce: from n/a through 5.5.2.	9.8	More Details
CVE-2022-45370	Improper Neutralization of Formula Elements in a CSV File vulnerability in WebToffee WordPress Comments Import & Export.This issue affects WordPress Comments Import & Export: from n/a through 2.3.1.	9.8	More Details
CVE-2023-47359	Videolan VLC prior to version 3.0.20 contains an incorrect offset read that leads to a Heap-Based Buffer Overflow in function GetPacket() and results in a memory corruption.	9.8	More Details
CVE-2023-38406	bgpd/bgp_flowspec.c in FRRouting (FRR) before 8.4.3 mishandles an nlri length of zero, aka a "flowspec overflow."	9.8	More Details
CVE-2023-23796	Improper Neutralization of Formula Elements in a CSV File vulnerability in Muneeb Form Builder	Create Responsive Contact Forms.This issue affects Form Builder	Create Responsive Contact Forms: from n/a through 1.9.9.0.	9.8	More Details
CVE-2023-22719	Improper Neutralization of Formula Elements in a CSV File vulnerability in GiveWP.This issue affects GiveWP: from n/a through 2.25.1.	9.8	More Details
CVE-2022-46802	Improper Neutralization of Formula Elements in a CSV File vulnerability in WebToffee Product Reviews Import Export for WooCommerce.This issue affects Product Reviews Import Export for WooCommerce: from n/a through 1.4.8.	9.8	More Details
CVE-2022-45357	Improper Neutralization of Formula Elements in a CSV File vulnerability in Lenderd 1003 Mortgage Application.This issue affects 1003 Mortgage Application: from n/a through 1.75.	9.8	More Details
CVE-2023-33481	RemoteClinic 2.0 is vulnerable to a time-based blind SQL injection attack in the 'start' GET parameter of patients/index.php.	9.8	More Details
CVE-2023-33479	RemoteClinic version 2.0 contains a SQL injection vulnerability in the /staff/edit.php file.	9.8	More Details
CVE-2023-33478	RemoteClinic 2.0 has a SQL injection vulnerability in the ID parameter of /medicines/stocks.php.	9.8	More Details
CVE-2023-42284	Blind SQL injection in api_version parameter in Tyk Gateway version 5.0.3 allows attacker to access and dump the database via a crafted SQL query.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42283	Blind SQL injection in api_id parameter in Tyk Gateway version 5.0.3 allows attacker to access and dump the database via a crafted SQL query.	9.8	More Details
CVE-2023-38547	A vulnerability in Veeam ONE allows an unauthenticated user to gain information about the SQL server connection Veeam ONE uses to access its configuration database. This may lead to remote code execution on the SQL server hosting the Veeam ONE configuration database.	9.8	More Details
CVE-2023-33045	Memory corruption in WLAN Firmware while parsing a NAN management frame carrying a S3 attribute.	9.8	More Details
CVE-2023-22388	Memory Corruption in Multi-mode Call Processor while processing bit mask API.	9.8	More Details
CVE-2023-47253	Qualitor through 8.20 allows remote attackers to execute arbitrary code via PHP code in the html/ad/adpesquisasql/request/processVariavel.php gridValoresPopHidden parameter.	9.8	More Details
CVE-2023-46800	Online Matrimonial Project v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'id' parameter of the view_profile.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-46981	SQL injection vulnerability in Novel-Plus v.4.2.0 allows a remote attacker to execute arbitrary code via a crafted script to the sort parameter in /common/log/list.	9.8	More Details
CVE-2023-46958	An issue in lmxcms v.1.41 allows a remote attacker to execute arbitrary code via a crafted script to the admin.php file.	9.8	More Details
CVE-2023-31579	Dromara Lamp-Cloud before v3.8.1 was discovered to use a hardcoded cryptographic key when creating and verifying a Json Web Token. This vulnerability allows attackers to authenticate to the application via a crafted JWT token.	9.8	More Details
CVE-2023-40922	kerawen before v2.5.1 was discovered to contain a SQL injection vulnerability via the ocs_id_cart parameter at KerawenDeliveryModuleFrontController::initContent().	9.8	More Details
CVE-2023-45346	Online Food Ordering System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The '*_role' parameter of the routers/user-router.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45345	Online Food Ordering System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The '*_deleted' parameter of the routers/user-router.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45338	Online Food Ordering System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'id' parameter of the routers/add-ticket.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45344	Online Food Ordering System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The '*_balance' parameter of the routers/user-router.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45343	Online Food Ordering System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'ticket_id' parameter of the routers/ticket-message.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45342	Online Food Ordering System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'phone' parameter of the routers/register-router.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45341	Online Food Ordering System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The '*_price' parameter of the routers/menu-router.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45340	Online Food Ordering System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'phone' parameter of the routers/details-router.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45336	Online Food Ordering System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'password' parameter of the routers/router.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45334	Online Food Ordering System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'status' parameter of the routers/edit-orders.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45325	Online Food Ordering System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'address' parameter of the routers/add-users.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45323	Online Food Ordering System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'name' parameter of the routers/add-item.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-47204	Unsafe YAML deserialization in yaml.Loader in transmute-core before 1.13.5 allows attackers to execute arbitrary Python code.	9.8	More Details
CVE-2023-45019	Online Bus Booking System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'category' parameter of the category.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45018	Online Bus Booking System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'username' parameter of the includes/login.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45015	Online Bus Booking System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'date' parameter of the bus_info.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45012	Online Bus Booking System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'user_email' parameter of the bus_info.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-45111	Online Examination System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The 'email' parameter of the feed.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-44025	SQL injection vulnerability in addify Addifyfreegifts v.1.0.2 and before allows a remote attacker to execute arbitrary code via a crafted script to the getrulebyid function in the AddifyfreegiftsModel.php component.	9.8	More Details
CVE-2023-39281	A stack buffer overflow vulnerability discovered in AsfSecureBootDxe in Insyde InsydeH2O with kernel 5.0 through 5.5 allows attackers to run arbitrary code execution during the DXE phase.	9.8	More Details
CVE-2023-46482	SQL injection vulnerability in wuzhicms v.4.1.0 allows a remote attacker to execute arbitrary code via the Database Backup Functionality in the coreframe/app/database/admin/index.php component.	9.8	More Details
CVE-2023-5766	A remote code execution vulnerability in Remote Desktop Manager 2023.2.33 and earlier on Windows allows an attacker to remotely execute code from another windows user session on the same host via a specially crafted TCP packet.	9.8	More Details
CVE-2023-5765	Improper access control in the password analyzer feature in Devolutions Remote Desktop Manager 2023.2.33 and earlier on Windows allows an attacker to bypass permissions via data source switching.	9.8	More Details
CVE-2023-42299	Buffer Overflow vulnerability in OpenImageIO oiio v.2.4.12.0 allows a remote attacker to execute arbitrary code and cause a denial of service via the read_subimage_data function.	9.8	More Details
CVE-2023-45347	Online Food Ordering System v1.0 is vulnerable to multiple Unauthenticated SQL Injection vulnerabilities. The '*_verified' parameter of the routers/user-router.php resource does not validate the characters received and they are sent unfiltered to the database.	9.8	More Details
CVE-2023-46954	SQL Injection vulnerability in Relativity ODA LLC RelativityOne v.12.1.537.3 Patch 2 and earlier allows a remote attacker to execute arbitrary code via the name parameter.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34383	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in weDevs WP Project Manager wedevs-project-manager allows SQL Injection.This issue affects WP Project Manager: from n/a through 2.6.0.	9.8	More Details
CVE-2023-36529	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Favethemes Houzez - Real Estate WordPress Theme allows SQL Injection.This issue affects Houzez - Real Estate WordPress Theme: from n/a through 1.3.4.	9.8	More Details
CVE-2023-25700	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Tutor LMS allows SQL Injection.This issue affects Tutor LMS: from n/a through 2.1.10.	9.8	More Details
CVE-2023-23368	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2376 build 20230421 and later QTS 4.5.4.2374 build 20230416 and later QuTS hero h5.0.1.2376 build 20230421 and later QuTS hero h4.5.4.2374 build 20230417 and later QuTScloud c5.0.1.2374 and later	9.8	More Details
CVE-2023-46980	An issue in Best Courier Management System v.1.0 allows a remote attacker to execute arbitrary code and escalate privileges via a crafted script to the userID parameter.	9.8	More Details
CVE-2022-46818	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Gopi Ramasamy Email posts to subscribers allows SQL Injection.This issue affects Email posts to subscribers: from n/a through 6.2.	9.8	More Details
CVE-2023-26015	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Chris Richardson MapPress Maps for WordPress mappress-google-maps-for-wordpress allows SQL Injection.This issue affects MapPress Maps for WordPress: from n/a through 2.85.4.	9.8	More Details
CVE-2022-47445	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Web-X Be POPIA Compliant be-popia-compliant allows SQL Injection.This issue affects Be POPIA Compliant: from n/a through 1.2.0.	9.8	More Details
CVE-2022-47426	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Neshan Maps Platform Neshan Maps neshan-maps allows SQL Injection.This issue affects Neshan Maps: from n/a through 1.1.4.	9.8	More Details
CVE-2022-46859	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Spiffy Plugins Spiffy Calendar spiffy-calendar allows SQL Injection.This issue affects Spiffy Calendar: from n/a through 4.9.1.	9.8	More Details
CVE-2022-45805	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Paytm Paytm Payment Gateway paytm-payments allows SQL Injection.This issue affects Paytm Payment Gateway: from n/a through 2.7.3.	9.8	More Details
CVE-2023-41652	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in David F. Carr RSVPMaker rsvpmaker allows SQL Injection.This issue affects RSVPMaker: from n/a through 10.6.6.	9.8	More Details
CVE-2023-3277	The MStore API plugin for WordPress is vulnerable to Unauthorized Account Access and Privilege Escalation in versions up to, and including, 4.10.7 due to improper implementation of the Apple login feature. This allows unauthenticated attackers to log in as any user as long as they know the user's email address. We are disclosing this issue as the developer has not yet released a patch, but continues to release updates and we escalated this issue to the plugin's team 30 days ago.	9.8	More Details
CVE-2022-46808	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Repute Infosystems ARMember armember-membership allows SQL Injection.This issue affects ARMember: from n/a through 3.4.11.	9.8	More Details
CVE-2022-47588	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Tips and Tricks HQ, Peter Petreski Simple Photo Gallery simple-photo-gallery allows SQL Injection.This issue affects Simple Photo Gallery: from n/a through v1.8.1.	9.8	More Details
CVE-2023-41355	Chunghwa Telecom NOKIA G-040W-Q Firewall function has a vulnerability of input validation for ICMP redirect messages. An unauthenticated remote attacker can exploit this vulnerability by sending a crafted package to modify the network routing table, resulting in a denial of service or sensitive information leaking.	9.8	More Details
CVE-2023-41351	Chunghwa Telecom NOKIA G-040W-Q has a vulnerability of authentication bypass, which allows an unauthenticated remote attacker to bypass the authentication mechanism to log in to the device by an alternative URL. This makes it possible for unauthenticated remote attackers to log in as any existing users, such as an administrator, to perform arbitrary system operations or disrupt service.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46817	An issue was discovered in phpFox before 4.8.14. The url request parameter passed to the /core/redirect route is not properly sanitized before being used in a call to the unserialize() PHP function. This can be exploited by remote, unauthenticated attackers to inject arbitrary PHP objects into the application scope, allowing them to perform a variety of attacks, such as executing arbitrary PHP code.	9.8	More Details
CVE-2023-43982	Bon Presta boninstagramcarousel between v5.2.1 to v7.0.0 was discovered to contain a Server-Side Request Forgery (SSRF) via the url parameter at insta_parser.php. This vulnerability allows attackers to use the vulnerable website as proxy to attack other websites or exfiltrate data via a HTTP call.	9.8	More Details
CVE-2023-38965	Lost and Found Information System 1.0 allows account takeover via username and password to a /classes/Users.php?f=save URI.	9.8	More Details
CVE-2023-46242	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions it's possible to execute a content with the right of any user via a crafted URL. A user must have `programming` privileges in order to exploit this vulnerability. This issue has been patched in XWiki 14.10.7 and 15.2RC1. Users are advised to upgrade. There are no known workarounds for for this vulnerability.	9.6	More Details
CVE-2023-1717	Prototype pollution in bitrix/templates/bitrix24/components/bitrix/menu/left_vertical/script.js in Bitrix24 22.0.300 allows remote attackers to execute arbitrary JavaScript code in the victim's browser, and possibly execute arbitrary PHP code on the server if the victim has administrator privilege, via polluting `__proto__[tag]` and `__proto__[text]`.	9.6	More Details
CVE-2023-46732	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. XWiki is vulnerable to reflected cross-site scripting (RXSS) via the `rev` parameter that is used in the content of the content menu without escaping. If an attacker can convince a user to visit a link with a crafted parameter, this allows the attacker to execute arbitrary actions in the name of the user, including remote code (Groovy) execution in the case of a user with programming right, compromising the confidentiality, integrity and availability of the whole XWiki installation. This has been patched in XWiki 15.6 RC1, 15.5.1 and 14.10.14. The patch in commit `04e325d57` can be manually applied without upgrading (or restarting) the instance. Users are advised to upgrade or to manually apply the patch. There are no known workarounds for this vulnerability.	9.6	More Details
CVE-2023-1720	Lack of mime type response header in Bitrix24 22.0.300 allows authenticated remote attackers to execute arbitrary JavaScript code in the victim's browser, and possibly execute arbitrary PHP code on the server if the victim has administrator privilege, via uploading a crafted HTML file through /desktop_app/file.ajax.php?action=uploadfile.	9.6	More Details
CVE-2023-46846	SQUID is vulnerable to HTTP request smuggling, caused by chunked decoder lenience, allows a remote attacker to perform Request/Response smuggling past firewall and frontend security systems.	9.3	More Details
CVE-2023-21671	Memory Corruption in Core during syscall for Sectools Fuse comparison feature.	9.3	More Details
CVE-2023-46253	Squidex is an open source headless CMS and content management hub. Affected versions are subject to an arbitrary file write vulnerability in the backup restore feature which allows an authenticated attacker to gain remote code execution (RCE). Squidex allows users with the `squidex.admin.restore` permission to create and restore backups. Part of these backups are the assets uploaded to an App. For each asset, the backup zip archive contains a `.asset` file with the actual content of the asset as well as a related `AssetCreatedEventV2` event, which is stored in a JSON file. Amongst other things, the JSON file contains the event type (`AssetCreatedEventV2`), the ID of the asset (`46c05041-9588-4179-b5eb-ddfcd9463e1e`), its filename (`test.txt`), and its file version (`0`). When a backup with this event is restored, the `BackupAssets.ReadAssetAsync` method is responsible for re-creating the asset. For this purpose, it determines the name of the `.asset` file in the zip archive, reads its content, and stores the content in the filestore. When the asset is stored in the filestore via the UploadAsync method, the assetId and fileVersion are passed as arguments. These are further passed to the method GetFileName, which determines the filename where the asset should be stored. The assetId is inserted into the filename without any sanitization and an attacker with squidex.admin.restore privileges to run arbitrary operating system commands on the underlying server (RCE).	9.1	More Details
CVE-2023-36621	An issue was discovered in the Boomerang Parental Control application through 13.83 for Android. The child can use Safe Mode to remove all restrictions temporarily or uninstall the application without the parents noticing.	9.1	More Details
CVE-2023-47456	Tenda AX1806 V1.0.0.1 contains a stack overflow vulnerability in function sub_455D4, called by function fromSetWirelessRepeat.	9.1	More Details
CVE-2023-46244	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. In affected versions it's possible for a user to write a script in which any velocity content is executed with the right of any other document content author. Since this API require programming right and the user does not have it, the expected result is `$doc.document.authors.contentAuthor` (not executed script), unfortunately with the security vulnerability it is possible for the attacker to get `XWiki.superadmin` which shows that the title was executed with the right of the unmodified document. This has been patched in XWiki versions 14.10.7 and 15.2RC1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47455	Tenda AX1806 V1.0.0.1 contains a heap overflow vulnerability in setSchedWifi function, in which the src and v12 are directly obtained from http request parameter schedStartTime and schedEndTime without checking their size.	9.1	More Details
CVE-2023-46501	An issue in BoltWire v.6.03 allows a remote attacker to obtain sensitive information via a crafted payload to the view and change admin password function.	9.1	More Details
CVE-2023-3961	A path traversal vulnerability was identified in Samba when processing client pipe names connecting to Unix domain sockets within a private directory. Samba typically uses this mechanism to connect SMB clients to remote procedure call (RPC) services like SAMR LSA or SPOOLSS, which Samba initiates on demand. However, due to inadequate sanitization of incoming client pipe names, allowing a client to send a pipe name containing Unix directory traversal characters (../). This could result in SMB clients connecting as root to Unix domain sockets outside the private directory. If an attacker or client managed to send a pipe name resolving to an external service using an existing Unix domain socket, it could potentially lead to unauthorized access to the service and consequential adverse events, including compromise or service crashes.	9.1	More Details
CVE-2023-42659	In WS_FTP Server versions prior to 8.7.6 and 8.8.4, an unrestricted file upload flaw has been identified. An authenticated Ad Hoc Transfer user has the ability to craft an API call which allows them to upload a file to a specified location on the underlying operating system hosting the WS_FTP Server application.	9.1	More Details
CVE-2023-28574	Memory corruption in core services when Diag handler receives a command to configure event listeners.	9.0	More Details
CVE-2023-23369	An OS command injection vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow users to execute commands via a network. We have already fixed the vulnerability in the following versions: Multimedia Console 2.1.2 (2023/05/04) and later Multimedia Console 1.4.8 (2023/05/05) and later QTS 5.1.0.2399 build 20230515 and later QTS 4.3.6.2441 build 20230621 and later QTS 4.3.4.2451 build 20230621 and later QTS 4.3.3.2420 build 20230621 and later QTS 4.2.6 build 20230621 and later Media Streaming add-on 500.1.1.2 (2023/06/12) and later Media Streaming add-on 500.0.0.11 (2023/06/16) and later	9.0	More Details
CVE-2023-1716	Cross-site scripting (XSS) vulnerability in Invoice Edit Page in Bitrix24 22.0.300 allows attackers to execute arbitrary JavaScript code in the victim's browser, and possibly execute arbitrary PHP code on the server if the victim has administrator privilege.	9.0	More Details
CVE-2023-1715	A logic error when using mb_strpos() to check for potential XSS payload in Bitrix24 22.0.300 allows attackers to bypass XSS sanitisation via placing HTML tags at the begining of the payload.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-45380	In the module "Order Duplicator " Clone and Delete Existing Order" (orderduplicate) in version <= 1.1.7 from Silbersaiten for PrestaShop, a guest can download personal information without restriction. Due to a lack of permissions control, a guest can download personal information from ps_customer/ps_address tables such as name / surname / phone number / full postal address.	8.8	More Details
CVE-2023-41348	ASUS RT-AX55's authentication-related function has a vulnerability of insufficient filtering of special characters within its code-authentication module. An authenticated remote attacker can exploit this vulnerability to perform a Command Injection attack to execute arbitrary commands, disrupt the system or terminate services.	8.8	More Details
CVE-2023-1713	Insecure temporary file creation in bitrix/modules/crm/lib/order/import/instagram.php in Bitrix24 22.0.300 hosted on Apache HTTP Server allows remote authenticated attackers to execute arbitrary code via uploading a crafted ".htaccess" file.	8.8	More Details
CVE-2023-47182	Cross-Site Request Forgery (CSRF) leading to a Stored Cross-Site Scripting (XSS) vulnerability in Nazmul Hossain Nihal Login Screen Manager plugin <= 3.5.2 versions.	8.8	More Details
CVE-2023-5482	Insufficient data validation in USB in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-41353	Chunghwa Telecom NOKIA G-040W-Q has a vulnerability of weak password requirements. A remote attacker with regular user privilege can easily infer the administrator password from system information after logging system, resulting in admin access and performing arbitrary system operations or disrupt service.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41357	Galaxy Software Services Corporation Vitals ESP is an online knowledge base management portal, it has insufficient filtering and validation during file upload. An authenticated remote attacker with general user privilege can exploit this vulnerability to upload and execute scripts onto arbitrary directories to perform arbitrary system operations or disrupt service.	8.8	More Details
CVE-2023-46947	Subrion 4.2.1 has a remote command execution vulnerability in the backend.	8.8	More Details
CVE-2023-20175	A vulnerability in a specific Cisco ISE CLI command could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, an attacker must have valid Read-only-level privileges or higher on the affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	8.8	More Details
CVE-2023-25800	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Tutor LMS allows SQL Injection.This issue affects Tutor LMS: from n/a through 2.2.0.	8.8	More Details
CVE-2023-25990	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Tutor LMS allows SQL Injection.This issue affects Tutor LMS: from n/a through 2.1.10.	8.8	More Details
CVE-2023-3893	A security issue was discovered in Kubernetes where a user that can create pods on Windows nodes running kubernetes-csi-proxy may be able to escalate to admin privileges on those nodes. Kubernetes clusters are only affected if they include Windows nodes running kubernetes-csi-proxy.	8.8	More Details
CVE-2023-5178	A use-after-free vulnerability was found in drivers/nvme/target/tcp.c` in `nvmet_tcp_free_crypto` due to a logical bug in the NVMe/TCP subsystem in the Linux kernel. This issue may allow a malicious user to cause a use-after-free and double-free problem, which may permit remote code execution or lead to local privilege escalation.	8.8	More Details
CVE-2023-47004	Buffer Overflow vulnerability in Redis RedisGraph v.2.x through v.2.12.8 and fixed in v.2.12.9 allows an attacker to execute arbitrary code via the code logic after valid authentication.	8.8	More Details
CVE-2023-36677	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Smartypants SP Project & Document Manager allows SQL Injection.This issue affects SP Project & Document Manager: from n/a through 4.67.	8.8	More Details
CVE-2023-5719	The Crimson 3.2 Windows-based configuration tool allows users with administrative access to define new passwords for users and to download the resulting security configuration to a device. If such a password contains the percent (%) character, invalid values will be included, potentially truncating the string if a NUL is encountered. If the simplified password is not detected by the administrator, the device might be left in a vulnerable state as a result of more-easily compromised credentials. Note that passwords entered via the Crimson system web server do not suffer from this vulnerability.	8.8	More Details
CVE-2023-35910	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Nucleus_genius Quasar form free – Contact Form Builder for WordPress allows SQL Injection.This issue affects Quasar form free – Contact Form Builder for WordPress: from n/a through 6.0.	8.8	More Details
CVE-2023-43336	Sangoma Technologies FreePBX before cdr 15.0.18, 16.0.40, 15.0.16, and 16.0.17 was discovered to contain an access control issue via a modified parameter value, e.g., changing extension=self to extension=101.	8.8	More Details
CVE-2023-44398	Exiv2 is a C++ library and a command-line utility to read, write, delete and modify Exif, IPTC, XMP and ICC image metadata. An out-of-bounds write was found in Exiv2 version v0.28.0. The vulnerable function, `BmffImage::brotliUncompress`, is new in v0.28.0, so earlier versions of Exiv2 are _not_ affected. The out-of-bounds write is triggered when Exiv2 is used to read the metadata of a crafted image file. An attacker could potentially exploit the vulnerability to gain code execution, if they can trick the victim into running Exiv2 on a crafted image file. This bug is fixed in version v0.28.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2023-40061	Insecure job execution mechanism vulnerability. This vulnerability can lead to other attacks as a result.	8.8	More Details
CVE-2023-46084	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in bPlugins LLC Icons Font Loader allows SQL Injection.This issue affects Icons Font Loader: from n/a through 1.1.2.	8.8	More Details
CVE-2023-5823	Cross-Site Request Forgery (CSRF) vulnerability in ThemeKraft TK Google Fonts GDPR Compliant plugin <= 2.2.11 versions.	8.8	More Details
CVE-2023-47186	Cross-Site Request Forgery (CSRF) vulnerability in Kadence WP Kadence WooCommerce Email Designer plugin <= 1.5.11 versions.	8.8	More Details
CVE-2023-46781	Cross-Site Request Forgery (CSRF) vulnerability in Roland Murg Current Menu Item for Custom Post Types plugin <= 1.5 versions.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46780	Cross-Site Request Forgery (CSRF) vulnerability in Alter plugin <= 1.0 versions.	8.8	More Details
CVE-2023-46779	Cross-Site Request Forgery (CSRF) vulnerability in EasyRecipe plugin <= 3.5.3251 versions.	8.8	More Details
CVE-2023-46778	Cross-Site Request Forgery (CSRF) vulnerability in TheFreeWindows Auto Limit Posts Reloaded plugin <= 2.5 versions.	8.8	More Details
CVE-2023-46777	Cross-Site Request Forgery (CSRF) vulnerability in Custom Login Page	Temporary Users	Rebrand Login	Login Captcha plugin <= 1.1.3 versions.	8.8	More Details
CVE-2023-46776	Cross-Site Request Forgery (CSRF) vulnerability in Serena Villa Auto Excerpt everywhere plugin <= 1.5 versions.	8.8	More Details
CVE-2023-5849	Integer overflow in USB in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-1714	Unsafe variable extraction in bitrix/modules/main/classes/general/user_options.php in Bitrix24 22.0.300 allows remote authenticated attackers to execute arbitrary code via (1) appending arbitrary content to existing PHP files or (2) PHAR deserialization.	8.8	More Details
CVE-2023-5709	The WD WidgetTwitter plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 1.0.9 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with contributor-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2022-44738	Improper Neutralization of Formula Elements in a CSV File vulnerability in Patrick Robrecht Posts and Users Stats.This issue affects Posts and Users Stats: from n/a through 1.1.3.	8.8	More Details
CVE-2023-5898	Cross-Site Request Forgery (CSRF) in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	8.8	More Details
CVE-2023-5897	Cross-Site Request Forgery (CSRF) in GitHub repository pkp/customLocale prior to 1.2.0-1.	8.8	More Details
CVE-2022-38702	Improper Neutralization of Formula Elements in a CSV File vulnerability in Nakashima Masahiro WP CSV Exporter.This issue affects WP CSV Exporter: from n/a through 2.0.	8.8	More Details
CVE-2022-41616	Improper Neutralization of Formula Elements in a CSV File vulnerability in Kaushik Kalathiya Export Users Data CSV.This issue affects Export Users Data CSV: from n/a through 2.1.	8.8	More Details
CVE-2022-42882	Improper Neutralization of Formula Elements in a CSV File vulnerability in Shambix Simple CSV/XLS Exporter.This issue affects Simple CSV/XLS Exporter: from n/a through 1.5.8.	8.8	More Details
CVE-2023-5893	Cross-Site Request Forgery (CSRF) in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	8.8	More Details
CVE-2022-47181	Cross-Site Request Forgery (CSRF) vulnerability in wpexpertsio Email Templates Customizer and Designer for WordPress and WooCommerce email-templates allows Cross Site Request Forgery.This issue affects Email Templates Customizer and Designer for WordPress and WooCommerce: from n/a through 1.4.2.	8.8	More Details
CVE-2023-5899	Cross-Site Request Forgery (CSRF) in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	8.8	More Details
CVE-2023-41798	Improper Neutralization of Formula Elements in a CSV File vulnerability in wpWax Directorist – WordPress Business Directory Plugin with Classified Ads Listing.This issue affects Directorist – WordPress Business Directory Plugin with Classified Ads Listings: from n/a through 7.7.1.	8.8	More Details
CVE-2023-5856	Use after free in Side Panel in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-5857	Inappropriate implementation in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to potentially execute arbitrary code via a malicious file. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-41346	ASUS RT-AX55's authentication-related function has a vulnerability of insufficient filtering of special characters within its token-refresh module. An authenticated remote attacker can exploit this vulnerability to perform a Command Injection attack to execute arbitrary commands, disrupt the system or terminate services.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41345	ASUS RT-AX55's authentication-related function has a vulnerability of insufficient filtering of special characters within its token-generated module. An authenticated remote attacker can exploit this vulnerability to perform a Command Injection attack to execute arbitrary commands, disrupt the system, or terminate services.	8.8	More Details
CVE-2023-46428	An arbitrary file upload vulnerability in HadSky v7.12.10 allows attackers to execute arbitrary code via a crafted file.	8.8	More Details
CVE-2022-45350	Improper Neutralization of Formula Elements in a CSV File vulnerability in Pär Thernström Simple History – user activity log, audit tool.This issue affects Simple History – user activity log, audit tool: from n/a through 3.3.1.	8.8	More Details
CVE-2023-46775	Cross-Site Request Forgery (CSRF) vulnerability in Djo Original texts Yandex WebMaster plugin <= 1.18 versions.	8.8	More Details
CVE-2022-46821	Improper Neutralization of Formula Elements in a CSV File vulnerability in Jackmail & Sarbacane Emails & Newsletters with Jackmail.This issue affects Emails & Newsletters with Jackmail: from n/a through 1.2.22.	8.8	More Details
CVE-2022-46804	Improper Neutralization of Formula Elements in a CSV File vulnerability in Narola Infotech Solutions LLP Export Users Data Distinct.This issue affects Export Users Data Distinct: from n/a through 1.3.	8.8	More Details
CVE-2022-47442	Improper Neutralization of Formula Elements in a CSV File vulnerability in AyeCode Ltd UsersWP.This issue affects UsersWP: from n/a through 1.2.3.9.	8.8	More Details
CVE-2023-33480	RemoteClinic 2.0 contains a critical vulnerability chain that can be exploited by a remote attacker with low-privileged user credentials to create admin users, escalate privileges, and execute arbitrary code on the target system via a PHP shell. The vulnerabilities are caused by a lack of input validation and access control in the staff/register.php endpoint and the edit-my-profile.php page. By sending a series of specially crafted requests to the RemoteClinic application, an attacker can create admin users with more privileges than their own, upload a PHP file containing arbitrary code, and execute arbitrary commands via the PHP shell.	8.8	More Details
CVE-2023-25983	Improper Neutralization of Formula Elements in a CSV File vulnerability in WPOmnia KB Support.This issue affects KB Support: from n/a through 1.5.84.	8.8	More Details
CVE-2023-36527	Improper Neutralization of Formula Elements in a CSV File vulnerability in BestWebSoft Post to CSV by BestWebSoft.This issue affects Post to CSV by BestWebSoft: from n/a through 1.4.0.	8.8	More Details
CVE-2023-5852	Use after free in Printing in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-41347	ASUS RT-AX55's authentication-related function has a vulnerability of insufficient filtering of special characters within its check token module. An authenticated remote attacker can exploit this vulnerability to perform a Command Injection attack to execute arbitrary commands, disrupt the system or terminate services.	8.8	More Details
CVE-2023-5854	Use after free in Profiles in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-5855	Use after free in Reading Mode in Google Chrome prior to 119.0.6045.105 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via specific UI gestures. (Chromium security severity: Medium)	8.8	More Details
CVE-2022-45348	Improper Neutralization of Formula Elements in a CSV File vulnerability in anmari amr users.This issue affects amr users: from n/a through 4.59.4.	8.8	More Details
CVE-2023-5950	Rapid7 Velociraptor versions prior to 0.7.0-4 suffer from a reflected cross site scripting vulnerability. This vulnerability allows attackers to inject JS into the error path, potentially leading to unauthorized execution of scripts within a user's web browser. This vulnerability is fixed in version 0.7.0-04 and a patch is available to download. Patches are also available for version 0.6.9 (0.6.9-1).	8.6	More Details
CVE-2023-46848	Squid is vulnerable to Denial of Service, where a remote attacker can perform DoS by sending ftp:// URLs in HTTP Request messages or constructing ftp:// URLs from FTP Native input.	8.6	More Details
CVE-2023-46847	Squid is vulnerable to a Denial of Service, where a remote attacker can perform buffer overflow attack by writing up to 2 MB of arbitrary data to heap memory when Squid is configured to accept HTTP Digest Authentication.	8.6	More Details
CVE-2023-20095	A vulnerability in the remote access VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of HTTPS requests. An attacker could exploit this vulnerability by sending crafted HTTPS requests to an affected system. A successful exploit could allow the attacker to cause resource exhaustion, resulting in a DoS condition.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20086	A vulnerability in ICMPv6 processing of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to improper processing of ICMPv6 messages. An attacker could exploit this vulnerability by sending crafted ICMPv6 messages to a targeted Cisco ASA or FTD system with IPv6 enabled. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2023-20083	A vulnerability in ICMPv6 inspection when configured with the Snort 2 detection engine for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the CPU of an affected device to spike to 100 percent, which could stop all traffic processing and result in a denial of service (DoS) condition. FTD management traffic is not affected by this vulnerability. This vulnerability is due to improper error checking when parsing fields within the ICMPv6 header. An attacker could exploit this vulnerability by sending a crafted ICMPv6 packet through an affected device. A successful exploit could allow the attacker to cause the device to exhaust CPU resources and stop processing traffic, resulting in a DoS condition. Note: To recover from the DoS condition, the Snort 2 Detection Engine or the Cisco FTD device may need to be restarted.	8.6	More Details
CVE-2023-46724	Squid is a caching proxy for the Web. Due to an Improper Validation of Specified Index bug, Squid versions 3.3.0.1 through 5.9 and 6.0 prior to 6.4 compiled using `--with-openssl` are vulnerable to a Denial of Service attack against SSL Certificate validation. This problem allows a remote server to perform Denial of Service against Squid Proxy by initiating a TLS Handshake with a specially crafted SSL Certificate in a server certificate chain. This attack is limited to HTTPS and SSL-Bump. This bug is fixed in Squid version 6.4. In addition, patches addressing this problem for the stable releases can be found in Squid's patch archives. Those who you use a prepackaged version of Squid should refer to the package vendor for availability information on updated packages.	8.6	More Details
CVE-2023-20244	A vulnerability in the internal packet processing of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series Firewalls could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper handling of certain packets when they are sent to the inspection engine. An attacker could exploit this vulnerability by sending a series of crafted packets to an affected device. A successful exploit could allow the attacker to deplete all 9,472 byte blocks on the device, resulting in traffic loss across the device or an unexpected reload of the device. If the device does not reload on its own, a manual reload of the device would be required to recover from this state.	8.6	More Details
CVE-2023-45830	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Online ADA Accessibility Suite by Online ADA allows SQL Injection.This issue affects Accessibility Suite by Online ADA: from n/a through 4.12.	8.5	More Details
CVE-2023-3399	An issue has been discovered in GitLab EE affecting all versions starting from 11.6 before 16.3.6, all versions starting from 16.4 before 16.4.2, all versions starting from 16.5 before 16.5.1. It was possible for an unauthorised project or group member to read the CI/CD variables using the custom project templates.	8.5	More Details
CVE-2023-33074	Memory corruption in Audio when SSR event is triggered after music playback is stopped.	8.4	More Details
CVE-2023-42536	An improper input validation in saped_dec in libsaped prior to SMR Nov-2023 Release 1 allows local attackers to cause out-of-bounds read and write.	8.4	More Details
CVE-2023-42537	An improper input validation in get_head_crc in libsaped prior to SMR Nov-2023 Release 1 allows local attackers to cause out-of-bounds read and write.	8.4	More Details
CVE-2023-24852	Memory Corruption in Core due to secure memory access by user while loading modem image.	8.4	More Details
CVE-2023-42535	Out-of-bounds Write in read_block of vold prior to SMR Nov-2023 Release 1 allows local attacker to execute arbitrary code.	8.4	More Details
CVE-2023-5846	Franklin Fueling System TS-550 versions prior to 1.9.23.8960 are vulnerable to attackers decoding admin credentials, resulting in unauthenticated access to the device.	8.3	More Details
CVE-2023-5889	Insufficient Session Expiration in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	8.2	More Details
CVE-2023-28545	Memory corruption in TZ Secure OS while loading an app ELF.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20063	A vulnerability in the inter-device communication mechanisms between devices that are running Cisco Firepower Threat Defense (FTD) Software and devices that are running Cisco Firepower Management (FMC) Software could allow an authenticated, local attacker to execute arbitrary commands with root permissions on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by accessing the expert mode of an affected device and submitting specific commands to a connected system. A successful exploit could allow the attacker to execute arbitrary code in the context of an FMC device if the attacker has administrative privileges on an associated FTD device. Alternatively, a successful exploit could allow the attacker to execute arbitrary code in the context of an FTD device if the attacker has administrative privileges on an associated FMC device.	8.2	More Details
CVE-2023-46381	LOYTEC LINX-151, LINX-212, LVIS-3ME12-A1, LIOB-586, LIOB-580 V2, LIOB-588, L-INX Configurator devices (all versions) lack authentication for the preinstalled version of LWEB-802 via an lweb802_pre/ URI. An unauthenticated attacker can edit any project (or create a new project) and control its GUI.	8.2	More Details
CVE-2023-31027	NVIDIA GPU Display Driver for Windows contains a vulnerability that allows Windows users with low levels of privilege to escalate privileges when an administrator is updating GPU drivers, which may lead to escalation of privileges.	8.2	More Details
CVE-2023-43885	Missing error handling in the HTTP server component of Tenda RX9 Pro Firmware V22.03.02.20 allows authenticated attackers to arbitrarily lock the device.	8.1	More Details
CVE-2023-46725	FoodCoopShop is open source software for food coops and local shops. Versions starting with 3.2.0 prior to 3.6.1 are vulnerable to server-side request forgery. In the Network module, a manufacturer account can use the `/api/updateProducts.json` endpoint to make the server send a request to an arbitrary host. This means that the server can be used as a proxy into the internal network where the server is. Furthermore, the checks on a valid image are not adequate, leading to a time of check time of use issue. For example, by using a custom server that returns 200 on HEAD requests, then return a valid image on first GET request and then a 302 redirect to final target on second GET request, the server will copy whatever file is at the redirect destination, making this a full SSRF. Version 3.6.1 fixes this vulnerability.	8.1	More Details
CVE-2023-5355	The Awesome Support WordPress plugin before 6.1.5 does not sanitize file paths when deleting temporary attachment files, allowing a ticket submitter to delete arbitrary files on the server.	8.1	More Details
CVE-2023-33226	The Network Configuration Manager was susceptible to a Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows a low-level user to perform the actions with SYSTEM privileges.	8.0	More Details
CVE-2023-33227	The Network Configuration Manager was susceptible to a Directory Traversal Remote Code Execution Vulnerability This vulnerability allows a low level user to perform the actions with SYSTEM privileges.	8.0	More Details
CVE-2023-40062	SolarWinds Platform Incomplete List of Disallowed Inputs Remote Code Execution Vulnerability. If executed, this vulnerability would allow a low-privileged user to execute commands with SYSTEM privileges.	8.0	More Details
CVE-2023-42361	Local File Inclusion vulnerability in Midori-global Better PDF Exporter for Jira Server and Jira Data Center v.10.3.0 and before allows an attacker to view arbitrary files and cause other impacts via use of crafted image during PDF export.	7.8	More Details
CVE-2023-5179	An issue was discovered in Open Design Alliance Drawings SDK before 2024.10. A corrupted value for the start of MiniFat sector in a crafted DGN file leads to an out-of-bounds read. This can allow attackers to cause a crash, potentially enabling a denial-of-service attack (Crash, Exit, or Restart) or possible code execution.	7.8	More Details
CVE-2023-3972	A vulnerability was found in insights-client. This security issue occurs because of insecure file operations or unsafe handling of temporary files and directories that lead to local privilege escalation. Before the insights-client has been registered on the system by root, an unprivileged local user or attacker could create the /var/tmp/insights-client directory (owning the directory with read, write, and execute permissions) on the system. After the insights-client is registered by root, an attacker could then control the directory content that insights are using by putting malicious scripts into it and executing arbitrary code as root (trivially bypassing SELinux protections because insights processes are allowed to disable SELinux system-wide).	7.8	More Details
CVE-2023-33059	Memory corruption in Audio while processing the VOC packet data from ADSP.	7.8	More Details
CVE-2023-33055	Memory Corruption in Audio while invoking callback function in driver from ADSP.	7.8	More Details
CVE-2023-3889	A local non-privileged user can make improper GPU memory processing operations. If the operations are carefully prepared, then they could be used to gain access to already freed memory.	7.8	More Details
CVE-2023-4295	A local non-privileged user can make improper GPU memory processing operations to gain access to already freed memory.	7.8	More Details
CVE-2023-33031	Memory corruption in Automotive Audio while copying data from ADSP shared buffer to the VOC packet data buffer.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31102	Ppmd7.c in 7-Zip before 23.00 allows an integer underflow and invalid read operation via a crafted 7Z archive.	7.8	More Details
CVE-2023-32837	In video, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08235273; Issue ID: ALPS08250357.	7.8	More Details
CVE-2023-31017	NVIDIA GPU Display Driver for Windows contains a vulnerability where an attacker may be able to write arbitrary data to privileged locations by using reparse points. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.	7.8	More Details
CVE-2023-31019	NVIDIA GPU Display Driver for Windows contains a vulnerability in wksServicePlugin.dll, where the driver implementation does not restrict or incorrectly restricts access from the named pipe server to a connecting client, which may lead to potential impersonation to the client's secure context.	7.8	More Details
CVE-2022-43554	Ivanti Avalanche Smart Device Service Missing Authentication Local Privilege Escalation Vulnerability	7.8	More Details
CVE-2023-41036	Macvim is a text editor for MacOS. Prior to version 178, Macvim makes use of an insecure interprocess communication (IPC) mechanism which could lead to a privilege escalation. Distributed objects are a concept introduced by Apple which allow one program to vend an interface to another program. What is not made clear in the documentation is that this service can vend this interface to any other program on the machine. The impact of exploitation is a privilege escalation to root - this is likely to affect anyone who is not careful about the software they download and use MacVim to edit files that would require root privileges. Version 178 contains a fix for this issue.	7.8	More Details
CVE-2022-43555	Ivanti Avalanche Printer Device Service Missing Authentication Local Privilege Escalation Vulnerability	7.8	More Details
CVE-2022-44569	A locally authenticated attacker with low privileges can bypass authentication due to insecure inter-process communication.	7.8	More Details
CVE-2023-41725	Ivanti Avalanche EnterpriseServer Service Unrestricted File Upload Local Privilege Escalation Vulnerability	7.8	More Details
CVE-2023-39283	An SMM memory corruption vulnerability in the SMM driver (SMRAM write) in CsmInt10HookSmm in Insyde InsydeH2O with kernel 5.0 through 5.5 allows attackers to send arbitrary data to SMM which could lead to privilege escalation.	7.8	More Details
CVE-2023-41726	Ivanti Avalanche Incorrect Default Permissions allows Local Privilege Escalation Vulnerability	7.8	More Details
CVE-2023-26454	Requests to fetch image metadata could be abused to include SQL queries that would be executed unchecked. Exploiting this vulnerability requires at least access to adjacent networks of the imageconverter service, which is not exposed to public networks by default. Arbitrary SQL statements could be executed in the context of the services database user account. API requests are now properly checked for valid content and attempts to circumvent this check are being logged as error. No publicly available exploits are known.	7.6	More Details
CVE-2023-26453	Requests to cache an image could be abused to include SQL queries that would be executed unchecked. Exploiting this vulnerability requires at least access to adjacent networks of the imageconverter service, which is not exposed to public networks by default. Arbitrary SQL statements could be executed in the context of the services database user account. API requests are now properly checked for valid content and attempts to circumvent this check are being logged as error. No publicly available exploits are known.	7.6	More Details
CVE-2023-26452	Requests to cache an image and return its metadata could be abused to include SQL queries that would be executed unchecked. Exploiting this vulnerability requires at least access to adjacent networks of the imageconverter service, which is not exposed to public networks by default. Arbitrary SQL statements could be executed in the context of the services database user account. API requests are now properly checked for valid content and attempts to circumvent this check are being logged as error. No publicly available exploits are known.	7.6	More Details
CVE-2023-39345	strapi is an open-source headless CMS. Versions prior to 4.13.1 did not properly restrict write access to fielded marked as private in the user registration endpoint. As such malicious users may be able to errantly modify their user records. This issue has been addressed in version 4.13.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.6	More Details
CVE-2023-41344	NCSIST ManageEngine Mobile Device Manager(MDM) APP's special function has a path traversal vulnerability. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and read arbitrary system files.	7.5	More Details
CVE-2023-47235	An issue was discovered in FRRouting FRR through 9.0.1. A crash can occur when a malformed BGP UPDATE message with an EOR is processed, because the presence of EOR does not lead to a treat-as-withdraw outcome.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46352	In the module "Pixel Plus: Events + CAPI + Pixel Catalog for Facebook Module" (facebookconversiontrackingplus) up to version 2.4.9 from Smart Modules for PrestaShop, a guest can download personal information without restriction. Due to a lack of permissions control, a guest can access exports from the module which can lead to a leak of personal information from ps_customer table such as name / surname / email.	7.5	More Details
CVE-2023-39057	An information leak in hirochanKAKIwaiting v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	7.5	More Details
CVE-2023-39054	An information leak in Tokudaya.ekimae_mc v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	7.5	More Details
CVE-2023-39053	An information leak in Hattoriya v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	7.5	More Details
CVE-2023-39051	An information leak in VISION MEAT WORKS Track Diner 10/10mbl v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	7.5	More Details
CVE-2023-39050	An information leak in Daiky-value.Fukueten v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	7.5	More Details
CVE-2023-39048	An information leak in Tokudaya.honten v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	7.5	More Details
CVE-2023-39047	An information leak in shouzu sweets oz v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	7.5	More Details
CVE-2023-39042	An information leak in Gyouza-newhushimi v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	7.5	More Details
CVE-2023-46380	LOYTEC LINX-151, LINX-212, LVIS-3ME12-A1, LIOB-586, LIOB-580 V2, LIOB-588, L-INX Configurator devices (all versions) send password-change requests via cleartext HTTP.	7.5	More Details
CVE-2023-46728	Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Due to a NULL pointer dereference bug Squid is vulnerable to a Denial of Service attack against Squid's Gopher gateway. The gopher protocol is always available and enabled in Squid prior to Squid 6.0.1. Responses triggering this bug are possible to be received from any gopher server, even those without malicious intent. Gopher support has been removed in Squid version 6.0.1. Users are advised to upgrade. Users unable to upgrade should reject all gopher URL requests.	7.5	More Details
CVE-2023-46382	LOYTEC LINX-151, LINX-212, LVIS-3ME12-A1, LIOB-586, LIOB-580 V2, LIOB-588, L-INX Configurator devices (all versions) use cleartext HTTP for login.	7.5	More Details
CVE-2023-20702	In 5G NRLC, there is a possible invalid memory access due to lack of error handling. This could lead to remote denial of service, if UE received invalid 1-byte rlc sdu, with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY00921261; Issue ID: MOLY01128895.	7.5	More Details
CVE-2023-38407	bgpd/bgp_label.c in FRRouting (FRR) before 8.5 attempts to read beyond the end of the stream during labeled unicast parsing.	7.5	More Details
CVE-2023-46251	MyBB is a free and open source forum software. Custom MyCode (BBCode) for the visual editor (_SCEditor_) doesn't escape input properly when rendering HTML, resulting in a DOM-based XSS vulnerability. This weakness can be exploited by pointing a victim to a page where the visual editor is active (e.g. as a post or Private Message) and operates on a maliciously crafted MyCode message. This may occur on pages where message content is pre-filled using a GET/POST parameter, or on reply pages where a previously saved malicious message is quoted. The impact is be mitigated when: 1. the visual editor is disabled globally (_Admin CP → Configuration → Settings → Clickable Smilies and BB Code: [Clickable MyCode Editor](https://github.com/mybb/mybb/blob/mybb_1836/install/resources/settings.xml#L2087-L2094)_ is set to _Off_), or 2. the visual editor is disabled for individual user accounts (_User CP → Your Profile → Edit Options_: _Show the MyCode formatting options on the posting pages_ checkbox is not checked). MyBB 1.8.37 resolves this issue with the commit `6dcaf0b4d`. Users are advised to upgrade. Users unable to upgrade may mitigate the impact without upgrading MyBB by changing the following setting (_Admin CP → Configuration → Settings_): - _Clickable Smilies and BB Code → [Clickable MyCode Editor](https://github.com/mybb/mybb/blob/mybb_1836/install/resources/settings.xml#L2087-L2094)_: _Off_. Similarly, individual MyBB forum users are able to disable the visual editor by diabling the account option (_User CP → Your Profile → Edit Options_) _Show the MyCode formatting options on the posting pages_.	7.5	More Details
CVE-2023-41378	In certain conditions for Calico Typha (v3.26.2, v3.25.1 and below), and Calico Enterprise Typha (v3.17.1, v3.16.3, v3.15.3 and below), a client TLS handshake can block the Calico Typha server indefinitely, resulting in denial of service. The TLS Handshake() call is performed inside the main server handle for loop without any timeout allowing an unclean TLS handshake to block the main loop indefinitely while other connections will be idle waiting for that handshake to finish.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-7252	bcrypt password hashing in Botan before 2.1.0 does not correctly handle passwords with a length between 57 and 72 characters, which makes it easier for attackers to determine the cleartext password.	7.5	More Details
CVE-2023-34260	Kyocera TASKalfa 4053ci printers through 2VG_S000.002.561 allow a denial of service (service outage) via /wlmdeu%2f%2e%2e%2f%2e%2e followed by a directory reference such as %2fetc%00index.htm to try to read the /etc directory.	7.5	More Details
CVE-2023-44271	An issue was discovered in Pillow before 10.0.0. It is a Denial of Service that uncontrollably allocates memory to process a given task, potentially causing a service to crash by having it run out of memory. This occurs for truetype in ImageFont when textlength in an ImageDraw instance operates on a long text argument.	7.5	More Details
CVE-2023-43984	Insecure permissions in Smart Soft advancedexport before v4.4.7 allow unauthenticated attackers to arbitrarily download user information from the ps_customer table.	7.5	More Details
CVE-2023-43665	In Django 3.2 before 3.2.22, 4.1 before 4.1.12, and 4.2 before 4.2.6, the django.utils.text.Truncator chars() and words() methods (when used with html=True) are subject to a potential DoS (denial of service) attack via certain inputs with very long, potentially malformed HTML text. The chars() and words() methods are used to implement the truncatechars_html and truncatewords_html template filters, which are thus also vulnerable. NOTE: this issue exists because of an incomplete fix for CVE-2019-14232.	7.5	More Details
CVE-2023-33061	Transient DOS in WLAN Firmware while parsing WLAN beacon or probe-response frame.	7.5	More Details
CVE-2023-5824	A flaw was found in Squid. The limits applied for validation of HTTP response headers are applied before caching. However, Squid may grow a cached HTTP response header beyond the configured maximum size, causing a stall or crash of the worker process when a large header is retrieved from the disk cache, resulting in a denial of service.	7.5	More Details
CVE-2023-41350	Chunghwa Telecom NOKIA G-040W-Q has a vulnerability of insufficient measures to prevent multiple failed authentication attempts. An unauthenticated remote attacker can execute a crafted Javascript to expose captcha in page, making it very easy for bots to bypass the captcha check and more susceptible to brute force attacks.	7.5	More Details
CVE-2023-33056	Transient DOS in WLAN Firmware when firmware receives beacon including T2LM IE.	7.5	More Details
CVE-2023-33048	Transient DOS in WLAN Firmware while parsing t2lm buffers.	7.5	More Details
CVE-2023-47360	Videolan VLC prior to version 3.0.20 contains an Integer underflow that leads to an incorrect packet length.	7.5	More Details
CVE-2023-33047	Transient DOS in WLAN Firmware while parsing no-inherit IES.	7.5	More Details
CVE-2023-39299	A path traversal vulnerability has been reported to affect Music Station. If exploited, the vulnerability could allow users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following versions: Music Station 4.8.11 and later Music Station 5.1.16 and later Music Station 5.3.23 and later	7.5	More Details
CVE-2023-5454	The Templately WordPress plugin before 2.2.6 does not properly authorize the `saved-templates/delete` REST API call, allowing unauthenticated users to delete arbitrary posts.	7.5	More Details
CVE-2023-5998	Out-of-bounds Read in GitHub repository gpac/gpac prior to 2.3.0-DEV.	7.5	More Details
CVE-2023-4154	A design flaw was found in Samba's DirSync control implementation, which exposes passwords and secrets in Active Directory to privileged users and Read-Only Domain Controllers (RODCs). This flaw allows RODCs and users possessing the GET_CHANGES right to access all attributes, including sensitive secrets and passwords. Even in a default setup, RODC DC accounts, which should only replicate some passwords, can gain access to all domain secrets, including the vital krbtgt, effectively eliminating the RODC / DC distinction. Furthermore, the vulnerability fails to account for error conditions (fail open), like out-of-memory situations, potentially granting access to secret attributes, even under low-privileged attacker influence.	7.5	More Details
CVE-2021-43419	An Information Disclosure vulnerability exists in Opay Mobile application 1.5.1.26 and maybe be higher in the logcat app.	7.5	More Details
CVE-2023-41260	Best Practical Request Tracker (RT) before 4.4.7 and 5.x before 5.0.5 allows Information Exposure in responses to mail-gateway REST API calls.	7.5	More Details
CVE-2023-41259	Best Practical Request Tracker (RT) before 4.4.7 and 5.x before 5.0.5 allows Information Disclosure via fake or spoofed RT email headers in an email message or a mail-gateway REST API call.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41164	In Django 3.2 before 3.2.21, 4.1 before 4.1.11, and 4.2 before 4.2.5, django.utils.encoding.uri_to_iri() is subject to a potential DoS (denial of service) attack via certain inputs with a very large number of Unicode characters.	7.5	More Details
CVE-2023-47234	An issue was discovered in FRRouting FRR through 9.0.1. A crash can occur when processing a crafted BGP UPDATE message with a MP_UNREACH_NLRI attribute and additional NLRI data (that lacks mandatory path attributes).	7.5	More Details
CVE-2023-45024	Best Practical Request Tracker (RT) 5 before 5.0.5 allows Information Disclosure via a transaction search in the transaction query builder.	7.5	More Details
CVE-2023-4591	A local file inclusion vulnerability has been found in WPN-XM Serverstack affecting version 0.8.6, which would allow an unauthenticated user to perform a local file inclusion (LFI) via the /tools/webinterface/index.php?page parameter by sending a GET request. This vulnerability could lead to the loading of a PHP file on the server, leading to a critical webshell exploit.	7.5	More Details
CVE-2023-1718	Improper file stream access in /desktop_app/file.ajax.php?action=uploadfile in Bitrix24 22.0.300 allows unauthenticated remote attackers to cause denial-of-service via a crafted "tmp_url".	7.5	More Details
CVE-2023-20155	A vulnerability in a logging API in Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to cause the device to become unresponsive or trigger an unexpected reload. This vulnerability could also allow an attacker with valid user credentials, but not Administrator privileges, to view a system log file that they would not normally have access to. This vulnerability is due to a lack of rate-limiting of requests that are sent to a specific API that is related to an FMC log. An attacker could exploit this vulnerability by sending a high rate of HTTP requests to the API. A successful exploit could allow the attacker to cause a denial of service (DoS) condition due to the FMC CPU spiking to 100 percent utilization or to the device reloading. CPU utilization would return to normal if the attack traffic was stopped before an unexpected reload was triggered.	7.5	More Details
CVE-2023-5627	A vulnerability has been identified in NPort 6000 Series, making the authentication mechanism vulnerable. This vulnerability arises from the incorrect implementation of sensitive information protection, potentially allowing malicious users to gain unauthorized access to the web service.	7.5	More Details
CVE-2023-4197	Improper input validation in Dolibarr ERP CRM <= v18.0.1 fails to strip certain PHP code from user-supplied input when creating a Website, allowing an attacker to inject and evaluate arbitrary PHP code.	7.5	More Details
CVE-2023-46695	An issue was discovered in Django 3.2 before 3.2.23, 4.1 before 4.1.13, and 4.2 before 4.2.7. The NFKC normalization is slow on Windows. As a consequence, django.contrib.auth.forms.UsernameField is subject to a potential DoS (denial of service) attack via certain inputs with a very large number of Unicode characters.	7.5	More Details
CVE-2023-1719	Global variable extraction in bitrix/modules/main/tools.php in Bitrix24 22.0.300 allows unauthenticated remote attackers to (1) enumerate attachments on the server and (2) execute arbitrary JavaScript code in the victim's browser, and possibly execute arbitrary PHP code on the server if the victim has administrator privilege, via overwriting uninitialised variables.	7.5	More Details
CVE-2023-46730	Group-Office is an enterprise CRM and groupware tool. In affected versions there is full Server-Side Request Forgery (SSRF) vulnerability in the /api/upload.php endpoint. The /api/upload.php endpoint does not filter URLs which allows a malicious user to cause the server to make resource requests to untrusted domains. Note that protocols like file:// can also be used to access the server disk. The request result (on success) can then be retrieved using /api/download.php. This issue has been addressed in versions 6.8.15, 6.7.54, and 6.6.177. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.4	More Details
CVE-2023-31016	NVIDIA GPU Display Driver for Windows contains a vulnerability where an uncontrolled search path element may allow an attacker to execute arbitrary code, which may lead to code execution, denial of service, escalation of privileges, information disclosure, or data tampering.	7.3	More Details
CVE-2023-45827	Dot diver is a lightweight, powerful, and dependency-free TypeScript utility library that provides types and functions to work with object paths in dot notation. In versions prior to 1.0.2 there is a Prototype Pollution vulnerability in the `setByPath` function which can leads to remote code execution (RCE). This issue has been addressed in commit `98daf567` which has been included in release 1.0.2. Users are advised to upgrade. There are no known workarounds to this vulnerability.	7.3	More Details
CVE-2023-36034	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-20219	Multiple vulnerabilities in the web management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. The attacker would need valid device credentials but does not require administrator privileges to exploit this vulnerability. These vulnerabilities are due to insufficient validation of user-supplied input for certain configuration options. An attacker could exploit these vulnerabilities by using crafted input within the device configuration GUI. A successful exploit could allow the attacker to execute arbitrary commands on the device including the underlying operating system which could also affect the availability of the device.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46823	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Avirtum ImageLinks Interactive Image Builder for WordPress allows SQL Injection.This issue affects ImageLinks Interactive Image Builder for WordPress: from n/a through 1.5.4.	7.2	More Details
CVE-2023-46821	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Milan Petrovic GD Security Headers allows auth. (admin+) SQL Injection.This issue affects GD Security Headers: from n/a through 1.7.	7.2	More Details
CVE-2022-48192	Cross-site Scripting vulnerability in Softing smartLink SW-HT before 1.30, which allows an attacker to execute a dynamic script (JavaScript, VBScript) in the context of the application.	7.2	More Details
CVE-2023-32121	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Highfivery LLC Zero Spam for WordPress allows SQL Injection.This issue affects Zero Spam for WordPress: from n/a through 5.4.4.	7.2	More Details
CVE-2023-5082	The History Log by click5 WordPress plugin before 1.0.13 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by admin users when using the Smash Balloon Social Photo Feed plugin alongside it.	7.2	More Details
CVE-2023-5408	A privilege escalation flaw was found in the node restriction admission plugin of the kubernetes api server of OpenShift. A remote attacker who modifies the node role label could steer workloads from the control plane and etcd nodes onto different worker nodes and gain broader access to the cluster.	7.2	More Details
CVE-2023-32508	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Rolf van Gelder Order Your Posts Manually allows SQL Injection.This issue affects Order Your Posts Manually: from n/a through 2.2.5.	7.2	More Details
CVE-2023-34179	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Groundhogg Inc. Groundhogg allows SQL Injection.This issue affects Groundhogg: from n/a through 2.7.11.	7.2	More Details
CVE-2023-40215	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Demonisblack demon image annotation allows SQL Injection.This issue affects demon image annotation: from n/a through 5.1.	7.2	More Details
CVE-2023-38391	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themesgrove Onepage Builder allows SQL Injection.This issue affects Onepage Builder: from n/a through 2.4.1.	7.2	More Details
CVE-2023-20220	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. To exploit these vulnerabilities, the attacker must have valid device credentials, but does not need Administrator privileges. These vulnerabilities are due to insufficient validation of user-supplied input for certain configuration options. An attacker could exploit these vulnerabilities by using crafted input within the device configuration GUI. A successful exploit could allow the attacker to execute arbitrary commands on the device, including on the underlying operating system, which could also affect the availability of the device.	7.2	More Details
CVE-2023-32741	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in IT Path Solutions PVT LTD Contact Form to Any API allows SQL Injection.This issue affects Contact Form to Any API: from n/a through 1.1.2.	7.2	More Details
CVE-2023-46845	EC-CUBE 3 series (3.0.0 to 3.0.18-p6) and 4 series (4.0.0 to 4.0.6-p3, 4.1.0 to 4.1.2-p2, and 4.2.0 to 4.2.2) contain an arbitrary code execution vulnerability due to improper settings of the template engine Twig included in the product. As a result, arbitrary code may be executed on the server where the product is running by a user with an administrative privilege.	7.2	More Details
CVE-2023-5860	The Icons Font Loader plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the upload function in all versions up to, and including, 1.1.2. This makes it possible for authenticated attackers, with administrator-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	7.2	More Details
CVE-2023-41352	Chunghwa Telecom NOKIA G-040W-Q has a vulnerability of insufficient filtering for user input. A remote attacker with administrator privilege can exploit this vulnerability to perform a Command Injection attack to execute arbitrary commands, disrupt the system or terminate services.	7.2	More Details
CVE-2022-45078	Improper Neutralization of Formula Elements in a CSV File vulnerability in Solwin Infotech User Blocker.This issue affects User Blocker: from n/a through 1.5.5.	7.2	More Details
CVE-2023-23678	Improper Neutralization of Formula Elements in a CSV File vulnerability in WPEkaClub WP Cookie Consent (for GDPR, CCPA & ePrivacy).This issue affects WP Cookie Consent (for GDPR, CCPA & ePrivacy): from n/a through 2.2.5.	7.2	More Details
CVE-2023-43886	A buffer overflow in the HTTP server component of Tenda RX9 Pro v22.03.02.20 might allow an authenticated attacker to overwrite memory.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-28407	In swtpm before 0.4.2 and 0.5.x before 0.5.1, a local attacker may be able to overwrite arbitrary files via a symlink attack against a temporary file such as TMP2-00.permall.	7.1	More Details
CVE-2023-28556	Cryptographic issue in HLOS during key management.	7.1	More Details
CVE-2023-1194	An out-of-bounds (OOB) memory read flaw was found in parse_lease_state in the KSMBD implementation of the in-kernel samba server and CIFS in the Linux kernel. When an attacker sends the CREATE command with a malformed payload to KSMBD, due to a missing check of `NameOffset` in the `parse_lease_state()` function, the `create_context` object can access invalid memory.	7.1	More Details
CVE-2023-41914	SchedMD Slurm 23.02.x before 23.02.6 and 22.05.x before 22.05.10 allows filesystem race conditions for gaining ownership of a file, overwriting a file, or deleting files.	7.0	More Details
CVE-2023-32832	In video, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08235273; Issue ID: ALPS08235273.	7.0	More Details
CVE-2023-1476	A use-after-free flaw was found in the Linux kernel's mm/mremap memory address space accounting source code. This issue occurs due to a race condition between rmap walk and mremap, allowing a local user to crash the system or potentially escalate their privileges on the system.	7.0	More Details
CVE-2023-3397	A race condition occurred between the functions lmLogClose and txEnd in JFS, in the Linux Kernel, executed in different threads. This flaw allows a local attacker with normal user privileges to crash the system or leak internal kernel information.	7.0	More Details
CVE-2023-20042	A vulnerability in the AnyConnect SSL VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to an implementation error within the SSL/TLS session handling process that can prevent the release of a session handler under specific conditions. An attacker could exploit this vulnerability by sending crafted SSL/TLS traffic to an affected device, increasing the probability of session handler leaks. A successful exploit could allow the attacker to eventually deplete the available session handler pool, preventing new sessions from being established and causing a DoS condition.	6.8	More Details
CVE-2023-5309	Versions of Puppet Enterprise prior to 2021.7.6 and 2023.5 contain a flaw which results in broken session management for SAML implementations.	6.8	More Details
CVE-2023-46252	Squidex is an open source headless CMS and content management hub. Affected versions are missing origin verification in a postMessage handler which introduces a Cross-Site Scripting (XSS) vulnerability. The editor-sdk.js file defines three different class-like functions, which employ a global message event listener: SquidexSidebar, SquidexWidget, and SquidexFormField. The registered event listener takes some action based on the type of the received message. For example, when the SquidexFormField receives a message with the type valueChanged, the value property is updated. The SquidexFormField class is for example used in the editor-editorjs.html file, which can be accessed via the public wwwroot folder. It uses the onValueChanged method to register a callback function, which passes the value provided from the message event to the editor.render. Passing an attacker-controlled value to this function introduces a Cross-Site Scripting (XSS) vulnerability.	6.8	More Details
CVE-2023-5763	In Eclipse Glassfish 5 or 6, running with old versions of JDK (lower than 6u211, or < 7u201, or < 8u191), allows remote attackers to load malicious code on the server via access to insecure ORB listeners.	6.8	More Details
CVE-2023-42655	In sim service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local escalation of privilege with System execution privileges needed	6.7	More Details
CVE-2023-46176	IBM MQ Appliance 9.3 CD could allow a local attacker to gain elevated privileges on the system, caused by improper validation of security keys. IBM X-Force ID: 269535.	6.7	More Details
CVE-2023-28570	Memory corruption while processing audio effects.	6.7	More Details
CVE-2023-32818	In vdec, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08163896 & ALPS08013430; Issue ID: ALPS07867715.	6.7	More Details
CVE-2023-32834	In secmem, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08161762; Issue ID: ALPS08161762.	6.7	More Details
CVE-2023-30739	Arbitrary File Descriptor Write vulnerability in libsec-ril prior to SMR Nov-2023 Release 1 allows local attacker to execute arbitrary code.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32835	In keyinstall, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08157918; Issue ID: ALPS08157918.	6.7	More Details
CVE-2023-32836	In display, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08126725; Issue ID: ALPS08126725.	6.7	More Details
CVE-2023-32838	In dpe, there is a possible out of bounds write due to a missing valid range checking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310805; Issue ID: ALPS07310805.	6.7	More Details
CVE-2023-32839	In dpe, there is a possible out of bounds write due to a missing valid range checking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262576; Issue ID: ALPS07262576.	6.7	More Details
CVE-2023-5847	Under certain conditions, a low privileged attacker could load a specially crafted file during installation or upgrade to escalate privileges on Windows and Linux hosts.	6.7	More Details
CVE-2023-42528	Improper Input Validation vulnerability in ProcessNvBuffering of libsec-ril prior to SMR Nov-2023 Release 1 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2023-42530	Improper access control vulnerability in SecSettings prior to SMR Nov-2023 Release 1 allows attackers to enable Wi-Fi and Wi-Fi Direct without User Interaction.	6.7	More Details
CVE-2023-42529	Out-of-bound write vulnerability in libsec-ril prior to SMR Nov-2023 Release 1 allows local attackers to execute arbitrary code.	6.7	More Details
CVE-2023-4769	A SSRF vulnerability has been found in ManageEngine Desktop Central affecting version 9.1.0, specifically the /smtpConfig.do component. This vulnerability could allow an authenticated attacker to launch targeted attacks, such as a cross-port attack, service enumeration and other attacks via HTTP requests.	6.6	More Details
CVE-2023-4996	Netskope was made aware of a security vulnerability in its NSClient product for version 100 & prior where a malicious non-admin user can disable the Netskope client by using a specially-crafted package. The root cause of the problem was a user control code when called by a Windows ServiceController did not validate the permissions associated with the user before executing the user control code. This user control code had permissions to terminate the NSClient service.	6.6	More Details
CVE-2023-36022	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	6.6	More Details
CVE-2023-40660	A flaw was found in OpenSC packages that allow a potential PIN bypass. When a token/card is authenticated by one process, it can perform cryptographic operations in other processes when an empty zero-length pin is passed. This issue poses a security risk, particularly for OS logon/screen unlock and for small, permanently connected tokens to computers. Additionally, the token can internally track login status. This flaw allows an attacker to gain unauthorized access, carry out malicious actions, or compromise the system without the user's awareness.	6.6	More Details
CVE-2023-42533	Improper Input Validation with USB Gadget Interface prior to SMR Nov-2023 Release 1 allows a physical attacker to execute arbitrary code in Kernel.	6.6	More Details
CVE-2023-28572	Memory corruption in WLAN HOST while processing the WLAN scan descriptor list.	6.6	More Details
CVE-2023-45189	A vulnerability in IBM Robotic Process Automation and IBM Robotic Process Automation for Cloud Pak 21.0.0 through 21.0.7.10, 23.0.0 through 23.0.10 may result in access to client vault credentials. This difficult to exploit vulnerability could allow a low privileged attacker to programmatically access client vault credentials. IBM X-Force ID: 268752.	6.5	More Details
CVE-2023-40453	Docker Machine through 0.16.2 allows an attacker, who has control of a worker node, to provide crafted version data, which might potentially trick an administrator into performing an unsafe action (via escape sequence injection), or might have a data size that causes a denial of service to a bastion node. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	6.5	More Details
CVE-2023-4956	A flaw was found in Quay. Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they intend to click on the top-level page. During the pentest, it has been detected that the config-editor page is vulnerable to clickjacking. This flaw allows an attacker to trick an administrator user into clicking on buttons on the config-editor panel, possibly reconfiguring some parts of the Quay instance.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2621	The McFeeder server (distributed as part of SSW package), is susceptible to an arbitrary file write vulnerability on the MAIN computer system. This vulnerability stems from the use of an outdated version of a third-party library, which is used to extract archives uploaded to McFeeder server. An authenticated malicious client can exploit this vulnerability by uploading a crafted ZIP archive via the network to McFeeder's service endpoint.	6.5	More Details
CVE-2023-4198	Improper Access Control in Dolibarr ERP CRM <= v17.0.3 allows an unauthorized authenticated user to read a database table containing customer data	6.5	More Details
CVE-2023-1193	A use-after-free flaw was found in setup_async_work in the KSMBD implementation of the in-kernel samba server and CIFS in the Linux kernel. This issue could allow an attacker to crash the system by accessing freed work.	6.5	More Details
CVE-2023-1192	A use-after-free flaw was found in smb2_is_status_io_timeout() in CIFS in the Linux Kernel. After CIFS transfers response data to a system call, there are still local variable points to the memory region, and if the system call frees it faster than CIFS uses it, CIFS will access a free memory region, leading to a denial of service.	6.5	More Details
CVE-2023-41356	NCSIST ManageEngine Mobile Device Manager(MDM) APP's special function has a path traversal vulnerability. An unauthenticated remote attacker can exploit this vulnerability to bypass authentication and read arbitrary system files.	6.5	More Details
CVE-2023-36409	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	6.5	More Details
CVE-2023-20114	A vulnerability in the file download feature of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to download arbitrary files from an affected system. This vulnerability is due to a lack of input sanitation. An attacker could exploit this vulnerability by sending a crafted HTTPS request. A successful exploit could allow the attacker to download arbitrary files from the affected system.	6.5	More Details
CVE-2023-42670	A flaw was found in Samba. It is susceptible to a vulnerability where multiple incompatible RPC listeners can be initiated, causing disruptions in the AD DC service. When Samba's RPC server experiences a high load or unresponsiveness, servers intended for non-AD DC purposes (for example, NT4-emulation "classic DCs") can erroneously start and compete for the same unix domain sockets. This issue leads to partial query responses from the AD DC, causing issues such as "The procedure number is out of range" when using tools like Active Directory Users. This flaw allows an attacker to disrupt AD DC services.	6.5	More Details
CVE-2023-4930	The Front End PM WordPress plugin before 11.4.3 does not block listing the contents of the directories where it stores attachments to private messages, allowing unauthenticated visitors to list and download private attachments if the autoindex feature of the web server is enabled.	6.5	More Details
CVE-2023-4091	A vulnerability was discovered in Samba, where the flaw allows SMB clients to truncate files, even with read-only permissions when the Samba VFS module "acl_xattr" is configured with "acl_xattr:ignore system acls = yes". The SMB protocol allows opening files when the client requests read-only access but then implicitly truncates the opened file to 0 bytes if the client specifies a separate OVERWRITE create disposition request. The issue arises in configurations that bypass kernel file system permissions checks, relying solely on Samba's permissions.	6.5	More Details
CVE-2023-5825	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.2 before 16.3.6, all versions starting from 16.4 before 16.4.2, all versions starting from 16.5 before 16.5.1. A low-privileged attacker can point a CI/CD Component to an incorrect path and cause the server to exhaust all available memory through an infinite loop and cause Denial of Service.	6.5	More Details
CVE-2023-4452	A vulnerability has been identified in the EDR-810, EDR-G902, and EDR-G903 Series, making them vulnerable to the denial-of-service vulnerability. This vulnerability stems from insufficient input validation in the URI, potentially enabling malicious users to trigger the device reboot.	6.5	More Details
CVE-2023-42669	A vulnerability was found in Samba's "rpcecho" development server, a non-Windows RPC server used to test Samba's DCE/RPC stack elements. This vulnerability stems from an RPC function that can be blocked indefinitely. The issue arises because the "rpcecho" service operates with only one worker in the main RPC task, allowing calls to the "rpcecho" server to be blocked for a specified time, causing service disruptions. This disruption is triggered by a "sleep()" call in the "dcesrv_echo_TestSleep()" function under specific conditions. Authenticated users or attackers can exploit this vulnerability to make calls to the "rpcecho" server, requesting it to block for a specified duration, effectively disrupting most services and leading to a complete denial of service on the AD DC. The DoS affects all other services as "rpcecho" runs in the main RPC task.	6.5	More Details
CVE-2023-47249	In International Color Consortium DemoIccMAX 79ecb74, a CIccXmlArrayType:::ParseText function (for unsigned short) in IccUtilXml.cpp in libIccXML.a has an out-of-bounds read.	6.5	More Details
CVE-2023-32840	In modem CCCI, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction may be also needed for exploitation Patch ID: MOLY01138425; Issue ID: MOLY01138425 (MSV-862).	6.5	More Details
CVE-2023-46278	Uncontrolled resource consumption vulnerability in Cybozu Remote Service 4.1.0 to 4.1.1 allows a remote authenticated attacker to consume huge storage space or cause significantly delayed communication.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43076	Dell PowerScale OneFS 8.2.x,9.0.0.x-9.5.0.x contains a denial-of-service vulnerability. A low privilege remote attacker could potentially exploit this vulnerability to cause an out of memory (OOM) condition.	6.5	More Details
CVE-2023-31018	NVIDIA GPU Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where an unprivileged regular user can cause a NULL-pointer dereference, which may lead to denial of service.	6.5	More Details
CVE-2023-5707	The SEO Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'slider' shortcode and post meta in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5659	The Interact: Embed A Quiz On Your Site plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'interact-quiz' shortcode in all versions up to, and including, 3.0.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5660	The SendPress Newsletters plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.22.3.31 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-2023-5567	The QR Code Tag plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'qrcodetag' shortcode in versions up to, and including, 1.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-4888	The Simple Like Page Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'sfp-page-plugin' shortcode in versions up to, and including, 1.5.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5661	The Social Feed plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'socialfeed' shortcode in all versions up to, and including, 1.5.4.6 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with author-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-2023-5669	The Featured Image Caption plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode and post meta in all versions up to, and including, 0.8.10 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-2023-4842	The Social Sharing Plugin - Social Warfare plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'social_warfare' shortcode in versions up to, and including, 4.4.3 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-2023-5743	The Telephone Number Linker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'telnumlink' shortcode in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5658	The WP MapIt plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wp_mapit' shortcode in all versions up to, and including, 2.7.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5703	The Gift Up Gift Cards for WordPress and WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'giftup' shortcode in all versions up to, and including, 2.20.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5507	The ImageMapper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'imagemap' shortcode in versions up to, and including, 1.2.6 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-2023-5088	A bug in QEMU could cause a guest I/O operation otherwise addressed to an arbitrary disk offset to be targeted to offset 0 instead (potentially overwriting the VM's boot code). This could be used, for example, by L2 guests with a virtual disk (vdiskL2) stored on a virtual disk of an L1 (vdiskL1) hypervisor to read and/or write data to LBA 0 of vdiskL1, potentially gaining control of L1 at its next reboot.	6.4	More Details
CVE-2023-5076	The Ziteboard Online Whiteboard plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'ziteboard' shortcode in versions up to, and including, 2.9.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5577	The Bitly's plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpbitly' shortcode in all versions up to, and including, 2.7.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-42555	Use of implicit intent for sensitive communication vulnerability in EasySetup prior to version 11.1.13 allows attackers to get the bluetooth address of user device.	6.3	More Details
CVE-2023-42534	Improper input validation vulnerability in ChooserActivity prior to SMR Nov-2023 Release 1 allows local attackers to read arbitrary files with system privilege.	6.3	More Details
CVE-2023-5918	A vulnerability, which was classified as critical, was found in SourceCodester Visitor 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. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-244308.	6.3	More Details
CVE-2023-38470	A vulnerability was found in Avahi. A reachable assertion exists in the avahi_escape_label() function.	6.2	More Details
CVE-2023-38473	A vulnerability was found in Avahi. A reachable assertion exists in the avahi_alternative_host_name() function.	6.2	More Details
CVE-2022-4900	A vulnerability was found in PHP where setting the environment variable PHP_CLI_SERVER_WORKERS to a large value leads to a heap buffer overflow.	6.2	More Details
CVE-2023-38469	A vulnerability was found in Avahi, where a reachable assertion exists in avahi_dns_packet_append_record.	6.2	More Details
CVE-2023-38471	A vulnerability was found in Avahi. A reachable assertion exists in the dbus_set_host_name function.	6.2	More Details
CVE-2023-38472	A vulnerability was found in Avahi. A reachable assertion exists in the avahi_rdata_parse() function.	6.2	More Details
CVE-2023-42543	Improper verification of intent by broadcast receiver vulnerability in Bixby Voice prior to version 3.3.35.12 allows attackers to access arbitrary data with Bixby Voice privilege.	6.2	More Details
CVE-2023-42531	Improper access control vulnerability in SmsController prior to SMR Nov-2023 Release1 allows local attackers to bypass restrictions on starting activities from the background.	6.2	More Details
CVE-2023-28553	Information Disclosure in WLAN Host when processing WMI event command.	6.1	More Details
CVE-2023-5946	The Digirisk plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'current_group_id' parameter in version 6.0.0.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-46998	Cross Site Scripting vulnerability in BootBox Bootbox.js v.3.2 through 6.0 allows a remote attacker to execute arbitrary code via a crafted payload to alert(), confirm(), prompt() functions.	6.1	More Details
CVE-2023-47510	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WPSolutions-HQ WPDBSpringClean plugin <= 1.6 versions.	6.1	More Details
CVE-2023-46822	Unauth. Reflected Cross-Site Scripting') vulnerability in Visser Labs Store Exporter for WooCommerce – Export Products, Export Orders, Export Subscriptions, and More plugin <= 2.7.2 versions.	6.1	More Details
CVE-2023-46911	There is a Cross Site Scripting (XSS) vulnerability in the choose_style_tree.do interface of Jspxcms v10.2.0 backend.	6.1	More Details
CVE-2023-47272	Roundcube 1.5.x before 1.5.6 and 1.6.x before 1.6.5 allows XSS via a Content-Type or Content-Disposition header (used for attachment preview or download).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-20206	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	6.1	More Details
CVE-2019-25155	DOMPurify before 1.0.11 allows reverse tabnabbing in demos/hooks-target-blank-demo.html because links lack a 'rel="noopener noreferrer"' attribute.	6.1	More Details
CVE-2023-5771	Proofpoint Enterprise Protection contains a stored XSS vulnerability in the AdminUI. An unauthenticated attacker can send a specially crafted email with HTML in the subject which triggers XSS when viewing quarantined messages. This issue affects Proofpoint Enterprise Protection: from 8.20.0 before patch 4796, from 8.18.6 before patch 4795 and all other prior versions.	6.1	More Details
CVE-2023-5354	The Awesome Support WordPress plugin before 6.1.5 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	6.1	More Details
CVE-2023-41425	Cross Site Scripting vulnerability in Wonder CMS v.3.2.0 thru v.3.4.2 allows a remote attacker to execute arbitrary code via a crafted script uploaded to the installModule component.	6.1	More Details
CVE-2023-31020	NVIDIA GPU Display Driver for Windows contains a vulnerability in the kernel mode layer, where an unprivileged regular user can cause improper access control, which may lead to denial of service or data tampering.	6.1	More Details
CVE-2023-46964	Cross Site Scripting (XSS) vulnerability in Hillstone Next Generation FireWall SG-6000-e3960 v.5.5 allows a remote attacker to execute arbitrary code via the use front-end filtering instead of back-end filtering.	6.1	More Details
CVE-2023-47258	Redmine before 4.2.11 and 5.0.x before 5.0.6 allows XSS in a Markdown formatter.	6.1	More Details
CVE-2023-47259	Redmine before 4.2.11 and 5.0.x before 5.0.6 allows XSS in the Textile formatter.	6.1	More Details
CVE-2023-28554	Information Disclosure in Qualcomm IPC while reading values from shared memory in VM.	6.1	More Details
CVE-2023-47260	Redmine before 4.2.11 and 5.0.x before 5.0.6 allows XSS via thumbnails.	6.1	More Details
CVE-2023-5532	The ImageMapper plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.6. This is due to missing or incorrect nonce validation on the 'imgmap_save_area_title' function. This makes it possible for unauthenticated attackers to update the post title and inject malicious JavaScript via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-4592	A Cross-Site Scripting vulnerability has been detected in WPN-XM Serverstack affecting version 0.8.6. This vulnerability could allow a remote attacker to send a specially crafted JavaScript payload through the /tools/webinterface/index.php parameter and retrieve the cookie session details of an authenticated user, resulting in a session hijacking.	6.1	More Details
CVE-2023-28569	Information disclosure in WLAN HAL while handling command through WMI interfaces.	6.1	More Details
CVE-2023-46448	Reflected Cross-Site Scripting (XSS) vulnerability in dmpop Mejiro Commit Versions Prior To 3096393 allows attackers to run arbitrary code via crafted string in metadata of uploaded images.	6.1	More Details
CVE-2023-45201	Online Examination System v1.0 is vulnerable to multiple Open Redirect vulnerabilities. The 'q' parameter of the admin.php resource allows an attacker to redirect a victim user to an arbitrary web site using a crafted URL.	6.1	More Details
CVE-2023-45202	Online Examination System v1.0 is vulnerable to multiple Open Redirect vulnerabilities. The 'q' parameter of the feed.php resource allows an attacker to redirect a victim user to an arbitrary web site using a crafted URL.	6.1	More Details
CVE-2023-29043	Presentations may contain references to images, which are user-controlled, and could include malicious script code that is being processed when editing a document. Script code embedded in malicious documents could be executed in the context of the user editing the document when performing certain actions, like copying content. The relevant attribute does now get encoded to avoid the possibility of executing script code. No publicly available exploits are known.	6.1	More Details
CVE-2023-5480	Inappropriate implementation in Payments in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to bypass XSS preventions via a malicious file. (Chromium security severity: High)	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28563	Information disclosure in IOE Firmware while handling WMI command.	6.1	More Details
CVE-2023-45203	Online Examination System v1.0 is vulnerable to multiple Open Redirect vulnerabilities. The 'q' parameter of the login.php resource allows an attacker to redirect a victim user to an arbitrary web site using a crafted URL.	6.1	More Details
CVE-2023-20264	A vulnerability in the implementation of Security Assertion Markup Language (SAML) 2.0 single sign-on (SSO) for remote access VPN in Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to intercept the SAML assertion of a user who is authenticating to a remote access VPN session. This vulnerability is due to insufficient validation of the login URL. An attacker could exploit this vulnerability by persuading a user to access a site that is under the control of the attacker, allowing the attacker to modify the login URL. A successful exploit could allow the attacker to intercept a successful SAML assertion and use that assertion to establish a remote access VPN session toward the affected device with the identity and permissions of the hijacked user, resulting in access to the protected network.	6.1	More Details
CVE-2023-43193	Submitty before v22.06.00 is vulnerable to Cross Site Scripting (XSS). An attacker can create a malicious link in the forum that leads to XSS.	6.1	More Details
CVE-2023-32966	Cross-Site Request Forgery (CSRF) vulnerability in CRUDLab Jazz Popups leads to Stored XSS.This issue affects Jazz Popups: from n/a through 1.8.7.	6.1	More Details
CVE-2023-47185	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in gVectors Team Comments — wpDiscuz plugin <= 7.6.11 versions.	6.1	More Details
CVE-2023-28566	Information disclosure in WLAN HAL while handling the WMI state info command.	6.1	More Details
CVE-2023-4768	A CRLF injection vulnerability has been found in ManageEngine Desktop Central affecting version 9.1.0. This vulnerability could allow a remote attacker to inject arbitrary HTTP headers and perform HTTP response splitting attacks via the fileName parameter in /STATE_ID/1613157927228/InvSWMetering.pdf.	6.1	More Details
CVE-2023-4767	A CRLF injection vulnerability has been found in ManageEngine Desktop Central affecting version 9.1.0. This vulnerability could allow a remote attacker to inject arbitrary HTTP headers and perform HTTP response splitting attacks via the fileName parameter in /STATE_ID/1613157927228/InvSWMetering.csv.	6.1	More Details
CVE-2023-28568	Information disclosure in WLAN HAL when reception status handler is called.	6.1	More Details
CVE-2023-5090	A flaw was found in KVM. An improper check in svm_set_x2apic_msr_interception() may allow direct access to host x2apic msrs when the guest resets its apic, potentially leading to a denial of service condition.	6.0	More Details
CVE-2023-20170	A vulnerability in a specific Cisco ISE CLI command could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, an attacker must have valid Administrator-level privileges on the affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	6.0	More Details
CVE-2023-31026	NVIDIA vGPU software for Windows and Linux contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where a NULL-pointer dereference may lead to denial of service.	6.0	More Details
CVE-2023-43018	IBM CICS TX Standard 11.1 and Advanced 10.1, 11.1 performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses. IBM X-Force ID: 266163.	5.9	More Details
CVE-2023-42538	An improper input validation in saped_rec_silence in libsaped prior to SMR Nov-2023 Release 1 allows local attackers to cause out-of-bounds read and write.	5.9	More Details
CVE-2023-46595	Net-NTLM leak via HTML injection in FireFlow VisualFlow workflow editor allows an attacker to obtain victim’s domain credentials and Net-NTLM hash which can lead to relay domain attacks. Fixed in A32.20 (b570 or above), A32.50 (b390 or above)	5.9	More Details
CVE-2023-42532	Improper Certificate Validation in FotaAgent prior to SMR Nov-2023 Release1 allows remote attacker to intercept the network traffic including Firmware information.	5.9	More Details
CVE-2023-4043	In Eclipse Parsson before versions 1.1.4 and 1.0.5, Parsing JSON from untrusted sources can lead malicious actors to exploit the fact that the built-in support for parsing numbers with large scale in Java has a number of edge cases where the input text of a number can lead to much larger processing time than one would expect. To mitigate the risk, parsson put in place a size limit for the numbers as well as their scale.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46327	Multiple MFPs (multifunction printers) provided by FUJIFILM Business Innovation Corp. and Xerox Corporation provide a facility to export the contents of their Address Book with encrypted form, but the encryption strength is insufficient. With the knowledge of the encryption process and the encryption key, the information such as the server credentials may be obtained from the exported Address Book data. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	5.9	More Details
CVE-2022-48193	Weak ciphers in Softing smartLink SW-HT before 1.30 are enabled during secure communication (SSL).	5.9	More Details
CVE-2023-20246	Multiple Cisco products are affected by a vulnerability in Snort access control policies that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. This vulnerability is due to a logic error that occurs when the access control policies are being populated. An attacker could exploit this vulnerability by establishing a connection to an affected device. A successful exploit could allow the attacker to bypass configured access control rules on the affected system.	5.8	More Details
CVE-2023-20270	A vulnerability in the interaction between the Server Message Block (SMB) protocol preprocessor and the Snort 3 detection engine for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass the configured policies or cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper error-checking when the Snort 3 detection engine is processing SMB traffic. An attacker could exploit this vulnerability by sending a crafted SMB packet stream through an affected device. A successful exploit could allow the attacker to cause the Snort process to reload, resulting in a DoS condition.	5.8	More Details
CVE-2023-20071	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass the configured policies on an affected system. This vulnerability is due to a flaw in the FTP module of the Snort detection engine. An attacker could exploit this vulnerability by sending crafted FTP traffic through an affected device. A successful exploit could allow the attacker to bypass FTP inspection and deliver a malicious payload.	5.8	More Details
CVE-2023-20245	Multiple vulnerabilities in the per-user-override feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass a configured access control list (ACL) and allow traffic that should be denied to flow through an affected device. These vulnerabilities are due to a logic error that could occur when the affected software constructs and applies per-user-override rules. An attacker could exploit these vulnerabilities by connecting to a network through an affected device that has a vulnerable configuration. A successful exploit could allow the attacker to bypass the interface ACL and access resources that would should be protected.	5.8	More Details
CVE-2023-42527	Improper input validation vulnerability in ProcessWriteFile of libsec-ril prior to SMR Nov-2023 Release 1 allows local attackers to expose sensitive information.	5.6	More Details
CVE-2023-26455	RMI was not requiring authentication when calling ChronosRMIService:setEventOrganizer. Attackers with local or adjacent network access could abuse the RMI service to modify calendar items using RMI. RMI access is restricted to localhost by default. The interface has been updated to require authenticated requests. No publicly available exploits are known.	5.6	More Details
CVE-2023-46930	GPAC 2.3-DEV-rev605-gfc9e29089-master contains a SEGV in gpac/MP4Box in gf_isom_find_od_id_for_track /afltest/gpac/src/isomedia/media_odf.c:522:14.	5.5	More Details
CVE-2023-46931	GPAC 2.3-DEV-rev605-gfc9e29089-master contains a heap-buffer-overflow in ffdmx_parse_side_data /afltest/gpac/src/filters/ff_dmx.c:202:14 in gpac/MP4Box.	5.5	More Details
CVE-2023-42650	In engineermode, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42651	In engineermode, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42545	Use of implicit intent for sensitive communication vulnerability in Phone prior to versions 12.7.20.12 in Android 11, 13.1.48, 13.5.28 in Android 12, and 14.7.38 in Android 13 allows attackers to access location data.	5.5	More Details
CVE-2023-42549	Use of implicit intent for sensitive communication vulnerability in startNameValidationActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	5.5	More Details
CVE-2023-42548	Use of implicit intent for sensitive communication vulnerability in startMandatoryCheckActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	5.5	More Details
CVE-2022-48457	In TeleService, there is a possible system crash due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-4910	A flaw was found In 3Scale Admin Portal. If a user logs out from the personal tokens page and then presses the back button in the browser, the tokens page is rendered from the browser cache.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48459	In TeleService, there is a possible system crash due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-46927	GPAC 2.3-DEV-rev605-gfc9e29089-master contains a heap-buffer-overflow in gf_isom_use_compact_size gpac/src/isomedia/isom_write.c:3403:3 in gpac/MP4Box.	5.5	More Details
CVE-2023-42652	In engineermode, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42550	Use of implicit intent for sensitive communication vulnerability in startSignIn in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	5.5	More Details
CVE-2023-42653	In faceid service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges	5.5	More Details
CVE-2023-42654	In dm service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42544	Improper access control vulnerability in Quick Share prior to 13.5.52.0 allows local attacker to access local files.	5.5	More Details
CVE-2023-42641	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2022-48458	In TeleService, there is a possible system crash due to improper input validation. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-42644	In dm service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42643	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42638	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42635	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42634	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-35140	The improper privilege management vulnerability in the Zyxel GS1900-24EP switch firmware version V2.70(ABTO.5) could allow an authenticated local user with read-only access to modify system settings on a vulnerable device.	5.5	More Details
CVE-2023-42645	In sim service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42636	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42633	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42632	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42640	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42631	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2022-48460	In setting service, there is a possible undefined behavior due to incorrect error handling. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-42639	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42646	In Ifaa service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42642	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42648	In engineermode, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42551	Use of implicit intent for sensitive communication vulnerability in startTncActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	5.5	More Details
CVE-2023-42649	In engineermode, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42637	In validationtools, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42647	In Ifaa service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-42546	Use of implicit intent for sensitive communication vulnerability in startAgreeToDisclaimerActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	5.5	More Details
CVE-2023-4272	A local non-privileged user can make GPU processing operations that expose sensitive data from previously freed memory.	5.5	More Details
CVE-2022-48454	In wifi service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-5924	A vulnerability classified as critical was found in Campcodes Simple Student Information System 1.0. This vulnerability affects unknown code of the file /admin/courses/view_course.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-244324.	5.5	More Details
CVE-2023-5925	A vulnerability, which was classified as critical, has been found in Campcodes Simple Student Information System 1.0. This issue affects some unknown processing of the file /classes/Master.php. The manipulation of the argument f leads to sql injection. The exploit has been disclosed to the public and may be used. The identifier VDB-244325 was assigned to this vulnerability.	5.5	More Details
CVE-2023-31023	NVIDIA Display Driver for Windows contains a vulnerability where an attacker may cause a pointer dereference of an untrusted value, which may lead to denial of service.	5.5	More Details
CVE-2018-25092	A vulnerability was found in Vaerys-Dawn DiscordSailv2 up to 2.10.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Command Mention Handler. The manipulation leads to improper access controls. Upgrading to version 2.10.3 is able to address this issue. The patch is named cc12e0be82a5d05d9f359ed8e56088f4f8b8eb69. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-244483.	5.5	More Details
CVE-2023-5926	A vulnerability, which was classified as critical, was found in Campcodes Simple Student Information System 1.0. Affected is an unknown function of the file /admin/students/update_status.php. The manipulation of the argument student_id leads to sql injection. The exploit has been disclosed to the public and may be used. VDB-244326 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2018-25093	A vulnerability was found in Vaerys-Dawn DiscordSailv2 up to 2.10.2. It has been rated as critical. Affected by this issue is some unknown functionality of the component Tag Handler. The manipulation leads to improper access controls. Upgrading to version 2.10.3 is able to address this issue. The name of the patch is cc12e0be82a5d05d9f359ed8e56088f4f8b8eb69. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-244484.	5.5	More Details
CVE-2023-46802	e-Tax software Version3.0.10 and earlier improperly restricts XML external entity references (XXE) due to the configuration of the embedded XML parser. By processing a specially crafted XML file, arbitrary files on the system may be read by an attacker.	5.5	More Details
CVE-2023-31022	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability in the kernel mode layer, where a NULL-pointer dereference may lead to denial of service.	5.5	More Details
CVE-2023-32825	In bluethooth service, there is a possible out of bounds reads due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07884130; Issue ID: ALPS07884130.	5.5	More Details
CVE-2023-31021	NVIDIA vGPU software for Windows and Linux contains a vulnerability in the Virtual GPU Manager (vGPU plugin), where a malicious user in the guest VM can cause a NULL-pointer dereference, which may lead to denial of service.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46928	GPAC 2.3-DEV-rev605-gfc9e29089-master contains a SEGV in gpac/MP4Box in gf_media_change_pl /afltest/gpac/src/media_tools/isom_tools.c:3293:42.	5.5	More Details
CVE-2023-5927	A vulnerability has been found in Campcodes Simple Student Information System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/courses/manage_course.php. The manipulation of the argument id leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-244327.	5.5	More Details
CVE-2023-5923	A vulnerability classified as critical has been found in Campcodes Simple Student Information System 1.0. This affects an unknown part of the file /admin/index.php. The manipulation of the argument id leads to sql injection. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-244323.	5.5	More Details
CVE-2022-48455	In wifi service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with no additional execution privileges needed	5.5	More Details
CVE-2023-5928	A vulnerability was found in Campcodes Simple Student Information System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/departments/manage_department.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-244328.	5.5	More Details
CVE-2023-42547	Use of implicit intent for sensitive communication vulnerability in startEmailValidationActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	5.5	More Details
CVE-2023-3164	A heap-buffer-overflow vulnerability was found in LibTIFF, in extractImageSection() at tools/tiffcrop.c:7916 and tools/tiffcrop.c:7801. This flaw allows attackers to cause a denial of service via a crafted tiff file.	5.5	More Details
CVE-2023-5929	A vulnerability was found in Campcodes Simple Student Information System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/students/manage_academic.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 VDB-244329 was assigned to this vulnerability.	5.5	More Details
CVE-2023-5948	Improper Authorization in GitHub repository teamamaze/amazefileutilities prior to 1.91.	5.5	More Details
CVE-2023-39284	An issue was discovered in IhisiServicesSmm in Insyde InsydeH2O with kernel 5.0 through 5.5. There are arbitrary calls to SetVariable with unsanitized arguments in the SMI handler.	5.5	More Details
CVE-2023-46001	Buffer Overflow vulnerability in gpac MP4Box v.2.3-DEV-rev573-g201320819-master allows a local attacker to cause a denial of service via the gpac/src/isomedia/isom_read.c:2807:51 function in gf_isom_get_user_data.	5.5	More Details
CVE-2023-46475	A Stored Cross-Site Scripting vulnerability was discovered in ZenTao 18.3 where a user can create a project, and in the name field of the project, they can inject malicious JavaScript code.	5.4	More Details
CVE-2023-5895	Cross-site Scripting (XSS) - DOM in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	5.4	More Details
CVE-2023-5894	Cross-site Scripting (XSS) - Stored in GitHub repository pkp/ojs prior to 3.3.0-16.	5.4	More Details
CVE-2023-38549	A vulnerability in Veeam ONE allows an unprivileged user who has access to the Veeam ONE Web Client the ability to acquire the NTLM hash of the account used by the Veeam ONE Reporting Service. Note: The criticality of this vulnerability is reduced as it requires interaction by a user with the Veeam ONE Administrator role.	5.4	More Details
CVE-2023-5903	Cross-site Scripting (XSS) - Stored in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	5.4	More Details
CVE-2023-47094	A Stored Cross-Site Scripting (XSS) vulnerability in the Account Plans tab of System Settings in Virtualmin 7.7 allows remote attackers to inject arbitrary web script or HTML via the Plan name field while editing Account plan details.	5.4	More Details
CVE-2023-45556	Cross Site Scripting vulnerability in Mybb Mybb Forums v.1.8.33 allows a local attacker to execute arbitrary code via the theme Name parameter in the theme management component.	5.4	More Details
CVE-2023-5506	The ImageMapper plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'imgmap_delete_area_ajax' function in versions up to, and including, 1.2.6. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to delete arbitrary posts and pages.	5.4	More Details
CVE-2023-44954	Cross Site Scripting vulnerability in BigTree CMS v.4.5.7 allows a remote attacker to execute arbitrary code via the ID parameter in the Developer Settings functions.	5.4	More Details
CVE-2023-47099	A Stored Cross-Site Scripting (XSS) vulnerability in the Create Virtual Server in Virtualmin 7.7 allows remote attackers to inject arbitrary web script or HTML via Description field while creating the Virtual server.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45360	An issue was discovered in MediaWiki before 1.35.12, 1.36.x through 1.39.x before 1.39.5, and 1.40.x before 1.40.1. There is XSS in youhavenewmessagesmanyusers and youhavenewmessages i18n messages. This is related to MediaWiki:Youhavenewmessagesfromusers.	5.4	More Details
CVE-2023-5904	Cross-site Scripting (XSS) - Stored in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	5.4	More Details
CVE-2023-28499	Auth. (author+) Stored Cross-Site Scripting (XSS) vulnerability in simonpedge Slide Anything – Responsive Content / HTML Slider and Carousel plugin <= 2.4.9 versions.	5.4	More Details
CVE-2023-5896	Cross-site Scripting (XSS) - Stored in GitHub repository pkp/pkp-lib prior to 3.4.0-4.	5.4	More Details
CVE-2023-5890	Cross-site Scripting (XSS) - Stored in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	5.4	More Details
CVE-2023-42554	Improper Authentication vulnerabiity in Samsung Pass prior to version 4.3.00.17 allows physical attackers to bypass authentication.	5.4	More Details
CVE-2023-5892	Cross-site Scripting (XSS) - Stored in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	5.4	More Details
CVE-2023-5982	The UpdraftPlus: WordPress Backup & Migration Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.23.10. This is due to a lack of nonce validation and insufficient validation of the instance_id on the 'updraftmethod-googledrive-auth' action used to update Google Drive remote storage location. This makes it possible for unauthenticated attackers to modify the Google Drive location that backups are sent to via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This can make it possible for attackers to receive backups for a site which may contain sensitive information.	5.4	More Details
CVE-2023-41343	Rogic No-Code Database Builder's file uploading function has insufficient filtering for special characters. A remote attacker with regular user privilege can inject JavaScript to perform XSS (Stored Cross-Site Scripting) attack.	5.4	More Details
CVE-2023-35896	IBM Content Navigator 3.0.13 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 259247.	5.4	More Details
CVE-2023-47177	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Yakir Sitbon, Ariel Klikstein Linker plugin <= 1.2.1 versions.	5.4	More Details
CVE-2023-5891	Cross-site Scripting (XSS) - Reflected in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	5.4	More Details
CVE-2023-46744	Squidex is an open source headless CMS and content management hub. In affected versions a stored Cross-Site Scripting (XSS) vulnerability enables privilege escalation of authenticated users. The SVG element filtering mechanism intended to stop XSS attacks through uploaded SVG images, is insufficient resulting to stored XSS attacks. Squidex allows the CMS contributors to be granted the permission of uploading an SVG asset. When the asset is uploaded, a filtering mechanism is performed to validate that the SVG does not contain malicious code. The validation logic consists of traversing the HTML nodes in the DOM. In order for the validation to succeed, 2 conditions must be met: 1. No HTML tags included in a "blacklist" called "InvalidSvgElements" are present. This list only contains the element "script". and 2. No attributes of HTML tags begin with "on" (i.e. onerror, onclick) (line 65). If either of the 2 conditions is not satisfied, validation fails and the file/asset is not uploaded. However it is possible to bypass the above filtering mechanism and execute arbitrary JavaScript code by introducing other HTML elements such as an <iframe> element with a "src" attribute containing a "javascript:" value. Authenticated adversaries with the "assets.create" permission, can leverage this vulnerability to upload a malicious SVG as an asset, targeting any registered user that will attempt to open/view the asset through the Squidex CMS.	5.4	More Details
CVE-2023-47097	A Stored Cross-Site Scripting (XSS) vulnerability in the Server Template under System Setting in Virtualmin 7.7 allows remote attackers to inject arbitrary web script or HTML via the Template name field while creating server templates.	5.4	More Details
CVE-2023-26456	Users were able to set an arbitrary "product name" for OX Guard. The chosen value was not sufficiently sanitized before processing it at the user interface, allowing for indirect cross-site scripting attacks. Accounts that were temporarily taken over could be configured to trigger persistent code execution, allowing an attacker to build a foothold. Sanitization is in place for product names now. No publicly available exploits are known.	5.4	More Details
CVE-2023-46783	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Bright Plugins Pre-Orders for WooCommerce plugin <= 1.2.13 versions.	5.4	More Details
CVE-2023-29044	Documents operations could be manipulated to contain invalid data types, possibly script code. Script code could be injected to an operation that would be executed for users that are actively collaborating on the same document. Operation data exchanged between collaborating parties does now get escaped to avoid code execution. No publicly available exploits are known.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29045	Documents operations, in this case "drawing", could be manipulated to contain invalid data types, possibly script code. Script code could be injected to an operation that would be executed for users that are actively collaborating on the same document. Operation data exchanged between collaborating parties does now gets checked for validity to avoid code execution. No publicly available exploits are known.	5.4	More Details
CVE-2023-40661	Several memory vulnerabilities were identified within the OpenSC packages, particularly in the card enrollment process using pkcs15-init when a user or administrator enrolls cards. To take advantage of these flaws, an attacker must have physical access to the computer system and employ a custom-crafted USB device or smart card to manipulate responses to APDUs. This manipulation can potentially allow compromise key generation, certificate loading, and other card management operations during enrollment.	5.4	More Details
CVE-2023-47096	A Reflected Cross-Site Scripting (XSS) vulnerability in the Cloudmin Services Client under System Setting in Virtualmin 7.7 allows remote attackers to inject arbitrary web script or HTML via the Cloudmin services master field.	5.4	More Details
CVE-2023-46782	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Chris Yee MomentoPress for Momento360 plugin <= 1.0.1 versions.	5.4	More Details
CVE-2023-47095	A Stored Cross-Site Scripting (XSS) vulnerability in the Custom fields of Edit Virtual Server under System Customization in Virtualmin 7.7 allows remote attackers to inject arbitrary web script or HTML via the Batch Label field while details of Virtual Server.	5.4	More Details
CVE-2023-0898	General Electric MiCOM S1 Agile is vulnerable to an attacker achieving code execution by placing malicious DLL files in the directory of the application.	5.3	More Details
CVE-2023-20255	A vulnerability in an API of the Web Bridge feature of Cisco Meeting Server could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending crafted HTTP packets to an affected device. A successful exploit could allow the attacker to cause a partial availability condition, which could cause ongoing video calls to be dropped due to the invalid packets reaching the Web Bridge.	5.3	More Details
CVE-2023-34261	Kyocera TASKalfa 4053ci printers through 2VG_S000.002.561 allow identification of valid user accounts via username enumeration because they lead to a "nicht einloggen" error rather than a falsch error.	5.3	More Details
CVE-2023-5625	A regression was introduced in the Red Hat build of python-eventlet due to a change in the patch application strategy, resulting in a patch for CVE-2021-21419 not being applied for all builds of all products.	5.3	More Details
CVE-2023-4625	Improper Restriction of Excessive Authentication Attempts vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F/iQ-R Series CPU modules Web server function allows a remote unauthenticated attacker to prevent legitimate users from logging into the Web server function for a certain period after the attacker has attempted to log in illegally by continuously attempting unauthorized login to the Web server function. The impact of this vulnerability will persist while the attacker continues to attempt unauthorized login.	5.3	More Details
CVE-2023-29047	Imageconverter API endpoints provided methods that were not sufficiently validating and sanitizing client input, allowing to inject arbitrary SQL statements. An attacker with access to the adjacent network and potentially API credentials, could read and modify database content which is accessible to the imageconverter SQL user account. None No publicly available exploits are known.	5.3	More Details
CVE-2023-46819	Missing Authentication in Apache Software Foundation Apache OFBiz when using the Solr plugin. This issue affects Apache OFBiz: before 18.12.09. Users are recommended to upgrade to version 18.12.09	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5678	Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the "-pubcheck" option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.	5.3	More Details
CVE-2023-5358	Improper access control in Report log filters feature in Devolutions Server 2023.2.10.0 and earlier allows attackers to retrieve logs from vaults or entries they are not allowed to access via the report request url query parameters.	5.3	More Details
CVE-2023-5969	Mattermost fails to properly sanitize the request to /api/v4/redirect_location allowing an attacker, sending a specially crafted request to /api/v4/redirect_location, to fill up the memory due to caching large items.	5.3	More Details
CVE-2023-5514	The response messages received from the eSOMS report generation using certain parameter queries with full file path can be abused for enumerating the local file system structure.	5.3	More Details
CVE-2023-47271	PKP-WAL (aka PKP Web Application Library or pkp-lib) before 3.3.0-16, as used in Open Journal Systems (OJS) and other products, does not verify that the file named in an XML document (used for the native import/export plugin) is an image file, before trying to use it for an issue cover image.	5.3	More Details
CVE-2023-5516	Poorly constructed webap requests and URI components with special characters trigger unhandled errors and exceptions, disclosing information about the underlying technology and other sensitive information details. The website unintentionally reveals sensitive information including technical details like version Info, endpoints, backend server, Internal IP. etc., which can potentially expose additional attack surface containing other interesting vulnerabilities.	5.3	More Details
CVE-2023-47102	UrBackup Server 2.5.31 allows brute-force enumeration of user accounts because a failure message confirms that a username is not valid.	5.3	More Details
CVE-2023-5515	The responses for web queries with certain parameters disclose internal path of resources. This information can be used to learn internal structure of the application and to further plot attacks against web servers and deployed web applications.	5.3	More Details
CVE-2023-46963	An issue in Beijing Yunfan Internet Technology Co., Ltd, Yunfan Learning Examination System v.6.5 allows a remote attacker to obtain sensitive information via the password parameter in the login function.	5.3	More Details
CVE-2023-43194	Submitty before v22.06.00 is vulnerable to Incorrect Access Control. An attacker can delete any post in the forum by modifying request parameter.	5.3	More Details
CVE-2022-3172	A security issue was discovered in kube-apiserver that allows an aggregated API server to redirect client traffic to any URL. This could lead to the client performing unexpected actions as well as forwarding the client's API server credentials to third parties.	5.1	More Details
CVE-2023-20256	Multiple vulnerabilities in the per-user-override feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass a configured access control list (ACL) and allow traffic that should be denied to flow through an affected device. These vulnerabilities are due to a logic error that could occur when the affected software constructs and applies per-user-override rules. An attacker could exploit these vulnerabilities by connecting to a network through an affected device that has a vulnerable configuration. A successful exploit could allow the attacker to bypass the interface ACL and access resources that would should be protected.	5.0	More Details
CVE-2023-20247	A vulnerability in the remote access SSL VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to bypass a configured multiple certificate authentication policy and connect using only a valid username and password. This vulnerability is due to improper error handling during remote access VPN authentication. An attacker could exploit this vulnerability by sending crafted requests during remote access VPN session establishment. A successful exploit could allow the attacker to bypass the configured multiple certificate authentication policy while retaining the privileges and permissions associated with the original connection profile.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46851	Allura Discussion and Allura Forum importing does not restrict URL values specified in attachments. Project administrators can run these imports, which could cause Allura to read local files and expose them. Exposing internal files then can lead to other exploits, like session hijacking, or remote code execution. This issue affects Apache Allura from 1.0.1 through 1.15.0. Users are recommended to upgrade to version 1.16.0, which fixes the issue. If you are unable to upgrade, set "disable_entry_points.allura.importers = forge-tracker, forge-discussion" in your .ini config file.	4.9	More Details
CVE-2023-5968	Mattermost fails to properly sanitize the user object when updating the username, resulting in the password hash being included in the response body.	4.9	More Details
CVE-2023-34259	Kyocera TASKalfa 4053ci printers through 2VG_S000.002.561 allow /wlmdeu%2f%2e%2e%2f%2e%2e directory traversal to read arbitrary files on the filesystem, even files that require root privileges. NOTE: this issue exists because of an incomplete fix for CVE-2020-23575.	4.9	More Details
CVE-2023-47098	A Stored Cross-Site Scripting (XSS) vulnerability in the Manage Extra Admins under Administration Options in Virtualmin 7.7 allows remote attackers to inject arbitrary web script or HTML via the real name or description field.	4.8	More Details
CVE-2023-42029	IBM CICS TX Standard 11.1, Advanced 10.1, 11.1, and TXSeries for Multiplatforms 8.1, 8.2, 9.1 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 266059.	4.8	More Details
CVE-2023-5181	The WP Discord Invite WordPress plugin before 2.5.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-20041	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2023-20005	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2023-47184	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Proper Fraction LLC. Admin Bar & Dashboard Access Control plugin <= 1.2.8 versions.	4.8	More Details
CVE-2023-46824	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Om Ak Solutions Slick Popup: Contact Form 7 Popup Plugin plugin <= 1.7.14 versions.	4.8	More Details
CVE-2023-5605	The URL Shortify WordPress plugin before 1.7.9.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-5530	The Ninja Forms Contact Form WordPress plugin before 3.6.34 does not sanitize and escape its label fields, which could allow high privilege users such as admin to perform Stored XSS attacks. Only users with the unfiltered_html capability can perform this, and such users are already allowed to use JS in posts/comments etc however the vendor acknowledged and fixed the issue	4.8	More Details
CVE-2023-5228	The User Registration WordPress plugin before 3.0.4.2 does not sanitize and escape some of its settings, which could allow high-privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-20074	Multiple vulnerabilities in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by inserting crafted input into various data fields in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface, or access sensitive, browser-based information. In some cases, it is also possible to cause a temporary availability impact to portions of the FMC Dashboard.	4.8	More Details
CVE-2023-23702	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Pixelgrade Comments Ratings plugin <= 1.1.7 versions.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4858	The Simple Table Manager WordPress plugin through 1.5.6 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-46925	Reportico 7.1.21 is vulnerable to Cross Site Scripting (XSS).	4.8	More Details
CVE-2023-4810	The Responsive Pricing Table WordPress plugin before 5.1.8 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-2023-5919	A vulnerability was found in SourceCodester Company Website CMS 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /dashboard/createblog of the component Create Blog Page. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-244310 is the identifier assigned to this vulnerability.	4.7	More Details
CVE-2023-42539	PendingIntent hijacking vulnerability in ChallengeNotificationManager in Samsung Health prior to version 6.25 allows local attackers to access data.	4.7	More Details
CVE-2023-20196	Two vulnerabilities in Cisco ISE could allow an authenticated, remote attacker to upload arbitrary files to an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. These vulnerabilities are due to improper validation of files that are uploaded to the web-based management interface. An attacker could exploit these vulnerabilities by uploading a crafted file to an affected device. A successful exploit could allow the attacker to store malicious files in specific directories on the device. The attacker could later use those files to conduct additional attacks, including executing arbitrary code on the affected device with root privileges.	4.7	More Details
CVE-2023-20195	Two vulnerabilities in Cisco ISE could allow an authenticated, remote attacker to upload arbitrary files to an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. These vulnerabilities are due to improper validation of files that are uploaded to the web-based management interface. An attacker could exploit these vulnerabilities by uploading a crafted file to an affected device. A successful exploit could allow the attacker to store malicious files in specific directories on the device. The attacker could later use those files to conduct additional attacks, including executing arbitrary code on the affected device with root privileges.	4.7	More Details
CVE-2023-36620	An issue was discovered in the Boomerang Parental Control application before 13.83 for Android. The app is missing the android:allowBackup="false" attribute in the manifest. This allows the user to backup the internal memory of the app to a PC. This gives the user access to the API token that is used to authenticate requests to the API.	4.6	More Details
CVE-2023-36769	Microsoft OneNote Spoofing Vulnerability	4.6	More Details
CVE-2023-4535	An out-of-bounds read vulnerability was found in OpenSC packages within the MyEID driver when handling symmetric key encryption. Exploiting this flaw requires an attacker to have physical access to the computer and a specially crafted USB device or smart card. This flaw allows the attacker to manipulate APDU responses and potentially gain unauthorized access to sensitive data, compromising the system's security.	4.5	More Details
CVE-2023-0436	The affected versions of MongoDB Atlas Kubernetes Operator may print sensitive information like GCP service account keys and API integration secrets while DEBUG mode logging is enabled. This issue affects MongoDB Atlas Kubernetes Operator versions: 1.5.0, 1.6.0, 1.6.1, 1.7.0. Please note that this is reported on an EOL version of the product, and users are advised to upgrade to the latest supported version. Required Configuration: DEBUG logging is not enabled by default, and must be configured by the end-user. To check the log-level of the Operator, review the flags passed in your deployment configuration (eg. https://github.com/mongodb/mongodb-atlas-kubernetes/blob/main/config/manager/manager.yaml#L27 https://github.com/mongodb/mongodb-atlas-kubernetes/blob/main/config/manager/manager.yaml#L27)	4.5	More Details
CVE-2023-33228	The SolarWinds Network Configuration Manager was susceptible to the Exposure of Sensitive Information Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to obtain sensitive information.	4.5	More Details
CVE-2023-5819	The Amazonify plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 0.8.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. However, please note that this can also be combined with CVE-2023-5818 for CSRF to XSS.	4.4	More Details
CVE-2023-5606	The ChatBot for WordPress is vulnerable to Stored Cross-Site Scripting via the FAQ Builder in versions 4.8.6 through 4.9.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled. NOTE: This vulnerability is a re-introduction of CVE-2023-4253.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48461	In sensor driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-42552	Implicit intent hijacking vulnerability in Firewall application prior to versions 12.1.00.24 in Android 11, 13.1.00.16 in Android 12 and 14.1.00.7 in Android 13 allows 3rd party application to tamper the database of Firewall.	4.4	More Details
CVE-2023-42750	In gnss service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2022-48456	In camera driver, there is a possible out of bounds write due to a incorrect bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-5818	The Amazonify plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 0.8.1. This is due to missing or incorrect nonce validation on the amazonifyOptionsPage() function. This makes it possible for unauthenticated attackers to update the plugins settings, including the Amazon Tracking ID, via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-5975	The ImageMapper plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.6. This is due to missing or incorrect nonce validation on multiple functions. This makes it possible for unauthenticated attackers to update the plugin settings via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-36029	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4.3	More Details
CVE-2023-43087	Dell PowerScale OneFS 8.2.x, 9.0.0.x-9.5.0.x contains an improper handling of insufficient permissions. A low privileged remote attacker could potentially exploit this vulnerability to cause information disclosure.	4.3	More Details
CVE-2023-5902	Cross-Site Request Forgery (CSRF) in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	4.3	More Details
CVE-2023-3909	An issue has been discovered in GitLab CE/EE affecting all versions starting from 12.3 before 16.3.6, all versions starting from 16.4 before 16.4.2, all versions starting from 16.5 before 16.5.1. A Regular Expression Denial of Service was possible by adding a large string in timeout input in gitlab-ci.yml file.	4.3	More Details
CVE-2023-5916	A vulnerability classified as critical has been found in Lissy93 Dashy 2.1.1. This affects an unknown part of the file /config-manager/save of the component Configuration Handler. The manipulation of the argument config leads to improper access controls. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-244305 was assigned to this vulnerability.	4.3	More Details
CVE-2023-5967	Mattermost fails to properly validate requests to the Calls plugin, allowing an attacker sending a request without a User Agent header to cause a panic and crash the Calls plugin	4.3	More Details
CVE-2023-20213	A vulnerability in the CDP processing feature of Cisco ISE could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition of the CDP process on an affected device. This vulnerability is due to insufficient bounds checking when an affected device processes CDP traffic. An attacker could exploit this vulnerability by sending crafted CDP traffic to the device. A successful exploit could cause the CDP process to crash, impacting neighbor discovery and the ability of Cisco ISE to determine the reachability of remote devices. After a crash, the CDP process must be manually restarted using the cdp enable command in interface configuration mode.	4.3	More Details
CVE-2023-46254	capsule-proxy is a reverse proxy for Capsule kubernetes multi-tenancy framework. A bug in the RoleBinding reflector used by `capsule-proxy` gives ServiceAccount tenant owners the right to list Namespaces of other tenants backed by the same owner kind and name. For example consider two tenants `solar` and `wind`. Tenant `solar`, owned by a ServiceAccount named `tenant-owner` in the Namespace `solar`. Tenant `wind`, owned by a ServiceAccount named `tenant-owner` in the Namespace `wind`. The Tenant owner `solar` would be able to list the namespaces of the Tenant `wind` and vice-versa, although this is not correct. The bug introduces an exfiltration vulnerability since allows the listing of Namespace resources of other Tenants, although just in some specific conditions: 1. `capsule-proxy` runs with the `--disable-caching=false` (default value: `false`) and 2. Tenant owners are ServiceAccount, with the same resource name, but in different Namespaces. This vulnerability doesn't allow any privilege escalation on the outer tenant Namespace-scoped resources, since the Kubernetes RBAC is enforcing this. This issue has been addressed in version 0.4.5. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2023-47233	The brcm80211 component in the Linux kernel through 6.5.10 has a brcmf_cfg80211_detach use-after-free in the device unplugging (disconnect the USB by hotplug) code. For physically proximate attackers with local access, this "could be exploited in a real world scenario." This is related to brcmf_cfg80211_escan_timeout_worker in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39301	A server-side request forgery (SSRF) vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated users to read application data via a network. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2514 build 20230906 and later QTS 5.1.1.2491 build 20230815 and later QuTS hero h5.0.1.2515 build 20230907 and later QuTS hero h5.1.1.2488 build 20230812 and later QuTScloud c5.1.0.2498 and later	4.3	More Details
CVE-2023-5352	The Awesome Support WordPress plugin before 6.1.5 does not correctly authorize the wpas_edit_reply function, allowing users to edit posts for which they do not have permission.	4.3	More Details
CVE-2023-38509	XWiki Platform is a generic wiki platform. In org.xwiki.platform:xwiki-platform-livetable-ui starting with version 3.5-milestone-1 and prior to versions 14.10.9 and 15.3-rc-1, the mail obfuscation configuration was not fully taken into account and is was still possible by obfuscated emails. This has been patched in XWiki 14.10.9 and XWiki 15.3-rc-1. A workaround is to modify the page `XWiki.LiveTableResultsMacros` following the patch.	4.3	More Details
CVE-2023-5945	The video carousel slider with lightbox plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing or incorrect nonce validation on the responsive_video_gallery_with_lightbox_video_management_func() function. This makes it possible for unauthenticated attackers to delete videos hosted from the video slider via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2023-28794	Origin Validation Error vulnerability in Zscaler Client Connector on Linux allows Privilege Abuse. This issue affects Zscaler Client Connector for Linux: before 1.3.1.6.	4.3	More Details
CVE-2023-45362	An issue was discovered in DifferenceEngine.php in MediaWiki before 1.35.12, 1.36.x through 1.39.x before 1.39.5, and 1.40.x before 1.40.1. diff-multi-sameuser (aka "X intermediate revisions by the same user not shown") ignores username suppression. This is an information leak.	4.3	More Details
CVE-2023-3246	An issue has been discovered in GitLab EE/CE affecting all versions starting before 16.3.6, all versions starting from 16.4 before 16.4.2, all versions starting from 16.5 before 16.5.1 which allows an attackers to block Sidekiq job processor.	4.3	More Details
CVE-2023-5850	Incorrect security UI in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-5851	Inappropriate implementation in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-5853	Incorrect security UI in Downloads in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-29046	Connections to external data sources, like e-mail autoconfiguration, were not terminated in case they hit a timeout, instead those connections were logged. Some connections use user-controlled endpoints, which could be malicious and attempt to keep the connection open for an extended period of time. As a result users were able to trigger large amount of egress network connections, possibly exhausting network pool resources and lock up legitimate requests. A new mechanism has been introduced to cancel external connections that might access user-controlled endpoints. No publicly available exploits are known.	4.3	More Details
CVE-2023-5858	Inappropriate implementation in WebApp Provider in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2023-38548	A vulnerability in Veeam ONE allows an unprivileged user who has access to the Veeam ONE Web Client the ability to acquire the NTLM hash of the account used by the Veeam ONE Reporting Service.	4.3	More Details
CVE-2023-5976	Improper Access Control in GitHub repository microweber/microweber prior to 2.0.	4.3	More Details
CVE-2023-41723	A vulnerability in Veeam ONE allows a user with the Veeam ONE Read-Only User role to view the Dashboard Schedule. Note: The criticality of this vulnerability is reduced because the user with the Read-Only role is only able to view the schedule and cannot make changes.	4.3	More Details
CVE-2023-5859	Incorrect security UI in Picture In Picture in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to perform domain spoofing via a crafted local HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2023-42027	IBM CICS TX Standard 11.1, Advanced 10.1, 11.1, and TXSeries for Multiplatforms 8.1, 8.2, 9.1 are vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 266057.	4.3	More Details
CVE-2023-20267	A vulnerability in the IP geolocation rules of Snort 3 could allow an unauthenticated, remote attacker to potentially bypass IP address restrictions. This vulnerability exists because the configuration for IP geolocation rules is not parsed properly. An attacker could exploit this vulnerability by spoofing an IP address until they bypass the restriction. A successful exploit could allow the attacker to bypass location-based IP address restrictions.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42541	Improper authorization in PushClientProvider of Samsung Push Service prior to version 3.4.10 allows attacker to access unique id.	4.0	More Details
CVE-2023-42540	Improper access control vulnerability in Samsung Account prior to version 14.5.01.1 allows attackers to access sensitive information via implicit intent.	4.0	More Details
CVE-2023-20031	A vulnerability in the SSL/TLS certificate handling of Snort 3 Detection Engine integration with Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the Snort 3 detection engine to restart. This vulnerability is due to a logic error that occurs when an SSL/TLS certificate that is under load is accessed when it is initiating an SSL connection. Under specific, time-based constraints, an attacker could exploit this vulnerability by sending a high rate of SSL/TLS connection requests to be inspected by the Snort 3 detection engine on an affected device. A successful exploit could allow the attacker to cause the Snort 3 detection engine to reload, resulting in either a bypass or a denial of service (DoS) condition, depending on device configuration. The Snort detection engine will restart automatically. No manual intervention is required.	4.0	More Details
CVE-2023-20177	A vulnerability in the SSL file policy implementation of Cisco Firepower Threat Defense (FTD) Software that occurs when the SSL/TLS connection is configured with a URL Category and the Snort 3 detection engine could allow an unauthenticated, remote attacker to cause the Snort 3 detection engine to unexpectedly restart. This vulnerability exists because a logic error occurs when a Snort 3 detection engine inspects an SSL/TLS connection that has either a URL Category configured on the SSL file policy or a URL Category configured on an access control policy with TLS server identity discovery enabled. Under specific, time-based constraints, an attacker could exploit this vulnerability by sending a crafted SSL/TLS connection through an affected device. A successful exploit could allow the attacker to trigger an unexpected reload of the Snort 3 detection engine, resulting in either a bypass or denial of service (DoS) condition, depending on device configuration. The Snort 3 detection engine will restart automatically. No manual intervention is required.	4.0	More Details
CVE-2023-42553	Improper authorization verification vulnerability in Samsung Email prior to version 6.1.90.4 allows attackers to read sandbox data of email.	4.0	More Details
CVE-2023-20070	A vulnerability in the TLS 1.3 implementation of the Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the Snort 3 detection engine to unexpectedly restart. This vulnerability is due to a logic error in how memory allocations are handled during a TLS 1.3 session. Under specific, time-based constraints, an attacker could exploit this vulnerability by sending a crafted TLS 1.3 message sequence through an affected device. A successful exploit could allow the attacker to cause the Snort 3 detection engine to reload, resulting in a denial of service (DoS) condition. While the Snort detection engine reloads, packets going through the FTD device that are sent to the Snort detection engine will be dropped. The Snort detection engine will restart automatically. No manual intervention is required.	4.0	More Details
CVE-2023-41354	Chunghwa Telecom NOKIA G-040W-Q Firewall function does not block ICMP TIMESTAMP requests by default, an unauthenticated remote attacker can exploit this vulnerability by sending a crafted package, resulting in partially sensitive information exposed to an actor.	4.0	More Details
CVE-2023-5831	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.0 before 16.3.6, all versions starting from 16.4 before 16.4.2, and all versions starting from 16.5.0 before 16.5.1 which have the `super_sidebar_logged_out` feature flag enabled. Affected versions with this default-disabled feature flag enabled may unintentionally disclose GitLab version metadata to unauthorized actors.	3.7	More Details
CVE-2023-5875	Mattermost Desktop fails to correctly handle permissions or prompt the user for consent on certain sensitive ones allowing media exploitation from a malicious mattermost server	3.7	More Details
CVE-2021-4430	A vulnerability classified as problematic has been found in Ortus Solutions ColdBox Elixir 3.1.6. This affects an unknown part of the file src/defaultConfig.js of the component ENV Variable Handler. The manipulation leads to information disclosure. Upgrading to version 3.1.7 is able to address this issue. The identifier of the patch is a3aa62daea2e44c76d08d1eac63768cd928cd69e. It is recommended to upgrade the affected component. The identifier VDB-244485 was assigned to this vulnerability.	3.5	More Details
CVE-2023-5930	A vulnerability was found in Campcodes Simple Student Information System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/students/manage_academic.php. The manipulation of the argument student_id leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-244330 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2017-20187	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in Magnesium-PHP up to 0.3.0. It has been classified as problematic. Affected is the function formatEmailString of the file src/Magnesium/Message/Base.php. The manipulation of the argument email/name leads to injection. Upgrading to version 0.3.1 is able to address this issue. The patch is identified as 500d340e1f6421007413cc08a8383475221c2604. It is recommended to upgrade the affected component. VDB-244482 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2023-5900	Cross-Site Request Forgery in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4700	An authorization issue affecting GitLab EE affecting all versions from 14.7 prior to 16.3.6, 16.4 prior to 16.4.2, and 16.5 prior to 16.5.1, allowed a user to run jobs in protected environments, bypassing any required approvals.	3.5	More Details
CVE-2019-25156	A vulnerability classified as problematic was found in dstar2018 Agency up to 61. Affected by this vulnerability is an unknown functionality of the file search.php. The manipulation of the argument QSType/QuickSearch leads to cross site scripting. The attack can be launched remotely. The patch is named 975b56953efabb434519d9feefcc53685fb8d0ab. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-244495.	3.5	More Details
CVE-2021-4431	A vulnerability classified as problematic has been found in msyk FMDataAPI up to 22. Affected is an unknown function of the file FMDataAPI_Sample.php. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 23 is able to address this issue. The patch is identified as 3bd1709a8f7b1720529bf5dfc9855ad609f436cf. It is recommended to upgrade the affected component. VDB-244494 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-5901	Cross-site Scripting in GitHub repository pkp/pkp-lib prior to 3.3.0-16.	3.5	More Details
CVE-2023-5748	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in cgi component in Synology SSL VPN Client before 1.4.7-0687 allows local users to conduct denial-of-service attacks via unspecified vectors.	3.3	More Details
CVE-2023-42542	Improper access control vulnerability in Samsung Push Service prior to 3.4.10 allows local attackers to get register ID to identify the device.	3.3	More Details
CVE-2023-5963	An issue has been discovered in GitLab EE with Advanced Search affecting all versions from 13.9 to 16.3.6, 16.4 prior to 16.4.2 and 16.5 prior to 16.5.1 that could allow a denial of service in the Advanced Search function by chaining too many syntax operators.	3.1	More Details
CVE-2023-46737	Cosign is a sigstore signing tool for OCI containers. Cosign is susceptible to a denial of service by an attacker controlled registry. An attacker who controls a remote registry can return a high number of attestations and/or signatures to Cosign and cause Cosign to enter a long loop resulting in an endless data attack. The root cause is that Cosign loops through all attestations fetched from the remote registry in pkg/cosign.FetchAttestations. The attacker needs to compromise the registry or make a request to a registry they control. When doing so, the attacker must return a high number of attestations in the response to Cosign. The result will be that the attacker can cause Cosign to go into a long or infinite loop that will prevent other users from verifying their data. In Kyvernos case, an attacker whose privileges are limited to making requests to the cluster can make a request with an image reference to their own registry, trigger the infinite loop and deny other users from completing their admission requests. Alternatively, the attacker can obtain control of the registry used by an organization and return a high number of attestations instead the expected number of attestations. The issue can be mitigated rather simply by setting a limit to the limit of attestations that Cosign will loop through. The limit does not need to be high to be within the vast majority of use cases and still prevent the endless data attack. This issue has been patched in version 2.2.1 and users are advised to upgrade.	3.1	More Details
CVE-2023-4217	A vulnerability has been identified in PT-G503 Series versions prior to v5.2, where the session cookies attribute is not set properly in the affected application. The vulnerability may lead to security risks, potentially exposing user session data to unauthorized access and manipulation.	3.1	More Details
CVE-2023-5035	A vulnerability has been identified in PT-G503 Series firmware versions prior to v5.2, where the Secure attribute for sensitive cookies in HTTPS sessions is not set, which could cause the cookie to be transmitted in plaintext over an HTTP session. The vulnerability may lead to security risks, potentially exposing user session data to unauthorized access and manipulation.	3.1	More Details
CVE-2023-5876	Mattermost fails to properly validate a RegExp built off the server URL path, allowing an attacker in control of an enrolled server to mount a Denial Of Service.	3.1	More Details
CVE-2023-5920	Mattermost Desktop for MacOS fails to utilize the secure keyboard input functionality provided by macOS, allowing for other processes to read the keyboard input.	2.9	More Details
CVE-2023-2622	Authenticated clients can read arbitrary files on the MAIN Computer system using the remote procedure call (RPC) of the InspectSetup service endpoint. The low privilege client is then allowed to read arbitrary files that they do not have authorization to read.	2.7	More Details
CVE-2023-5910	A vulnerability was found in PopojiCMS 2.0.1 and classified as problematic. This issue affects some unknown processing of the file install.php of the component Web Config. The manipulation of the argument Site Title with the input <script>alert(1)</script> leads to cross site scripting. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-244229 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5917	A vulnerability, which was classified as problematic, has been found in phpBB up to 3.3.10. This issue affects the function main of the file phpBB/includes/acp/acp_icons.php of the component Smiley Pack Handler. The manipulation of the argument pak leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 3.3.11 is able to address this issue. The patch is named ccf6e6c255d38692d72fcb613b113e6eaa240aac. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-244307.	2.4	More Details
CVE-2023-45016	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-46678	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45324	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-46799	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-46798	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-46797	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-46796	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-46795	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-46794	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-46792	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45326	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45327	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45328	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-46790	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-46786	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-46680	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-46676	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45014	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45329	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45333	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45332	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45335	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45331	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-37835	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-45396. Reason: This record is a duplicate of CVE-2023-45396. Notes: All CVE users should reference CVE-2023-45396 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-46517	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-2023-45330	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45339	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45112	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45017	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45113	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45114	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45013	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2023-45337	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details