SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 30 October 2024

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-2024-51568	CyberPanel (aka Cyber Panel) before 2.3.5 allows Command Injection via completePath in the ProcessUtilities.outputExecutioner() sink. There is /filemanager/upload (aka File Manager upload) unauthenticated remote code execution via shell metacharacters.	10.0	More Details
CVE-2024-50420	Unrestricted Upload of File with Dangerous Type vulnerability in adirectory aDirectory allows Upload a Web Shell to a Web Server.This issue affects aDirectory: from n/a through 1.3.	10.0	More Details
CVE-2024-50473	Unrestricted Upload of File with Dangerous Type vulnerability in Ajar Productions Ajar in5 Embed allows Upload a Web Shell to a Web Server.This issue affects Ajar in5 Embed: from n/a through 3.1.3.	10.0	More Details
CVE-2024-50494	Unrestricted Upload of File with Dangerous Type vulnerability in Amin Omer Sudan Payment Gateway for WooCommerce allows Upload a Web Shell to a Web Server.This issue affects Sudan Payment Gateway for WooCommerce: from n/a through 1.2.2.	10.0	More Details
CVE-2024-50493	Unrestricted Upload of File with Dangerous Type vulnerability in masterhomepage Automatic Translation allows Upload a Web Shell to a Web Server.This issue affects Automatic Translation: from n/a through 1.0.4.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49668	Unrestricted Upload of File with Dangerous Type vulnerability in Admin Verbalize WP Upload a Web Shell to a Web Server.This issue affects Verbalize WP: from n/a through 1.0.	10.0	More Details
CVE-2024-50484	Unrestricted Upload of File with Dangerous Type vulnerability in mahlamusa Multi Purpose Mail Form allows Upload a Web Shell to a Web Server.This issue affects Multi Purpose Mail Form: from n/a through 1.0.2.	10.0	More Details
CVE-2024-50482	Unrestricted Upload of File with Dangerous Type vulnerability in Chetan Khandla Woocommerce Product Design allows Upload a Web Shell to a Web Server.This issue affects Woocommerce Product Design: from n/a through 1.0.0.	10.0	More Details
CVE-2024-47901	A vulnerability has been identified in InterMesh 7177 Hybrid 2.0 Subscriber (All versions < V8.2.12), InterMesh 7707 Fire Subscriber (All versions < V7.2.12 only if the IP interface is enabled (which is not the default configuration)). The web server of affected devices does not sanitize the input parameters in specific GET requests that allow for code execution on operating system level. In combination with other vulnerabilities (CVE-2024-47902, CVE-2024-47903, CVE-2024-47904) this could allow an unauthenticated remote attacker to execute arbitrary code with root privileges.	10.0	More Details
CVE-2024-51567	upgrademysqlstatus in databases/views.py in CyberPanel (aka Cyber Panel) before 5b08cd6 allows remote attackers to bypass authentication and execute arbitrary commands via /dataBases/upgrademysqlstatus by bypassing secMiddleware (which is only for a POST request) and using shell metacharacters in the statusfile property, as exploited in the wild in October 2024 by PSAUX. Versions through 2.3.6 and (unpatched) 2.3.7 are affected.	10.0	More Details
CVE-2024-51378	getresetstatus in dns/views.py and ftp/views.py in CyberPanel (aka Cyber Panel) before 1c0c6cb allows remote attackers to bypass authentication and execute arbitrary commands via /dns/getresetstatus or /ftp/getresetstatus by bypassing secMiddleware (which is only for a POST request) and using shell metacharacters in the statusfile property, as exploited in the wild in October 2024 by PSAUX. Versions through 2.3.6 and (unpatched) 2.3.7 are affected.	10.0	More Details
CVE-2024-50498	Improper Control of Generation of Code ('Code Injection') vulnerability in LUBUS WP Query Console allows Code Injection.This issue affects WP Query Console: from n/a through 1.0.	10.0	More Details
CVE-2024-50496	Unrestricted Upload of File with Dangerous Type vulnerability in Web and Print Design AR For WordPress allows Upload a Web Shell to a Web Server.This issue affects AR For WordPress: from n/a through 6.2.	10.0	More Details
CVE-2024-50495	Unrestricted Upload of File with Dangerous Type vulnerability in WidgiLabs Plugin Propagator allows Upload a Web Shell to a Web Server.This issue affects Plugin Propagator: from n/a through 0.1.	10.0	More Details
CVE-2024-50480	Unrestricted Upload of File with Dangerous Type vulnerability in azexo Marketing Automation by AZEXO allows Upload a Web Shell to a Web Server.This issue affects Marketing Automation by AZEXO: from n/a through 1.27.80.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50427	Unrestricted Upload of File with Dangerous Type vulnerability in Devsoft Baltic OÜ SurveyJS: Drag & Drop WordPress Form Builder.This issue affects SurveyJS: Drag & Drop WordPress Form Builder: from n/a through 1.9.136.	9.9	More Details
CVE-2024-20424	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software, formerly Firepower Management Center Software, could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system as root. This vulnerability is due to insufficient input validation of certain HTTP requests. An attacker could exploit this vulnerability by authenticating to the web-based management interface of an affected device and then sending a crafted HTTP request to the device. A successful exploit could allow the attacker to execute arbitrary commands with root permissions on the underlying operating system of the Cisco FMC device or to execute commands on managed Cisco Firepower Threat Defense (FTD) devices. To exploit this vulnerability, the attacker would need valid credentials for a user account with at least the role of Security Analyst (Read Only).	9.9	More Details
CVE-2024-20329	A vulnerability in the SSH subsystem of Cisco Adaptive Security Appliance (ASA) Software could allow an authenticated, remote attacker to execute operating system commands as root. This vulnerability is due to insufficient validation of user input. An attacker could exploit this vulnerability by submitting crafted input when executing remote CLI commands over SSH. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges. An attacker with limited user privileges could use this vulnerability to gain complete control over the system.	9.9	More Details
CVE-2024-49671	Unrestricted Upload of File with Dangerous Type vulnerability in Dogu Pekgoz AI Image Generator for Your Content & Featured Images – AI Postpix allows Upload a Web Shell to a Web Server.This issue affects AI Image Generator for Your Content & Featured Images – AI Postpix: from n/a through 1.1.8.	9.9	More Details
CVE-2024-49669	Unrestricted Upload of File with Dangerous Type vulnerability in Alexander De Ridder INK Official allows Upload a Web Shell to a Web Server.This issue affects INK Official: from n/a through 4.1.2.	9.9	More Details
CVE-2024-49658	Unrestricted Upload of File with Dangerous Type vulnerability in Ecomerciar Woocommerce Custom Profile Picture allows Upload a Web Shell to a Web Server.This issue affects Woocommerce Custom Profile Picture: from n/a through 1.0.	9.9	More Details
CVE-2024-49653	Unrestricted Upload of File with Dangerous Type vulnerability in James Eggers Portfolleo portfolleo allows Upload a Web Shell to a Web Server.This issue affects Portfolleo: from n/a through 1.2.	9.9	More Details
CVE-2024-49652	Unrestricted Upload of File with Dangerous Type vulnerability in ReneeCussack 3D Work In Progress allows Upload a Web Shell to a Web Server.This issue affects 3D Work In Progress: from n/a through 1.0.3.	9.9	More Details
CVE-2024-48357	LyLme Spage 1.2.0 through 1.6.0 is vulnerable to SQL Injection via /admin/apply.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48465	The MRBS version 1.5.0 has an SQL injection vulnerability in the edit_entry_handler.php file, specifically in the rooms%5B%5D parameter	9.8	More Details
CVE-2024-48356	LyLme Spage <=1.6.0 is vulnerable to SQL Injection via /admin/group.php.	9.8	More Details
CVE-2024-50483	Authorization Bypass Through User-Controlled Key vulnerability in Meetup allows Privilege Escalation.This issue affects Meetup: from n/a through 0.1.	9.8	More Details
CVE-2024-50478	Authentication Bypass by Primary Weakness vulnerability in Swoop 1-Click Login: Passwordless Authentication allows Authentication Bypass.This issue affects 1-Click Login: Passwordless Authentication: 1.4.5.	9.8	More Details
CVE-2024-45656	IBM Flexible Service Processor (FSP) FW860.00 through FW860.B3, FW950.00 through FW950.C0, FW1030.00 through FW1030.61, FW1050.00 through FW1050.21, and FW1060.00 through FW1060.10 has static credentials which may allow network users to gain service privileges to the FSP.	9.8	More Details
CVE-2024-39205	An issue in pyload-ng v0.5.0b3.dev85 running under python3.11 or below allows attackers to execute arbitrary code via a crafted HTTP request.	9.8	More Details
CVE-2024-5982	A path traversal vulnerability exists in the latest version of gaizhenbiao/chuanhuchatgpt. The vulnerability arises from unsanitized input handling in multiple features, including user upload, directory creation, and template loading. Specifically, the load_chat_history function in modules/models/base_model.py allows arbitrary file uploads, potentially leading to remote code execution (RCE). The get_history_names function in utils.py permits arbitrary directory creation. Additionally, the load_template function in utils.py can be exploited to leak the first column of CSV files. These issues stem from improper sanitization of user inputs concatenated with directory paths using os.path.join.	9.8	More Details
CVE-2024-50475	Missing Authorization vulnerability in Scott Gamon Signup Page allows Privilege Escalation.This issue affects Signup Page: from n/a through 1.0.	9.8	More Details
CVE-2024-50476	Missing Authorization vulnerability in GRÜN Software Group GmbH GRÜN spendino Spendenformular allows Privilege Escalation.This issue affects GRÜN spendino Spendenformular: from n/a through 1.0.1.	9.8	More Details
CVE-2024-50485	: Incorrect Privilege Assignment vulnerability in Udit Rawat Exam Matrix allows Privilege Escalation.This issue affects Exam Matrix: from n/a through 1.5.	9.8	More Details
CVE-2024-50490	Missing Authorization vulnerability in Szabolcs Szecsenyi PegaPoll allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects PegaPoll: from n/a through 1.0.2.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6868	mudler/LocalAI version 2.17.1 allows for arbitrary file write due to improper handling of automatic archive extraction. When model configurations specify additional files as archives (e.g., .tar), these archives are automatically extracted after downloading. This behavior can be exploited to perform a 'tarslip' attack, allowing files to be written to arbitrary locations on the server, bypassing checks that normally restrict files to the models directory. This vulnerability can lead to remote code execution (RCE) by overwriting backend assets used by the server.	9.8	More Details
CVE-2024-7042	A vulnerability in the GraphCypherQAChain class of langchain-ai/langchainjs versions 0.2.5 and all versions with this class allows for prompt injection, leading to SQL injection. This vulnerability permits unauthorized data manipulation, data exfiltration, denial of service (DoS) by deleting all data, breaches in multi-tenant security environments, and data integrity issues. Attackers can create, update, or delete nodes and relationships without proper authorization, extract sensitive data, disrupt services, access data across different tenants, and compromise the integrity of the database.	9.8	More Details
CVE-2024-8309	A vulnerability in the GraphCypherQAChain class of langchain-ai/langchain version 0.2.5 allows for SQL injection through prompt injection. This vulnerability can lead to unauthorized data manipulation, data exfiltration, denial of service (DoS) by deleting all data, breaches in multi-tenant security environments, and data integrity issues. Attackers can create, update, or delete nodes and relationships without proper authorization, extract sensitive data, disrupt services, access data across different tenants, and compromise the integrity of the database.	9.8	More Details
CVE-2024-8923	ServiceNow has addressed an input validation vulnerability that was identified in the Now Platform. This vulnerability could enable an unauthenticated user to remotely execute code within the context of the Now Platform. ServiceNow deployed an update to hosted instances and ServiceNow provided the update to our partners and self-hosted customers. Further, the vulnerability is addressed in the listed patches and hot fixes.	9.8	More Details
CVE-2024-9988	The Crypto plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.15. This is due to missing validation on the user being supplied in the 'crypto_connect_ajax_process::register' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the username.	9.8	More Details
CVE-2024-9989	The Crypto plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.15. This is due a to limited arbitrary method call to 'crypto_connect_ajax_process::log_in' function in the 'crypto_connect_ajax_process' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the username.	9.8	More Details
CVE-2024-48063	In PyTorch <=2.4.1, the RemoteModule has Deserialization RCE. NOTE: this is disputed by multiple parties because this is intended behavior in PyTorch distributed computing.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48206	A Deserialization of Untrusted Data vulnerability in chainer v7.8.1.post1 leads to execution of arbitrary code.	9.8	More Details
CVE-2024-44081	In Jitsi Meet before 2.0.9779, the functionality to share a video file was implemented in an insecure way, resulting in clients loading videos from an arbitrary URL if a message from another participant contains a URL encoded in the expected format.	9.8	More Details
CVE-2024-48138	A remote code execution (RCE) vulnerability in the component /PluXml/core/admin/parametres_edittpl.php of PluXml v5.8.16 and lower allows attackers to execute arbitrary code via injecting a crafted payload into a template.	9.8	More Details
CVE-2024-48573	A NoSQL injection vulnerability in AquilaCMS 1.409.20 and prior allows unauthenticated attackers to reset user and administrator account passwords via the "Reset password" feature.	9.8	More Details
CVE-2024-50489	Authentication Bypass Using an Alternate Path or Channel vulnerability in Realty Workstation allows Authentication Bypass.This issue affects Realty Workstation: from n/a through 1.0.45.	9.8	More Details
CVE-2024-47575	A missing authentication for critical function in FortiManager 7.6.0, FortiManager 7.4.0 through 7.4.4, FortiManager 7.2.0 through 7.2.7, FortiManager 7.0.0 through 7.0.12, FortiManager 6.4.0 through 6.4.14, FortiManager 6.2.0 through 6.2.12, Fortinet FortiManager Cloud 7.4.1 through 7.4.4, FortiManager Cloud 7.2.1 through 7.2.7, FortiManager Cloud 7.0.1 through 7.0.12, FortiManager Cloud 6.4.1 through 6.4.7 allows attacker to execute arbitrary code or commands via specially crafted requests.	9.8	More Details
CVE-2024-50486	Authentication Bypass Using an Alternate Path or Channel vulnerability in Acnoo Acnoo Flutter API allows Authentication Bypass.This issue affects Acnoo Flutter API: from n/a through 1.0.5.	9.8	More Details
CVE-2024-48581	File Upload vulnerability in Best courier management system in php v.1.0 allows a remote attacker to execute arbitrary code via the admin_class.php component.	9.8	More Details
CVE-2024-48538	Incorrect access control in the firmware update and download processes of Neye3C v4.5.2.0 allows attackers to access sensitive information by analyzing the code and data within the APK file.	9.8	More Details
CVE-2024-48539	Neye3C v4.5.2.0 was discovered to contain a hardcoded encryption key in the firmware update mechanism.	9.8	More Details
CVE-2024-46478	HTMLDOC v1.9.18 contains a buffer overflow in parse_pre function,ps-pdf.cxx:5681.	9.8	More Details
CVE-2024-48514	php-heic-to-jpg <= 1.0.5 is vulnerable to code injection (fixed in 1.0.6). An attacker who can upload heic images is able to execute code on the remote server via the file name. As a result, the CIA is no longer guaranteed. This affects php-heic-to-jpg 1.0.5 and below.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7763	In WhatsUp Gold versions released before 2024.0.0, an Authentication Bypass issue exists which allows an attacker to obtain encrypted user credentials.	9.8	More Details
CVE-2024-41617	Money Manager EX WebApp (web-money-manager-ex) 1.2.2 is vulnerable to Incorrect Access Control. The `redirect_if_not_loggedin` function in `functions_security.php` fails to terminate script execution after redirecting unauthenticated users. This flaw allows an unauthenticated attacker to upload arbitrary files, potentially leading to Remote Code Execution.	9.8	More Details
CVE-2024-41618	Money Manager EX WebApp (web-money-manager-ex) 1.2.2 is vulnerable to SQL Injection in the `transaction_delete_group` function. The vulnerability is due to improper sanitization of user input in the `TrDeleteArr` parameter, which is directly incorporated into an SQL query.	9.8	More Details
CVE-2024-9488	The Comments – wpDiscuz plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 7.6.24. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email and the user does not have an already-existing account for the service returning the token.	9.8	More Details
CVE-2024-50477	Authentication Bypass Using an Alternate Path or Channel vulnerability in Stacks Stacks Mobile App Builder stacks-mobile-app-builder allows Authentication Bypass.This issue affects Stacks Mobile App Builder: from n/a through 5.2.3.	9.8	More Details
CVE-2024-48428	An issue in Olive VLE allows an attacker to obtain sensitive information via the reset password function.	9.8	More Details
CVE-2022-30355	OvalEdge 5.2.8.0 and earlier is affected by an Account Takeover vulnerability via a POST request to /profile/updateProfile via the userId and email parameters. Authentication is required.	9.8	More Details
CVE-2024-48204	SQL injection vulnerability in Hanzhou Haobo network management system 1.0 allows a remote attacker to execute arbitrary code via a crafted script.	9.8	More Details
CVE-2024-48579	SQL Injection vulnerability in Best House rental management system project in php v.1.0 allows a remote attacker to execute arbitrary code via the username parameter of the login request.	9.8	More Details
CVE-2024-48580	SQL Injection vulnerability in Best courier management system in php v.1.0 allows a remote attacker to execute arbitrary code via the email parameter of the login request.	9.8	More Details
CVE-2024-10381	This vulnerability exists in Matrix Door Controller Cosec Vega FAXQ due to improper implementation of session management at the web-based management interface. A remote attacker could exploit this vulnerability by sending a specially crafted http request on the vulnerable device. Successful exploitation of this vulnerability could allow remote attacker to gain unauthorized access and take complete control of the targeted device.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10386	CVE-2024-10386 IMPACT An authentication vulnerability exists in the affected product. The vulnerability could allow a threat actor with network access to send crafted messages to the device, potentially resulting in database manipulation.	9.8	More Details
CVE-2024-9933	The WatchTowerHQ plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.9.6. This is due to the 'watchtower_ota_token' default value is empty, and the not empty check is missing in the 'Password_Less_Access::login' function. This makes it possible for unauthenticated attackers to log in to the WatchTowerHQ client administrator user.	9.8	More Details
CVE-2024-10440	The eHDR CTMS from Sunnet has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL command to read, modify, and delete database contents.	9.8	More Details
CVE-2024-48237	WTCMS 1.0 is vulnerable to Incorrect Access Control in \Common\Controller\HomebaseController.class.php.	9.8	More Details
CVE-2024-50623	In Cleo Harmony before 5.8.0.21, VLTrader before 5.8.0.21, and LexiCom before 5.8.0.21, there is an unrestricted file upload and download that could lead to remote code execution.	9.8	More Details
CVE-2024-9501	The Wp Social Login and Register Social Counter plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 3.0.7. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email and the user does not have an already-existing account for the service returning the token.	9.8	More Details
CVE-2024-50487	Authentication Bypass Using an Alternate Path or Channel vulnerability in MaanTheme MaanStore API allows Authentication Bypass.This issue affects MaanStore API: from n/a through 1.0.1.	9.8	More Details
CVE-2024-9932	The Wux Blog Editor plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the 'wuxbt_insertImageNew' function in versions up to, and including, 3.0.0. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2024-9931	The Wux Blog Editor plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 3.0.0. This is due to missing validation on the token being supplied during the autologin through the plugin. This makes it possible for unauthenticated attackers to log in to the first administrator user.	9.8	More Details
CVE-2024-9930	The Extensions by HocWP Team plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 0.2.3.2. This is due to missing validation on the user being supplied in the 'verify_email' action. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator. The vulnerability is in the Account extension.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40867	A custom URL scheme handling issue was addressed with improved input validation. This issue is fixed in iOS 18.1 and iPadOS 18.1. A remote attacker may be able to break out of Web Content sandbox.	9.6	More Details
CVE-2024-50491	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Micah Blu RSVP ME allows SQL Injection.This issue affects RSVP ME: from n/a through 1.9.9.	9.3	More Details
CVE-2024-20412	A vulnerability in Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 1000, 2100, 3100, and 4200 Series could allow an unauthenticated, local attacker to access an affected system using static credentials. This vulnerability is due to the presence of static accounts with hard-coded passwords on an affected system. An attacker could exploit this vulnerability by logging in to the CLI of an affected device with these credentials. A successful exploit could allow the attacker to access the affected system and retrieve sensitive information, perform limited troubleshooting actions, modify some configuration options, or render the device unable to boot to the operating system, requiring a reimage of the device.	9.3	More Details
CVE-2024-49681	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SWIT WP Sessions Time Monitoring Full Automatic allows SQL Injection.This issue affects WP Sessions Time Monitoring Full Automatic: from n/a through 1.0.9.	9.3	More Details
CVE-2024-44206	An issue in the handling of URL protocols was addressed with improved logic. This issue is fixed in tvOS 17.6, visionOS 1.3, Safari 17.6, watchOS 10.6, iOS 17.6 and iPadOS 17.6, macOS Sonoma 14.6. A user may be able to bypass some web content restrictions.	9.3	More Details
CVE-2024-50479	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mansur Ahamed Woocommerce Quote Calculator allows Blind SQL Injection.This issue affects Woocommerce Quote Calculator: from n/a through 1.1.	9.3	More Details
CVE-2024-48548	The APK file in Cloud Smart Lock v2.0.1 has a leaked a URL that can call an API for binding physical devices. This vulnerability allows attackers to arbitrarily construct a request to use the app to bind to unknown devices by finding a valid serial number via a bruteforce attack.	9.3	More Details
CVE-2024-47406	Sharp and Toshiba Tec MFPs improperly process HTTP authentication requests, resulting in an authentication bypass vulnerability.	9.1	More Details
CVE-2024-38821	Spring WebFlux applications that have Spring Security authorization rules on static resources can be bypassed under certain circumstances. For this to impact an application, all of the following must be true: * It must be a WebFlux application * It must be using Spring's static resources support * It must have a non-permitAll authorization rule applied to the static resources support	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47821	pyLoad is a free and open-source Download Manager. The folder `/.pyload/scripts` has scripts which are run when certain actions are completed, for e.g. a download is finished. By downloading a executable file to a folder in /scripts and performing the respective action, remote code execution can be achieved in versions prior to 0.5.0b3.dev87. A file can be downloaded to such a folder by changing the download folder to a folder in `/scripts` path and using the `/flashgot` API to download the file. This vulnerability allows an attacker with access to change the settings on a pyload server to execute arbitrary code and completely compromise the system. Version 0.5.0b3.dev87 fixes this issue.	9.1	More Details
CVE-2024-49768	Waitress is a Web Server Gateway Interface server for Python 2 and 3. A remote client may send a request that is exactly recv_bytes (defaults to 8192) long, followed by a secondary request using HTTP pipelining. When request lookahead is disabled (default) we won't read any more requests, and when the first request fails due to a parsing error, we simply close the connection. However when request lookahead is enabled, it is possible to process and receive the first request, start sending the error message back to the client while we read the next request and queue it. This will allow the secondary request to be serviced by the worker thread while the connection should be closed. Waitress 3.0.1 fixes the race condition. As a workaround, disable channel_request_lookahead, this is set to 0 by default disabling this feature.	9.1	More Details
CVE-2024-48143	A lack of rate limiting in the OTP validation component of Digitory Multi Channel Integrated POS v1.0 allows attackers to gain access to the ordering system and place an excessive amount of food orders.	9.1	More Details
CVE-2024-48144	A prompt injection vulnerability in the chatbox of Fusion Chat Chat AI Assistant Ask Me Anything v1.2.4.0 allows attackers to access and exfiltrate all previous and subsequent chat data between the user and the AI assistant via a crafted message.	9.1	More Details
CVE-2024-48145	A prompt injection vulnerability in the chatbox of Netangular Technologies ChatNet AI Version v1.0 allows attackers to access and exfiltrate all previous and subsequent chat data between the user and the AI assistant via a crafted message.	9.1	More Details
CVE-2024-7774	A path traversal vulnerability exists in the `getFullPath` method of langchain-ai/langchainjs version 0.2.5. This vulnerability allows attackers to save files anywhere in the filesystem, overwrite existing text files, read `.txt` files, and delete files. The vulnerability is exploited through the `setFileContent`, `getParsedFile`, and `mdelete` methods, which do not properly sanitize user input.	9.1	More Details
CVE-2024-44217	A permissions issue was addressed by removing vulnerable code and adding additional checks. This issue is fixed in iOS 18 and iPadOS 18. Password autofill may fill in passwords after failing authentication.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47883	The OpenRefine fork of the MIT Simile Butterfly server is a modular web application framework. The Butterfly framework uses the `java.net.URL` class to refer to (what are expected to be) local resource files, like images or templates. This works: "opening a connection" to these URLs opens the local file. However, prior to version 1.2.6, if a `file:/` URL is directly given where a relative path (resource name) is expected, this is also accepted in some code paths; the app then fetches the file, from a remote machine if indicated, and uses it as if it was a trusted part of the app's codebase. This leads to multiple weaknesses and potential weaknesses. An attacker that has network access to the application could use it to gain access to files, either on the the server's filesystem (path traversal) or shared by nearby machines (server-side request forgery with e.g. SMB). An attacker that can lead or redirect a user to a crafted URL belonging to the app could cause arbitrary attacker-controlled JavaScript to be loaded in the victim's browser (cross-site scripting). If an app is written in such a way that an attacker can influence the resource name used for a template, that attacker could cause the app to fetch and execute an attacker-controlled template (remote code execution). Version 1.2.6 contains a patch.	9.1	More Details
CVE-2024-5823	A file overwrite vulnerability exists in gaizhenbiao/chuanhuchatgpt versions <= 20240410. This vulnerability allows an attacker to gain unauthorized access to overwrite critical configuration files within the system. Exploiting this vulnerability can lead to unauthorized changes in system behavior or security settings. Additionally, tampering with these configuration files can result in a denial of service (DoS) condition, disrupting normal system operation.	9.1	More Details
CVE-2024-7475	An improper access control vulnerability in lunary-ai/lunary version 1.3.2 allows an attacker to update the SAML configuration without authorization. This vulnerability can lead to manipulation of authentication processes, fraudulent login requests, and theft of user information. Appropriate access controls should be implemented to ensure that the SAML configuration can only be updated by authorized users.	9.1	More Details
CVE-2024-6581	A vulnerability in the discussion image upload function of the Lollms application, version v9.9, allows for the uploading of SVG files. Due to incomplete filtering in the sanitize_svg function, this can lead to cross-site scripting (XSS) vulnerabilities, which in turn pose a risk of remote code execution. The sanitize_svg function only removes script elements and 'on*' event attributes, but does not account for other potential vectors for XSS within SVG files. This vulnerability can be exploited when authorized users access a malicious URL containing the crafted SVG file.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-48655	An issue in Total.js CMS v.1.0 allows a remote attacker to execute arbitrary code via the func.js file.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45263	An issue was discovered on certain GL-iNet devices, including MT6000, MT3000, MT2500, AXT1800, and AX1800 4.6.2. The upload interface allows the uploading of arbitrary files to the device. Once the device executes the files, it can lead to information leakage, enabling complete control.	8.8	More Details
CVE-2024-45262	An issue was discovered on certain GL-iNet devices, including MT6000, MT3000, MT2500, AXT1800, and AX1800 4.6.2. The params parameter in the call method of the /rpc endpoint is vulnerable to arbitrary directory traversal, which enables attackers to execute scripts under any path.	8.8	More Details
CVE-2024-10282	A vulnerability classified as critical was found in Tenda RX9 and RX9 Pro 22.03.02.10/22.03.02.20. Affected by this vulnerability is the function sub_42EA38 of the file /goform/SetVirtualServerCfg. The manipulation of the argument list leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-10283	A vulnerability, which was classified as critical, has been found in Tenda RX9 and RX9 Pro 22.03.02.20. Affected by this issue is the function sub_4337EC of the file /goform/SetNetControlList. The manipulation of the argument list leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-48427	A SQL injection vulnerability in Sourcecodester Packers and Movers Management System v1.0 allows remote authenticated users to execute arbitrary SQL commands via the id parameter in /mpms/admin/?page=services/manage_service&id	8.8	More Details
CVE-2024-48441	Wuhan Tianyu Information Industry Co., Ltd Tianyu CPE Router CommonCPExCPETS_v3.2.468.11.04_P4 was discovered to contain a command injection vulnerability via the component at_command.asp.	8.8	More Details
CVE-2024-48440	Shenzhen Tuoshi Network Communications Co.,Ltd 5G CPE Router NR500-EA RG500UEAABxCOMSLICv3.2.2543.12.18 was discovered to contain a command injection vulnerability via the component at_command.asp.	8.8	More Details
CVE-2024-9637	The School Management System – WPSchoolPress plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 2.2.10. This is due to the plugin not properly validating a user's identity prior to updating their details like email. This makes it possible for authenticated attackers, with teacher-level access and above, to change arbitrary user's email addresses, including administrators, and leverage that to reset the user's password and gain access to their account.	8.8	More Details
CVE-2024-49675	Authentication Bypass Using an Alternate Path or Channel vulnerability in Vitalii Bryl iBryl Switch User allows Authentication Bypass.This issue affects iBryl Switch User: from n/a through 1.0.1.	8.8	More Details
CVE-2024-50416	Deserialization of Untrusted Data vulnerability in WPClever WPC Shop as a Customer for WooCommerce allows Object Injection.This issue affects WPC Shop as a Customer for WooCommerce: from n/a through 1.2.6.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50408	Deserialization of Untrusted Data vulnerability in Kiboko Labs Namaste! LMS allows Object Injection.This issue affects Namaste! LMS: from n/a through 2.6.3.	8.8	More Details
CVE-2024-10008	The Masteriyo LMS – eLearning and Online Course Builder for WordPress plugin for WordPress is vulnerable to unauthorized user profile modification due to missing authorization checks on the /wp-json/masteriyo/v1/users/$id REST API endpoint in all versions up to, and including, 1.13.3. This makes it possible for authenticated attackers, with student-level access and above, to modify the roles of arbitrary users. As a result, attackers can escalate their privileges to the Administrator and demote existing administrators to students.	8.8	More Details
CVE-2024-40431	A lack of input validation in Realtek SD card reader driver before 10.0.26100.21374 through the implementation of the IOCTL_SCSI_PASS_THROUGH control of the SD card reader driver allows an attacker to write to predictable kernel memory locations, even as a low-privileged user.	8.8	More Details
CVE-2024-9990	The Crypto plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 2.15. This is due to missing nonce validation in the 'crypto_connect_ajax_process::check' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2024-10487	Out of bounds write in Dawn in Google Chrome prior to 130.0.6723.92 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2024-10488	Use after free in WebRTC in Google Chrome prior to 130.0.6723.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-44122	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sequoia 15, macOS Sonoma 14.7.1. An application may be able to break out of its sandbox.	8.8	More Details
CVE-2024-10434	A vulnerability was found in Tenda AC1206 up to 20241027. It has been classified as critical. This affects the function ate_Tenda_mfg_check_usb/ate_Tenda_mfg_check_usb3 of the file /goform/ate. The manipulation of the argument arg leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-10281	A vulnerability classified as critical has been found in Tenda RX9 and RX9 Pro 22.03.02.10/22.03.02.20. Affected is the function sub_42EEE0 of the file /goform/SetStaticRouteCfg. The manipulation of the argument list leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50616	Ironman PowerShell Universal 5.x before 5.0.12 allows an authenticated attacker to elevate their privileges and view job information.	8.8	More Details
CVE-2024-9598	The AMP for WP – Accelerated Mobile Pages plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.0.99.1. This is due to missing or incorrect nonce validation on the 'proxy' function. This makes it possible for unauthenticated attackers to send the logged in user's cookies to their own server via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2022-30358	OvalEdge 5.2.8.0 and earlier is affected by an Account Takeover vulnerability via a POST request to /user/updatePassword via the userId and newPsw parameters. Authentication is required.	8.8	More Details
CVE-2024-10436	The WPC Smart Messages for WooCommerce plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 4.2.1 via the get_condition_value function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.	8.8	More Details
CVE-2024-10467	Memory safety bugs present in Firefox 131, Firefox ESR 128.3, and Thunderbird 128.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	8.8	More Details
CVE-2024-50481	Incorrect Privilege Assignment vulnerability in Stack Themes Bstone Demo Importer allows Privilege Escalation.This issue affects Bstone Demo Importer: from n/a through 1.0.1.	8.8	More Details
CVE-2024-47014	Android before 2024-10-05 on Google Pixel devices allows privilege escalation in the ABL component, A-330537292.	8.8	More Details
CVE-2024-9890	The User Toolkit plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.2.3. This is due to an improper capability check in the 'switchUser' function. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to log in as any existing user on the site, such as an administrator.	8.8	More Details
CVE-2024-37847	An arbitrary file upload vulnerability in MangoOS before 5.1.4 and Mango API before 4.5.5 allows attackers to execute arbitrary code via a crafted file.	8.8	More Details
CVE-2022-30357	OvalEdge 5.2.8.0 and earlier is affected by an Account Takeover vulnerability via a POST request to /profile/updateProfile via the userId and email parameters. Authentication is required.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49376	Autolab, a course management service that enables auto-graded programming assignments, has misconfigured reset password permissions in version 3.0.0. For email-based accounts, users with insufficient privileges could reset and theoretically access privileged users' accounts by resetting their passwords. This issue is fixed in version 3.0.1. No known workarounds exist.	8.8	More Details
CVE-2024-42028	A Local privilege escalation vulnerability found in a Self-Hosted UniFi Network Server with UniFi Network Application (Version 8.4.62 and earlier) allows a malicious actor with a local operational system user to execute high privilege actions on UniFi Network Server.	8.8	More Details
CVE-2024-9235	The Mapster WP Maps plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to an insufficient capability check on the mapster_wp_maps_set_option_from_js() function in all versions up to, and including, 1.5.0. This makes it possible for authenticated attackers, with contributor-level access and above, to update arbitrary options on the WordPress site. This can be leveraged to update the default role for registration to administrator and enable user registration for attackers to gain administrative user access to a vulnerable site.	8.8	More Details
CVE-2024-10351	A vulnerability was found in Tenda RX9 Pro 22.03.02.20. It has been rated as critical. This issue affects the function sub_424CE0 of the file /goform/setMacFilterCfg of the component POST Request Handler. The manipulation of the argument deviceList leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-50488	Authentication Bypass Using an Alternate Path or Channel vulnerability in Priyabrata Sarkar Token Login allows Authentication Bypass.This issue affects Token Login: from n/a through 1.0.3.	8.8	More Details
CVE-2024-48594	File Upload vulnerability in Prison Management System v.1.0 allows a remote attacker to execute arbitrary code via the file upload component.	8.8	More Details
CVE-2024-48177	MRCMS 3.1.2 contains a SQL injection vulnerability via the RID parameter in /admin/article/delete.do.	8.8	More Details
CVE-2024-8312	An issue has been discovered in GitLab CE/EE affecting all versions from 15.10 before 17.3.6, 17.4 before 17.4.3, and 17.5 before 17.5.1. An attacker could inject HTML into the Global Search field on a diff view leading to XSS.	8.7	More Details
CVE-2024-20495	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 the device to reload unexpectedly, resulting in a denial of service (DoS) condition on an affected device. This vulnerability is due to improper validation of client key data after the TLS session is established. An attacker could exploit this vulnerability by sending a crafted key value to an affected system over the secure TLS session. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20426	A vulnerability in the Internet Key Exchange version 2 (IKEv2) protocol for VPN termination 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 insufficient input validation. An attacker could exploit this vulnerability by sending crafted IKEv2 traffic to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2024-20494	A vulnerability in the TLS cryptography functionality of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to improper data validation during the TLS 1.3 handshake. An attacker could exploit this vulnerability by sending a crafted TLS 1.3 packet to an affected system through a TLS 1.3-enabled listening socket. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: This vulnerability can also impact the integrity of a device by causing VPN HostScan communication failures or file transfer failures when Cisco ASA Software is upgraded using Cisco Adaptive Security Device Manager (ASDM).	8.6	More Details
CVE-2024-20260	A vulnerability in the VPN and management web servers of the Cisco Adaptive Security Virtual Appliance (ASAv) and Cisco Secure Firewall Threat Defense Virtual (FTDv), formerly Cisco Firepower Threat Defense Virtual, platforms could allow an unauthenticated, remote attacker to cause the virtual devices to run out of system memory, which could cause SSL VPN connection processing to slow down and eventually cease all together. This vulnerability is due to a lack of proper memory management for new incoming SSL/TLS connections on the virtual platforms. An attacker could exploit this vulnerability by sending a large number of new incoming SSL/TLS connections to the targeted virtual platform. A successful exploit could allow the attacker to deplete system memory, resulting in a denial of service (DoS) condition. The memory could be reclaimed slowly if the attack traffic is stopped, but a manual reload may be required to restore operations quickly.	8.6	More Details
CVE-2024-20402	A vulnerability in the SSL VPN feature for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to a logic error in memory management when the device is handling SSL VPN connections. An attacker could exploit this vulnerability by sending crafted SSL/TLS packets to the SSL VPN server of the affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20351	A vulnerability in the TCP/IP traffic handling function of the Snort Detection Engine of Cisco Firepower Threat Defense (FTD) Software and Cisco FirePOWER Services could allow an unauthenticated, remote attacker to cause legitimate network traffic to be dropped, resulting in a denial of service (DoS) condition. This vulnerability is due to the improper handling of TCP/IP network traffic. An attacker could exploit this vulnerability by sending a large amount of TCP/IP network traffic through the affected device. A successful exploit could allow the attacker to cause the Cisco FTD device to drop network traffic, resulting in a DoS condition. The affected device must be rebooted to resolve the DoS condition.	8.6	More Details
CVE-2024-48208	pure-ftpd before 1.0.52 is vulnerable to Buffer Overflow. There is an out of bounds read in the domlsd() function of the ls.c file.	8.6	More Details
CVE-2024-44270	A logic issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A sandboxed process may be able to circumvent sandbox restrictions.	8.6	More Details
CVE-2024-20330	A vulnerability in the Snort 2 and Snort 3 TCP and UDP detection engine of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series Appliances could allow an unauthenticated, remote attacker to cause memory corruption, which could cause the Snort detection engine to restart unexpectedly. This vulnerability is due to improper memory management when the Snort detection engine processes specific TCP or UDP packets. An attacker could exploit this vulnerability by sending crafted TCP or UDP packets through a device that is inspecting traffic using the Snort detection engine. A successful exploit could allow the attacker to restart the Snort detection engine repeatedly, which could cause a denial of service (DoS) condition. The DoS condition impacts only the traffic through the device that is examined by the Snort detection engine. The device can still be managed over the network. Note: Once a memory block is corrupted, it cannot be cleared until the Cisco Firepower 2100 Series Appliance is manually reloaded. This means that the Snort detection engine could crash repeatedly, causing traffic that is processed by the Snort detection engine to be dropped until the device is manually reloaded.	8.6	More Details
CVE-2024-44256	The issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to break out of its sandbox.	8.6	More Details
CVE-2024-20339	A vulnerability in the TLS processing feature of Cisco Firepower Threat Defense (FTD) Software for Cisco Firepower 2100 Series could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to an issue that occurs when TLS traffic is processed. An attacker could exploit this vulnerability by sending certain TLS traffic over IPv4 through an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition and impacting traffic to and through the affected device.	8.6	More Details
CVE-2024-50465	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WP SEO – Calin Vingan Premium SEO Pack allows SQL Injection.This issue affects Premium SEO Pack: from n/a through 1.6.001.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48542	Incorrect access control in the firmware update and download processes of Yamaha Headphones Controller v1.6.7 allows attackers to access sensitive information by analyzing the code and data within the APK file.	8.4	More Details
CVE-2024-48544	Incorrect access control in the firmware update and download processes of Sylvania Smart Home v3.0.3 allows attackers to access sensitive information by analyzing the code and data within the APK file.	8.4	More Details
CVE-2024-48545	Incorrect access control in the firmware update and download processes of IVY Smart v4.5.0 allows attackers to access sensitive information by analyzing the code and data within the APK file.	8.4	More Details
CVE-2024-48546	Incorrect access control in the firmware update and download processes of Wear Sync v1.2.0 allows attackers to access sensitive information by analyzing the code and data within the APK file.	8.4	More Details
CVE-2024-48547	Incorrect access control in the firmware update and download processes of DreamCatcher Life v1.8.7 allows attackers to access sensitive information by analyzing the code and data within the APK file.	8.4	More Details
CVE-2024-48541	Incorrect access control in the firmware update and download processes of Ruochan Smart v4.4.7 allows attackers to access sensitive information by analyzing the code and data within the APK file.	8.4	More Details
CVE-2024-50492	Improper Control of Generation of Code ('Code Injection') vulnerability in Scott Paterson ScottCart allows Code Injection.This issue affects ScottCart: from n/a through 1.1.	8.3	More Details
CVE-2024-5608	Zohocorp ManageEngine ADAudit Plus versions below 8121 are vulnerable to SQL Injection in the technician reports feature.	8.3	More Details
CVE-2024-0126	NVIDIA GPU Display Driver for Windows and Linux contains a vulnerability which could allow a privileged attacker to escalate permissions. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	8.2	More Details
CVE-2024-9302	The App Builder – Create Native Android & iOS Apps On The Flight plugin for WordPress is vulnerable to privilege escalation via account takeover in all versions up to, and including, 5.3.7. This is due to the verify_otp_forgot_password() and update_password() functions not having enough controls to prevent a successful brute force attack of the OTP to change a password, or verify that a password reset request came from an authorized user. This makes it possible for unauthenticated attackers to generate and brute force an OTP that makes it possible to change any users passwords, including an administrator.	8.1	More Details
CVE-2024-10011	The BuddyPress plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 14.1.0 via the id parameter. This makes it possible for authenticated attackers, with Subscriber-level access and above, to perform actions on files outside of the originally intended directory and enables file uploads to directories outside of the web root. Depending on server configuration it may be possible to upload files with double extensions. This vulnerability only affects Windows.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47881	OpenRefine is a free, open source tool for working with messy data. Starting in version 3.4-beta and prior to version 3.8.3, in the `database` extension, the "enable_load_extension" property can be set for the SQLite integration, enabling an attacker to load (local or remote) extension DLLs and so run arbitrary code on the server. The attacker needs to have network access to the OpenRefine instance. Version 3.8.3 fixes this issue.	8.1	More Details
CVE-2024-47880	OpenRefine is a free, open source tool for working with messy data. Prior to version 3.8.3, the `export-rows` command can be used in such a way that it reflects part of the request verbatim, with a Content-Type header also taken from the request. An attacker could lead a user to a malicious page that submits a form POST that contains embedded JavaScript code. This code would then be included in the response, along with an attacker-controlled `Content-Type` header, and so potentially executed in the victim's browser as if it was part of OpenRefine. The attacker-provided code can do anything the user can do, including deleting projects, retrieving database passwords, or executing arbitrary Jython or Closure expressions, if those extensions are also present. The attacker must know a valid project ID of a project that contains at least one row. Version 3.8.3 fixes the issue.	8.1	More Details
CVE-2024-47878	OpenRefine is a free, open source tool for working with messy data. Prior to version 3.8.3, the `/extension/gdata/authorized` endpoint includes the `state` GET parameter verbatim in a `<script>` tag in the output, so without escaping. An attacker could lead or redirect a user to a crafted URL containing JavaScript code, which would then cause that code to be executed in the victim's browser as if it was part of OpenRefine. Version 3.8.3 fixes this issue.	8.1	More Details
CVE-2024-47023	there is a possible man-in-the-middle attack due to a logic error in the code. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	8.1	More Details
CVE-2024-48955	Broken access control in NetAdmin 4.030319 returns data with functionalities on the endpoint that "assembles" the functionalities menus, the return of this call is not encrypted and as the system does not validate the session authorization, an attacker can copy the content of the browser of a user with greater privileges having access to the functionalities of the user that the code was copied.	8.1	More Details
CVE-2024-10327	A vulnerability in Okta Verify for iOS versions 9.25.1 (beta) and 9.27.0 (including beta) allows push notification responses through the iOS ContextExtension feature allowing the authentication to proceed regardless of the user’s selection. When a user long-presses the notification banner and selects an option, both options allow the authentication to succeed. The ContextExtension feature is one of several push mechanisms available when using Okta Verify Push on iOS devices. The vulnerable flows include: * When a user is presented with a notification on a locked screen, the user presses on the notification directly and selects their reply without unlocking the device; * When a user is presented with a notification on the home screen and drags the notification down and selects their reply; * When an Apple Watch is used to reply directly to a notification. A pre-condition for this vulnerability is that the user must have enrolled in Okta Verify while the Okta customer was using Okta Classic. This applies irrespective of whether the organization has since upgraded to Okta Identity Engine.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7474	In version 1.3.2 of lunary-ai/lunary, an Insecure Direct Object Reference (IDOR) vulnerability exists. A user can view or delete external users by manipulating the 'id' parameter in the request URL. The application does not perform adequate checks on the 'id' parameter, allowing unauthorized access to external user data.	8.1	More Details
CVE-2024-50550	Incorrect Privilege Assignment vulnerability in LiteSpeed Technologies LiteSpeed Cache allows Privilege Escalation.This issue affects LiteSpeed Cache: from n/a through 6.5.1.	8.1	More Details
CVE-2024-9947	The ProfilePress Pro plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 4.11.1. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email and the user does not have an already-existing account for the service returning the token.	8.1	More Details
CVE-2024-48178	newbee-mall v1.0.0 is vulnerable to Server-Side Request Forgery (SSRF) via the goodsCoverImg parameter.	8.1	More Details
CVE-2024-50497	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in BuyNowDepot Advanced Online Ordering and Delivery Platform allows PHP Local File Inclusion.This issue affects Advanced Online Ordering and Delivery Platform: from n/a through 2.0.0.	8.1	More Details
CVE-2024-47005	Sharp and Toshiba Tec MFPs provide configuration related APIs. They are expected to be called by administrative users only, but insufficiently restricted. A non-administrative user may execute some configuration APIs.	8.1	More Details
CVE-2024-10313	iniNet Solutions SpiderControl SCADA PC HMI Editor has a path traversal vulnerability. When the software loads a malicious ‘ems' project template file constructed by an attacker, it can write files to arbitrary directories. This can lead to overwriting system files, causing system paralysis, or writing to startup items, resulting in remote control.	8.0	More Details
CVE-2024-45260	An issue was discovered on certain GL-iNet devices, including MT6000, MT3000, MT2500, AXT1800, and AX1800 4.6.2. Users who belong to unauthorized groups can invoke any interface of the device, thereby gaining complete control over it.	8.0	More Details
CVE-2024-45261	An issue was discovered on certain GL-iNet devices, including MT6000, MT3000, MT2500, AXT1800, and AX1800 4.6.2. The SID generated for a specific user is not tied to that user itself, which allows other users to potentially use it for authentication. Once an attacker bypasses the application's authentication procedures, they can generate a valid SID, escalate privileges, and gain full control.	8.0	More Details
CVE-2024-48074	An authorized RCE vulnerability exists in the DrayTek Vigor2960 router version 1.4.4, where an attacker can place a malicious command into the table parameter of the doPPPoE function in the cgi-bin/mainfunction.cgi route, and finally the command is executed by the system function.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48826	Tenda AC7 v.15.03.06.44 ate_iwpriv_set has pre-authentication command injection allowing remote attackers to execute arbitrary code.	8.0	More Details
CVE-2024-48825	Tenda AC7 v.15.03.06.44 ate_ifconfig_set has pre-authentication command injection allowing remote attackers to execute arbitrary code.	8.0	More Details
CVE-2024-50071	In the Linux kernel, the following vulnerability has been resolved: pinctrl: nuvoton: fix a double free in ma35_pinctrl_dt_node_to_map_func() 'new_map' is allocated using devm_* which takes care of freeing the allocated data on device removal, call to .dt_free_map = pinconf_generic_dt_free_map double frees the map as pinconf_generic_dt_free_map() calls pinctrl_utils_free_map(). Fix this by using kcalloc() instead of auto-managed devm_kcalloc().	7.8	More Details
CVE-2024-8597	A maliciously crafted STP file when parsed in ASMDATAX230A.dll through Autodesk AutoCAD can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-0121	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2024-9489	A maliciously crafted DWG file when parsed in ACAD.exe through Autodesk AutoCAD can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-0127	NVIDIA vGPU software contains a vulnerability in the GPU kernel driver of the vGPU Manager for all supported hypervisors, where a user of the guest OS can cause an improper input validation by compromising the guest OS kernel. A successful exploit of this vulnerability might lead to code execution, escalation of privileges, data tampering, denial of service, and information disclosure.	7.8	More Details
CVE-2024-47904	A vulnerability has been identified in InterMesh 7177 Hybrid 2.0 Subscriber (All versions < V8.2.12), InterMesh 7707 Fire Subscriber (All versions < V7.2.12 only if the IP interface is enabled (which is not the default configuration)). The affected devices contain a SUID binary that could allow an authenticated local attacker to execute arbitrary commands with root privileges.	7.8	More Details
CVE-2024-47035	In vring_init of external/headers/include/virtio/virtio_ring.h, there is a possible out of bounds write due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-47041	In valid_address of syscall.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44285	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 18.1 and iPadOS 18.1, watchOS 11.1, visionOS 2.1, tvOS 18.1. An app may be able to cause unexpected system termination or corrupt kernel memory.	7.8	More Details
CVE-2024-50073	In the Linux kernel, the following vulnerability has been resolved: tty: n_gsm: Fix use-after-free in gsm_cleanup_mux BUG: KASAN: slab-use-after-free in gsm_cleanup_mux+0x77b/0x7b0 drivers/tty/n_gsm.c:3160 [n_gsm] Read of size 8 at addr ffff88815fe99c00 by task poc/3379 CPU: 0 UID: 0 PID: 3379 Comm: poc Not tainted 6.11.0+ #56 Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 11/12/2020 Call Trace: <TASK> gsm_cleanup_mux+0x77b/0x7b0 drivers/tty/n_gsm.c:3160 [n_gsm] __pfx_gsm_cleanup_mux+0x10/0x10 drivers/tty/n_gsm.c:3124 [n_gsm] __pfx_sched_clock_cpu+0x10/0x10 kernel/sched/clock.c:389 update_load_avg+0x1c1/0x27b0 kernel/sched/fair.c:4500 __pfx_min_vruntime_cb_rotate+0x10/0x10 kernel/sched/fair.c:846 __rb_insert_augmented+0x492/0xbf0 lib/rbtree.c:161 gsmld_ioctl+0x395/0x1450 drivers/tty/n_gsm.c:3408 [n_gsm] _raw_spin_lock_irqsave+0x92/0xf0 arch/x86/include/asm/atomic.h:107 __pfx_gsmld_ioctl+0x10/0x10 drivers/tty/n_gsm.c:3822 [n_gsm] ktime_get+0x5e/0x140 kernel/time/timekeeping.c:195 ldsem_down_read+0x94/0x4e0 arch/x86/include/asm/atomic64_64.h:79 __pfx_ldsem_down_read+0x10/0x10 drivers/tty/tty_ldsem.c:338 __pfx_do_vfs_ioctl+0x10/0x10 fs/ioctl.c:805 tty_ioctl+0x643/0x1100 drivers/tty/tty_io.c:2818 Allocated by task 65: gsm_data_alloc.constprop.0+0x27/0x190 drivers/tty/n_gsm.c:926 [n_gsm] gsm_send+0x2c/0x580 drivers/tty/n_gsm.c:819 [n_gsm] gsm1_receive+0x547/0xad0 drivers/tty/n_gsm.c:3038 [n_gsm] gsmld_receive_buf+0x176/0x280 drivers/tty/n_gsm.c:3609 [n_gsm] tty_ldisc_receive_buf+0x101/0x1e0 drivers/tty/tty_buffer.c:391 tty_port_default_receive_buf+0x61/0xa0 drivers/tty/tty_port.c:39 flush_to_ldisc+0x1b0/0x750 drivers/tty/tty_buffer.c:445 process_scheduled_works+0x2b0/0x10d0 kernel/workqueue.c:3229 worker_thread+0x3dc/0x950 kernel/workqueue.c:3391 kthread+0x2a3/0x370 kernel/kthread.c:389 ret_from_fork+0x2d/0x70 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:257 Freed by task 3367: kfree+0x126/0x420 mm/slub.c:4580 gsm_cleanup_mux+0x36c/0x7b0 drivers/tty/n_gsm.c:3160 [n_gsm] gsmld_ioctl+0x395/0x1450 drivers/tty/n_gsm.c:3408 [n_gsm] tty_ioctl+0x643/0x1100 drivers/tty/tty_io.c:2818 [Analysis] gsm_msg on the tx_ctrl_list or tx_data_list of gsm_mux can be freed by multi threads through ioctl,which leads to the occurrence of uaf. Protect it by gsm tx lock.	7.8	More Details
CVE-2024-44277	The issue was addressed with improved memory handling. This issue is fixed in iOS 18.1 and iPadOS 18.1, visionOS 2.1, tvOS 18.1. An app may be able to cause unexpected system termination or corrupt kernel memory.	7.8	More Details
CVE-2024-9826	A maliciously crafted 3DM file when parsed in atf_api.dll through Autodesk AutoCAD can force a Use-After-Free vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8596	A maliciously crafted MODEL file when parsed in libodxdll.dll through Autodesk AutoCAD can force an Out-of-Bound Write vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-9827	A maliciously crafted CATPART file when parsed in CC5Dll.dll through Autodesk AutoCAD can force an Out-of-Bounds Read vulnerability. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-9996	A maliciously crafted DWG file when parsed in acdb25.dll through Autodesk AutoCAD can force an Out-of-Bounds Write vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-9997	A maliciously crafted DWG file when parsed in acdb25.dll through Autodesk AutoCAD can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-8598	A maliciously crafted STP file when parsed in ACTranslators.exe through Autodesk AutoCAD can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-45242	EnGenius ENH1350EXT A8J-ENH1350EXT devices through 3.9.3.2_c1.9.51 allow (blind) OS Command Injection via shell metacharacters to the Ping or Speed Test utility. During the time of initial setup, the device creates an open unsecured network whose admin panel is configured with the default credentials of admin/admin. An unauthorized attacker in proximity to the Wi-Fi network can exploit this window of time to execute arbitrary OS commands with root-level permissions.	7.8	More Details
CVE-2024-0120	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2024-47033	In lwis_allocator_free of lwis_allocator.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-47027	In sm_mem_compat_get_vmm_obj of lib/sm/shared_mem.c, there is a possible arbitrary physical memory access due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-47024	In vring_size of external/headers/include/virtio/virtio_ring.h, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47017	In ufshc_scsi_cmd of ufs.c, there is a possible stack variable use after free due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-47016	there is a possible privilege escalation due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-8896	A maliciously crafted DXF file when parsed in acdb25.dll through Autodesk AutoCAD can force to access a variable prior to initialization. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-0119	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2024-48423	An issue in assimp v.5.4.3 allows a local attacker to execute arbitrary code via the CallbackToLogRedirector function within the Assimp library.	7.8	More Details
CVE-2024-0118	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2024-0117	NVIDIA GPU Display Driver for Windows contains a vulnerability in the user mode layer, where an unprivileged regular user can cause an out-of-bounds read. A successful exploit of this vulnerability might lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2024-47013	In pmucal_rae_handle_seq_int of flexpmu_cal_rae.c, there is a possible arbitrary write due to uninitialized data. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-50074	In the Linux kernel, the following vulnerability has been resolved: parport: Proper fix for array out-of-bounds access The recent fix for array out-of-bounds accesses replaced sprintf() calls blindly with snprintf(). However, since snprintf() returns the would-be-printed size, not the actually output size, the length calculation can still go over the given limit. Use scnprintf() instead of snprintf(), which returns the actually output letters, for addressing the potential out-of-bounds access properly.	7.8	More Details
CVE-2024-47012	In mm_GetMobileIdIndexForNsUpdate of mm_GmmPduCodec.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-8600	A maliciously crafted SLDPRT file when parsed in odxsw_dll.dll through Autodesk AutoCAD can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8599	A maliciously crafted STP file when parsed in ACTranslators.exe through Autodesk AutoCAD can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-8590	A maliciously crafted 3DM file when parsed in atf_api.dll through Autodesk AutoCAD can force a Use-After-Free vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-44126	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sequoia 15, iOS 17.7 and iPadOS 17.7, macOS Sonoma 14.7, visionOS 2, iOS 18 and iPadOS 18. Processing a maliciously crafted file may lead to heap corruption.	7.8	More Details
CVE-2024-8587	A maliciously crafted SLDPRT file when parsed in odxsw_dll.dll through Autodesk AutoCAD can force a Heap Based Buffer Overflow vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-44255	A path handling issue was addressed with improved logic. This issue is fixed in visionOS 2.1, iOS 18.1 and iPadOS 18.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, tvOS 18.1. A malicious app may be able to run arbitrary shortcuts without user consent.	7.8	More Details
CVE-2024-8595	A maliciously crafted MODEL file when parsed in libodxdll.dll through Autodesk AutoCAD can force a Use-After-Free vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-8594	A maliciously crafted MODEL file when parsed in libodxdll.dll through Autodesk AutoCAD can force a Heap-Based Overflow vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-8593	A maliciously crafted CATPART file when parsed in ASMKERN230A.dll through Autodesk AutoCAD can force a Out-of-Bounds Write vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
	In the Linux kernel, the following vulnerability has been resolved: uprobe: avoid out-of-bounds memory access of fetching args Uprobe needs to fetch args into a percpu buffer, and then copy to ring buffer to avoid non-atomic context problem. Sometimes user-space strings, arrays can be very large, but the size of percpu buffer is only page size. And store_trace_args() won't check whether these data exceeds a single page or not, caused out-of-bounds memory access. It could be reproduced by following steps: 1. build kernel with CONFIG_KASAN enabled 2. save follow program as test.c ``` \#include <stdio.h> \#include <stdlib.h> \#include <string.h> // If string length large than MAX_STRING_SIZE, the fetch_store_strlen() // will return 0, cause __get_data_size() return shorter size, and // store_trace_args() will not trigger out-of-bounds access. // So make string length less than 4096. \#define STRLEN 4093 void generate_string(char *str, int n) { int i; for (i = 0; i < n; ++i) { char c = i % 26 + 'a'; str[i] = c; } str[n-1] = '\0'; }		

CVE Number	Description	Base Score	Reference
CVE-2024-50067	void print_string(char *str) { printf("%s\n", str); } int main() { char tmp[STRLEN]; generate_string(tmp, STRLEN); print_string(tmp); return 0; } ``` 3. compile program `gcc -o test test.c` 4. get the offset of `print_string()` ``` objdump -t test | grep -w print_string 0000000000401199 g F .text 000000000000001b print_string ``` 5. configure uprobe with offset 0x1199 ``` off=0x1199 cd /sys/kernel/debug/tracing/ echo "p /root/test:${off} arg1=+0(%di):ustring arg2=\$comm arg3=+0(%di):ustring" > uprobe_events echo 1 > events/uprobes/enable echo 1 > tracing_on ``` 6. run `test`, and kasan will report error. == BUG: KASAN: use-after-free in strncpy_from_user+0x1d6/0x1f0 Write of size 8 at addr ffff88812311c004 by task test/499CPU: 0 UID: 0 PID: 499 Comm: test Not tainted 6.12.0-rc3+ #18 Hardware name: Red Hat KVM, BIOS 1.16.0-4.al8 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x55/0x70 print_address_description.constprop.0+0x27/0x310 kasan_report+0x10f/0x120 ? strncpy_from_user+0x1d6/0x1f0 strncpy_from_user+0x1d6/0x1f0 ? rmqueue.constprop.0+0x70d/0x2ad0 process_fetch_insn+0xb26/0x1470 ? __pfx_process_fetch_insn+0x10/0x10 ? _raw_spin_lock+0x85/0xe0 ? __pfx__raw_spin_lock+0x10/0x10 ? __pte_offset_map+0x1f/0x2d0 ? unwind_next_frame+0xc5f/0x1f80 ? arch_stack_walk+0x68/0xf0 ? is_bpf_text_address+0x23/0x30 ? kernel_text_address.part.0+0xbb/0xd0 ? __kernel_text_address+0x66/0xb0 ? unwind_get_return_address+0x5e/0xa0 ? __pfx_stack_trace_consume_entry+0x10/0x10 ? arch_stack_walk+0xa2/0xf0 ? _raw_spin_lock_irqsave+0x8b/0xf0 ? __pfx__raw_spin_lock_irqsave+0x10/0x10 ? depot_alloc_stack+0x4c/0x1f0 ? _raw_spin_unlock_irqrestore+0xe/0x30 ? stack_depot_save_flags+0x35d/0x4f0 ? kasan_save_stack+0x34/0x50 ? kasan_save_stack+0x24/0x50 ? mutex_lock+0x91/0xe0 ? __pfx_mutex_lock+0x10/0x10 prepare_uprobe_buffer.part.0+0x2cd/0x500 uprobe_dispatcher+0x2c3/0x6a0 ? __pfx_uprobe_dispatcher+0x10/0x10 ? __kasan_slab_alloc+0x4d/0x90 handler_chain+0xdd/0x3e0 handle_swbp+0x26e/0x3d0 ? __pfx_handle_swbp+0x10/0x10 ? uprobe_pre_sstep_notifier+0x151/0x1b0 irqentry_exit_to_user_mode+0xe2/0x1b0 asm_exc_int3+0x39/0x40 RIP: 0033:0x401199 Code: 01 c2 0f b6 45 fb 88 02 83 45 fc 01 8b 45 fc 3b 45 e4 7c b7 8b 45 e4 48 98 48 8d 50 ff 48 8b 45 e8 48 01 d0 ce RSP: 002b:00007ffdf00576a8 EFLAGS: 00000206 RAX: 00007ffdf00576b0 RBX: 0000000000000000 RCX: 0000000000000ff2 RDX: 0000000000000ffc RSI: 0000000000000ffd RDI: 00007ffdf00576b0 RBP: 00007ffdf00586b0 R08: 00007feb2f9c0d20 R09: 00007feb2f9c0d20 R10: 0000000000000001 R11: 0000000000000202 R12: 0000000000401040 R13: 00007ffdf0058780 R14: 0000000000000000 R15: 0000000000000000 </TASK> This commit enforces the buffer's maxlen less than a page-size to avoid store_trace_args() out-of-memory access.	7.8	More Details
CVE-2024-50088	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix uninitialized pointer free in add_inode_ref() The add_inode_ref() function does not initialize the "name" struct when it is declared. If any of the following calls to "read_one_inode() returns NULL, dir = read_one_inode(root, parent_objectid); if (!dir) { ret = -ENOENT; goto out; } inode = read_one_inode(root, inode_objectid); if (!inode) { ret = -EIO; goto out; } then "name.name" would be freed on "out" before being initialized. out: ... kfree(name.name); This issue was reported by Coverity with CID 1526744.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7991	A maliciously crafted DWG file, when parsed through Autodesk AutoCAD and certain AutoCAD-based products, can force an Out-of-Bounds Write. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-8592	A maliciously crafted CATPART file when parsed in AcTranslators.exe through Autodesk AutoCAD can force a Memory Corruption vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-44218	This issue was addressed with improved checks. This issue is fixed in iOS 17.7.1 and iPadOS 17.7.1, macOS Sonoma 14.7.1, iOS 18.1 and iPadOS 18.1. Processing a maliciously crafted file may lead to heap corruption.	7.8	More Details
CVE-2024-8591	A maliciously crafted 3DM file when parsed in AcTranslators.exe through Autodesk AutoCAD can force a Heap-Based Buffer Overflow vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-8589	A maliciously crafted SLDPRT file when parsed in odxsw_dll.dll through Autodesk AutoCAD can force a Out-of-Bounds Read vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-7992	A maliciously crafted DWG file, when parsed through Autodesk AutoCAD and certain AutoCAD-based products, can force a Stack-based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-8588	A maliciously crafted SLDPRT file when parsed in odxsw_dll.dll through Autodesk AutoCAD can force a Out-of-Bounds Read vulnerability. A malicious actor can leverage this vulnerability to cause a crash, write sensitive data, or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-20408	A vulnerability in the Dynamic Access Policies (DAP) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to cause an affected device to reload unexpectedly. To exploit this vulnerability, an attacker would need valid remote access VPN user credentials on the affected device. This vulnerability is due to improper validation of data in HTTPS POST requests. An attacker could exploit this vulnerability by sending a crafted HTTPS POST request to an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a denial of service (DoS) condition.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20268	A vulnerability in the Simple Network Management Protocol (SNMP) feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, remote attacker to cause an unexpected reload of the device. This vulnerability is due to insufficient input validation of SNMP packets. An attacker could exploit this vulnerability by sending a crafted SNMP request to an affected device using IPv4 or IPv6. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a denial of service (DoS) condition. This vulnerability affects all versions of SNMP (versions 1, 2c, and 3) and requires a valid SNMP community string or valid SNMPv3 user credentials.	7.7	More Details
CVE-2024-49657	Missing Authorization vulnerability in ReneeCussack 3D Work In Progress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects 3D Work In Progress: from n/a through 1.0.3.	7.7	More Details
CVE-2024-49691	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Woobewoo Product Filter by WBW allows SQL Injection.This issue affects Product Filter by WBW: from n/a through 2.7.0.	7.6	More Details
CVE-2024-47879	OpenRefine is a free, open source tool for working with messy data. Prior to version 3.8.3, lack of cross-site request forgery protection on the `preview-expression` command means that visiting a malicious website could cause an attacker-controlled expression to be executed. The expression can contain arbitrary Clojure or Python code. The attacker must know a valid project ID of a project that contains at least one row, and the attacker must convince the victim to open a malicious webpage. Version 3.8.3 fixes the issue.	7.6	More Details
CVE-2024-48931	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In version 1.2.4 and all prior versions, the ZimaOS API endpoint `http://<Zima_Server_IP:PORT>/v3/file?token=<token>&files=<file_path>` is vulnerable to arbitrary file reading due to improper input validation. By manipulating the `files` parameter, authenticated users can read sensitive system files, including `/etc/shadow`, which contains password hashes for all users. This vulnerability exposes critical system data and poses a high risk for privilege escalation or system compromise. The vulnerability occurs because the API endpoint does not validate or restrict file paths provided via the `files` parameter. An attacker can exploit this by manipulating the file path to access sensitive files outside the intended directory. As of time of publication, no known patched versions are available.	7.5	More Details
CVE-2024-49357	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In version 1.2.4 and all prior versions, the API endpoints in ZimaOS, such as `http://<Server-IP>/v1/users/image?path=/var/lib/casaos/1/app_order.json` and `http://<Server-IP>/v1/users/image?path=/var/lib/casaos/1/system.json`, expose sensitive data like installed applications and system information without requiring any authentication or authorization. This sensitive data leak can be exploited by attackers to gain detailed knowledge about the system setup, installed applications, and other critical information. As of time of publication, no known patched versions are available.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49761	REXML is an XML toolkit for Ruby. The REXML gem before 3.3.9 has a ReDoS vulnerability when it parses an XML that has many digits between &# and x...; in a hex numeric character reference (&#x...;). This does not happen with Ruby 3.2 or later. Ruby 3.1 is the only affected maintained Ruby. The REXML gem 3.3.9 or later include the patch to fix the vulnerability.	7.5	More Details
CVE-2024-42011	The Spotify app 8.9.58 for iOS has a buffer overflow in its use of strcat.	7.5	More Details
CVE-2024-10438	The eHRD CTMS from Sunnet has an Authentication Bypass vulnerability, allowing unauthenticated remote attackers to bypass authentication by satisfying specific conditions in order to access certain functionalities.	7.5	More Details
CVE-2024-44259	This issue was addressed through improved state management. This issue is fixed in iOS 17.7.1 and iPadOS 17.7.1, visionOS 2.1, iOS 18.1 and iPadOS 18.1, macOS Sequoia 15.1, Safari 18.1. An attacker may be able to misuse a trust relationship to download malicious content.	7.5	More Details
CVE-2024-42420	Sharp and Toshiba Tec MFPs contain multiple Out-of-bounds Read vulnerabilities, due to improper processing of keyword search input and improper processing of SOAP messages. Crafted HTTP requests may cause affected products crashed.	7.5	More Details
CVE-2024-43424	Sharp and Toshiba Tec MFPs improperly process HTTP request headers, resulting in an Out-of-bounds Read vulnerability. Crafted HTTP requests may cause affected products crashed.	7.5	More Details
CVE-2024-44080	In Jitsi Meet before 2.0.9779, the functionality to share an image using giphy was implemented in an insecure way, resulting in clients loading GIFs from any arbitrary URL if a message from another participant contains a URL encoded in the expected format.	7.5	More Details
CVE-2024-48142	A prompt injection vulnerability in the chatbox of Butterfly Effect Limited Monica ChatGPT AI Assistant v2.4.0 allows attackers to access and exfiltrate all previous and subsequent chat data between the user and the AI assistant via a crafted message.	7.5	More Details
CVE-2024-45785	MUSASI version 3 contains an issue with use of client-side authentication. If this vulnerability is exploited, other users' credential and sensitive information may be retrieved.	7.5	More Details
CVE-2024-6049	The web server of Lawo AG vsm LTC Time Sync (vTimeSync) is affected by a "..." (triple dot) path traversal vulnerability. By sending a specially crafted HTTP request, an unauthenticated remote attacker could download arbitrary files from the operating system. As a limitation, the exploitation is only possible if the requested file has some file extension, e. g. .exe or .txt.	7.5	More Details
CVE-2024-45802	Squid is an open source caching proxy for the Web supporting HTTP, HTTPS, FTP, and more. Due to Input Validation, Premature Release of Resource During Expected Lifetime, and Missing Release of Resource after Effective Lifetime bugs, Squid is vulnerable to Denial of Service attacks by a trusted server against all clients using the proxy. This bug is fixed in the default build configuration of Squid version 6.10.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10466	By sending a specially crafted push message, a remote server could have hung the parent process, causing the browser to become unresponsive. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	7.5	More Details
CVE-2024-50083	In the Linux kernel, the following vulnerability has been resolved: tcp: fix mptcp DSS corruption due to large pmtu xmit Syzkaller was able to trigger a DSS corruption: TCP: request_sock_subflow_v4: Possible SYN flooding on port [::]:20002. Sending cookies. ------------[cut here]------------ WARNING: CPU: 0 PID: 5227 at net/mptcp/protocol.c:695 __mptcp_move_skbs_from_subflow+0x20a9/0x21f0 net/mptcp/protocol.c:695 Modules linked in: CPU: 0 UID: 0 PID: 5227 Comm: syz-executor350 Not tainted 6.11.0-syzkaller-08829-gaf9c191ac2a0 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024 RIP: 0010:__mptcp_move_skbs_from_subflow+0x20a9/0x21f0 net/mptcp/protocol.c:695 Code: 0f b6 dc 31 ff 89 de e8 b5 dd ea f5 89 d8 48 81 c4 50 01 00 00 5b 41 5c 41 5d 41 5e 41 5f 5d c3 cc cc cc cc e8 98 da ea f5 90 <0f> 0b 90 e9 47 ff ff ff e8 8a da ea f5 90 0f 0b 90 e9 99 e0 ff ff RSP: 0018:ffffc90000006db8 EFLAGS: 00010246 RAX: ffffffff8ba9df18 RBX: 00000000000055f0 RCX: ffff888030023c00 RDX: 0000000000000100 RSI: 00000000000081e5 RDI: 00000000000055f0 RBP: 1ffff110062bf1ae R08: ffffffff8ba9cf12 R09: 1ffff110062bf1b8 R10: dffffc0000000000 R11: ffffed10062bf1b9 R12: 0000000000000000 R13: dffffc0000000000 R14: 00000000700cec61 R15: 00000000000081e5 FS: 000055556679c380(0000) GS:ffff8880b8600000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000020287000 CR3: 0000000077892000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <IRQ> move_skbs_to_msk net/mptcp/protocol.c:811 [inline] mptcp_data_ready+0x29c/0xa90 net/mptcp/protocol.c:854 subflow_data_ready+0x34a/0x920 net/mptcp/subflow.c:1490 tcp_data_queue+0x20fd/0x76c0 net/ipv4/tcp_input.c:5283 tcp_rcv_established+0xfba/0x2020 net/ipv4/tcp_input.c:6237 tcp_v4_do_rcv+0x96d/0xc70 net/ipv4/tcp_ipv4.c:1915 tcp_v4_rcv+0x2dc0/0x37f0 net/ipv4/tcp_ipv4.c:2350 ip_protocol_deliver_rcu+0x22e/0x440 net/ipv4/ip_input.c:205 ip_local_deliver_finish+0x341/0x5f0 net/ipv4/ip_input.c:233 NF_HOOK+0x3a4/0x450 include/linux/netfilter.h:314 NF_HOOK+0x3a4/0x450 include/linux/netfilter.h:314 __netif_receive_skb_one_core net/core/dev.c:5662 [inline] __netif_receive_skb+0x2bf/0x650 net/core/dev.c:5775 process_backlog+0x662/0x15b0 net/core/dev.c:6107 __napi_poll+0xcb/0x490 net/core/dev.c:6771 napi_poll net/core/dev.c:6840 [inline] net_rx_action+0x89b/0x1240 net/core/dev.c:6962 handle_softirqs+0x2c5/0x980 kernel/softirq.c:554 do_softirq+0x11b/0x1e0 kernel/softirq.c:455 </IRQ> <TASK> __local_bh_enable_ip+0x1bb/0x200 kernel/softirq.c:382 local_bh_enable include/linux/bottom_half.h:33 [inline] rcu_read_unlock_bh include/linux/rcupdate.h:919 [inline] __dev_queue_xmit+0x1764/0x3e80 net/core/dev.c:4451 dev_queue_xmit include/linux/netdevice.h:3094 [inline] neigh_hh_output include/net/neighbour.h:526 [inline] neigh_output include/net/neighbour.h:540 [inline] ip_finish_output2+0xd41/0x1390 net/ipv4/ip_output.c:236 ip_local_out net/ipv4/ip_output.c:130 [inline] __ip_queue_xmit+0x118c/0x1b80 net/ipv4/ip_output.c:536 __tcp_transmit_skb+0x2544/0x3b30 net/ipv4/tcp_output.c:1466 tcp_transmit_skb net/ipv4/tcp_output.c:1484 [inline] tcp_mtu_probe net/ipv4/tcp_output.c:2547 [inline] tcp_write_xmit+0x641d/0x6bf0	7.5	More Details

CVE Number	Description	Base Score	Reference
	net/ipv4/tcp_output.c:2752 __tcp_push_pending_frames+0x9b/0x360 net/ipv4/tcp_output.c:3015 tcp_push_pending_frames include/net/tcp.h:2107 [inline] tcp_data_snd_check net/ipv4/tcp_input.c:5714 [inline] tcp_rcv_established+0x1026/0x2020 net/ipv4/tcp_input.c:6239 tcp_v4_do_rcv+0x96d/0xc70 net/ipv4/tcp_ipv4.c:1915 sk_backlog_rcv include/net/sock.h:1113 [inline] __release_sock+0x214/0x350 net/core/sock.c:3072 release_sock+0x61/0x1f0 net/core/sock.c:3626 mptcp_push_ ---truncated---		
CVE-2024-10387	CVE-2024-10387 IMPACT A Denial-of-Service vulnerability exists in the affected product. The vulnerability could allow a threat actor with network access to send crafted messages to the device, potentially resulting in Denial-of-Service.	7.5	More Details
CVE-2024-10459	An attacker could have caused a use-after-free when accessibility was enabled, leading to a potentially exploitable crash. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Firefox ESR < 115.17, Thunderbird < 128.4, and Thunderbird < 132.	7.5	More Details
CVE-2024-10458	A permission leak could have occurred from a trusted site to an untrusted site via `embed` or `object` elements. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Firefox ESR < 115.17, Thunderbird < 128.4, and Thunderbird < 132.	7.5	More Details
CVE-2022-30354	OvalEdge 5.2.8.0 and earlier is affected by a Sensitive Data Exposure vulnerability via a GET request to /user/getUserWithTeam. Authentication is required. The information disclosed is associated with all registered user ID numbers.	7.5	More Details
CVE-2024-49757	The open-source identity infrastructure software Zitadel allows administrators to disable the user self-registration. Due to a missing security check in versions prior to 2.64.0, 2.63.5, 2.62.7, 2.61.4, 2.60.4, 2.59.5, and 2.58.7, disabling the "User Registration allowed" option only hid the registration button on the login page. Users could bypass this restriction by directly accessing the registration URL (/ui/login/loginname) and register a user that way. Versions 2.64.0, 2.63.5, 2.62.7, 2.61.4, 2.60.4, 2.59.5, and 2.58.7 contain a patch. No known workarounds are available.	7.5	More Details
CVE-2024-49381	Plenti, a static site generator, has an arbitrary file deletion vulnerability in versions prior to 0.7.2. The `/postLocal` endpoint is vulnerable to an arbitrary file write deletion when a plenti user serves their website. This issue may lead to information loss. Version 0.7.2 fixes the vulnerability.	7.5	More Details
CVE-2024-44228	This issue was addressed with improved permissions checking. This issue is fixed in Xcode 16. An app may be able to inherit Xcode permissions and access user data.	7.5	More Details
CVE-2024-44208	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15. An app may be able to bypass certain Privacy preferences.	7.5	More Details
CVE-2024-44100	Android before 2024-10-05 on Google Pixel devices allows information disclosure in the modem component, A-299774545.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49767	Werkzeug is a Web Server Gateway Interface web application library. Applications using `werkzeug.formparser.MultiPartParser` corresponding to a version of Werkzeug prior to 3.0.6 to parse `multipart/form-data` requests (e.g. all flask applications) are vulnerable to a relatively simple but effective resource exhaustion (denial of service) attack. A specifically crafted form submission request can cause the parser to allocate and block 3 to 8 times the upload size in main memory. There is no upper limit; a single upload at 1 Gbit/s can exhaust 32 GB of RAM in less than 60 seconds. Werkzeug version 3.0.6 fixes this issue.	7.5	More Details
CVE-2024-44203	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access a user's Photos Library.	7.5	More Details
CVE-2024-10455	Reachable Assertion in BPv7 parser in μD3TN v0.14.0 allows attacker to disrupt service via malformed Extension Block	7.5	More Details
CVE-2024-47022	Android before 2024-10-05 on Google Pixel devices allows information disclosure in the ACPM component, A-331255656.	7.5	More Details
CVE-2024-47021	In sms_ExtractCbLanguage of sms_CellBroadcast.c, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2024-47020	Android before 2024-10-05 on Google Pixel devices allows information disclosure in the ABL component, A-331966488.	7.5	More Details
CVE-2024-48140	A prompt injection vulnerability in the chatbox of Butterfly Effect Limited Monica Your AI Copilot powered by ChatGPT4 v6.3.0 allows attackers to access and exfiltrate all previous and subsequent chat data between the user and the AI assistant via a crafted message.	7.5	More Details
CVE-2024-44101	there is a possible Null Pointer Dereference (modem crash) due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2024-48141	A prompt injection vulnerability in the chatbox of Zhipu AI CodeGeeX v2.17.0 allows attackers to access and exfiltrate all previous and subsequent chat data between the user and the AI assistant via a crafted message.	7.5	More Details
CVE-2024-49359	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In version 1.2.4 and all prior versions, the API endpoint `http://<Zima_Server_IP:PORT>/v2_1/file` in ZimaOS is vulnerable to a directory traversal attack, allowing authenticated users to list the contents of any directory on the server. By manipulating the path parameter, attackers can access sensitive system directories such as `/etc`, potentially exposing critical configuration files and increasing the risk of further attacks. As of time of publication, no known patched versions are available.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48139	A prompt injection vulnerability in the chatbox of Blackbox AI v1.3.95 allows attackers to access and exfiltrate all previous and subsequent chat data between the user and the AI assistant via a crafted message.	7.5	More Details
CVE-2024-49769	Waitress is a Web Server Gateway Interface server for Python 2 and 3. When a remote client closes the connection before waitress has had the opportunity to call getpeername() waitress won't correctly clean up the connection leading to the main thread attempting to write to a socket that no longer exists, but not removing it from the list of sockets to attempt to process. This leads to a busy-loop calling the write function. A remote attacker could run waitress out of available sockets with very little resources required. Waitress 3.0.1 contains fixes that remove the race condition.	7.5	More Details
CVE-2024-50435	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Theme Horse Meta News.This issue affects Meta News: from n/a through 1.1.7.	7.5	More Details
CVE-2024-7807	A vulnerability in gaizhenbiao/chuanhuchatgpt version 20240628 allows for a Denial of Service (DOS) attack. When uploading a file, if an attacker appends a large number of characters to the end of a multipart boundary, the system will continuously process each character, rendering ChuanhuChatGPT inaccessible. This uncontrolled resource consumption can lead to prolonged unavailability of the service, disrupting operations and causing potential data inaccessibility and loss of productivity.	7.5	More Details
CVE-2024-7962	An arbitrary file read vulnerability exists in gaizhenbiao/chuanhuchatgpt version 20240628 due to insufficient validation when loading prompt template files. An attacker can read any file that matches specific criteria using an absolute path. The file must not have a .json extension and, except for the first line, every other line must contain commas. This vulnerability allows reading parts of format-compliant files, including code and log files, which may contain highly sensitive information such as account credentials.	7.5	More Details
CVE-2024-50436	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Theme Horse Clean Retina.This issue affects Clean Retina: from n/a through 3.0.6.	7.5	More Details
CVE-2024-50457	: Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Qode Interactive Qode Essential Addons.This issue affects Qode Essential Addons: from n/a through 1.6.3.	7.5	More Details
CVE-2020-26311	Useragent is a user agent parser for Node.js. All versions as of time of publication contain one or more regular expressions that are vulnerable to Regular Expression Denial of Service (ReDoS). As of time of publication, no patches are available.	7.5	More Details
CVE-2024-22066	There is a privilege escalation vulnerability in ZTE ZXR10 ZSR V2 intelligent multi service router . An authenticated attacker could use the vulnerability to obtain sensitive information about the device.	7.5	More Details
CVE-2024-48196	An issue in eyouCMS v.1.6.7 allows a remote attacker to obtain sensitive information via a crafted script to the post parameter.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48964	The package Snyk CLI before 1.1294.0 is vulnerable to Code Injection when scanning an untrusted Gradle project. The vulnerability can be triggered if Snyk test is run inside the untrusted project due to the improper handling of the current working directory name. Snyk recommends only scanning trusted projects.	7.5	More Details
CVE-2024-48963	The package Snyk CLI before 1.1294.0 is vulnerable to Code Injection when scanning an untrusted PHP project. The vulnerability can be triggered if Snyk test is run inside the untrusted project due to the improper handling of the current working directory name. Snyk recommends only scanning trusted projects.	7.5	More Details
CVE-2024-44289	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to read sensitive location information.	7.5	More Details
CVE-2024-7783	mintplex-labs/anything-llm version latest contains a vulnerability where sensitive information, specifically a password, is improperly stored within a JWT (JSON Web Token) used as a bearer token in single user mode. When decoded, the JWT reveals the password in plaintext. This improper storage of sensitive information poses significant security risks, as an attacker who gains access to the JWT can easily decode it and retrieve the password. The issue is fixed in version 1.0.3.	7.5	More Details
CVE-2024-50434	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Theme Horse NewsCard.This issue affects NewsCard: from n/a through 1.3.	7.5	More Details
CVE-2024-7985	The FileOrganizer – Manage WordPress and Website Files plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the "fileorganizer_ajax_handler" function in all versions up to, and including, 1.0.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, and permissions granted by an administrator, to upload arbitrary files on the affected site's server which may make remote code execution possible. NOTE: The FileOrganizer Pro plugin must be installed and active to allow Subscriber+ users to upload files.	7.5	More Details
CVE-2020-26305	CommonRegexJS is a CommonRegex port for JavaScript. All available versions contain one or more regular expressions that are vulnerable to Regular Expression Denial of Service (ReDoS). As of time of publication, no known patches are available.	7.5	More Details
CVE-2024-49701	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Theme Horse Mags.This issue affects Mags: from n/a through 1.1.6.	7.5	More Details
CVE-2024-50453	Relative Path Traversal vulnerability in Webangon The Pack Elementor addons allows PHP Local File Inclusion.This issue affects The Pack Elementor addons: from n/a through 2.0.9.	7.5	More Details
CVE-2020-26304	Foundation is a front-end framework. Versions 6.3.3 and prior contain one or more regular expressions that are vulnerable to Regular Expression Denial of Service (ReDoS). As of time of publication, it is unknown if any fixes are available.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49690	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Qode Interactive Qi Blocks.This issue affects Qi Blocks: from n/a through 1.3.2.	7.5	More Details
CVE-2020-26303	insane is a whitelist-oriented HTML sanitizer. Versions 2.6.2 and prior contain one or more regular expressions that are vulnerable to Regular Expression Denial of Service (ReDoS). As of time of publication, no known patches are available.	7.5	More Details
CVE-2019-25219	Asio C++ Library before 1.13.0 lacks a fallback error code in the case of SSL_ERROR_SYSCALL with no associated error information from the SSL library being used.	7.5	More Details
CVE-2024-8924	ServiceNow has addressed a blind SQL injection vulnerability that was identified in the Now Platform. This vulnerability could enable an unauthenticated user to extract unauthorized information. ServiceNow deployed an update to hosted instances, and ServiceNow provided the update to our partners and self-hosted customers. Further, the vulnerability is addressed in the listed patches and hot fixes.	7.5	More Details
CVE-2024-10402	The Forminator Forms – Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on a function in all versions up to, and including, 1.35.1. This makes it possible for authenticated attackers, with Contributor-level access and above, and permissions granted by an Administrator, to create new or edit existing forms, including updating the default registration role to Administrator on User Registration forms.	7.5	More Details
CVE-2024-10295	A flaw was found in Gateway. Sending a non-base64 'basic' auth with special characters can cause APICast to incorrectly authenticate a request. A malformed basic authentication header containing special characters bypasses authentication and allows unauthorized access to the backend. This issue can occur due to a failure in the base64 decoding process, which causes APICast to skip the rest of the authentication checks and proceed with routing the request upstream.	7.5	More Details
CVE-2024-50441	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CozyThemes Cozy Blocks allows Stored XSS.This issue affects Cozy Blocks: from n/a through 2.0.15.	7.4	More Details
CVE-2024-47549	Sharp and Toshiba Tec MFPs improperly process query parameters in HTTP requests, which may allow contamination of unintended data to HTTP response headers. Accessing a crafted URL which points to an affected product may cause malicious script executed on the web browser.	7.4	More Details
CVE-2024-47801	Sharp and Toshiba Tec MFPs improperly process query parameters in HTTP requests, resulting in a reflected cross-site scripting vulnerability. Accessing a crafted URL which points to an affected product may cause malicious script executed on the web browser.	7.4	More Details
CVE-2024-47031	Android before 2024-10-05 on Google Pixel devices allows privilege escalation in the ABL component, A-329163861.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6245	Use of Default Credentials vulnerability in Maruti Suzuki SmartPlay on Linux (Infotainment Hub modules) allows attacker to try common or default usernames and passwords.The issue was detected on a 2022 Maruti Suzuki Brezza in India Market. This issue affects SmartPlay: 66T0.05.50.	7.4	More Details
CVE-2024-44098	In lwis_device_event_states_clear_locked of lwis_event.c, there is a possible privilege escalation due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.4	More Details
CVE-2024-10432	A vulnerability has been found in Project Worlds Simple Web-Based Chat Application 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10430	A vulnerability, which was classified as critical, has been found in Codezips Pet Shop Management System 1.0. This issue affects some unknown processing of the file /animalsupdate.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10336	A vulnerability was found in SourceCodeHero Clothes Recommendation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/index.php of the component Admin Login Page. The manipulation of the argument t1 leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10449	A vulnerability, which was classified as critical, was found in Codezips Hospital Appointment System 1.0. This affects an unknown part of the file /loginAction.php. The manipulation of the argument Username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10335	A vulnerability was found in SourceCodester Garbage Collection Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file login.php. The manipulation of the argument username/password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "username" to be affected. But it must be assumed that the parameter "password" is affected as well.	7.3	More Details
CVE-2024-48459	A command execution vulnerability exists in the AX2 Pro home router produced by Shenzhen Tenda Technology Co., Ltd. (Jixiang Tenda) v.DI_7003G-19.12.24A1V16.03.29.50;V16.03.29.50;V16.03.29.50. An attacker can exploit this vulnerability by constructing a malicious payload to execute commands and further obtain shell access to the router's file system with the highest privileges.	7.3	More Details
CVE-2024-10431	A vulnerability, which was classified as critical, was found in Codezips Pet Shop Management System 1.0. Affected is an unknown function of the file /deletebird.php. The manipulation of the argument t1 leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10368	A vulnerability was found in Codezips Sales Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /addstock.php. The manipulation of the argument prodtype leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-50450	Improper Control of Generation of Code ('Code Injection') vulnerability in realmag777 WordPress Meta Data and Taxonomies Filter (MDTF) allows Code Injection.This issue affects WordPress Meta Data and Taxonomies Filter (MDTF): from n/a through 1.3.3.4.	7.3	More Details
CVE-2024-9772	The The Uix Shortcodes – Compatible with Gutenberg plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.9.9. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-10369	A vulnerability was found in Codezips Sales Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /addcustcom.php. The manipulation of the argument refno leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10370	A vulnerability was found in Codezips Sales Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /addcustind.php. The manipulation of the argument refno leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-8392	The WordPress Post Grid Layouts with Pagination – Sogrid plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 1.5.2 via the 'tab' parameter. This makes it possible for authenticated attackers, with Administrator-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included. This can also be exploited via CSRF techniques.	7.2	More Details
CVE-2024-10429	A vulnerability classified as critical has been found in WAVLINK WN530H4, WN530HG4 and WN572HG3 up to 20221028. Affected is the function set_ipv6 of the file internet.cgi. The manipulation of the argument IPv6OpMode/IPv6IPAddr/IPv6WANIPAddr/IPv6GWAddr leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-48226	Funadmin 5.0.2 is vulnerable to SQL Injection in curd/table/savefield.	7.2	More Details
CVE-2024-48229	funadmin 5.0.2 has a SQL injection vulnerability in the Curd one click command mode plugin.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48230	funadmin 5.0.2 is vulnerable to SQL Injection via the parentField parameter in the index method of \backend\controller\auth\Auth.php.	7.2	More Details
CVE-2024-48454	An issue in SourceCodester Purchase Order Management System v1.0 allows a remote attacker to execute arbitrary code via the /admin?page=user component	7.2	More Details
CVE-2024-9162	The All-in-One WP Migration and Backup plugin for WordPress is vulnerable to arbitrary PHP Code Injection due to missing file type validation during the export in all versions up to, and including, 7.86. This makes it possible for authenticated attackers, with Administrator-level access and above, to create an export file with the .php extension on the affected site's server, adding an arbitrary PHP code to it, which may make remote code execution possible.	7.2	More Details
CVE-2024-48218	Funadmin v5.0.2 has a SQL injection vulnerability in /curd/table/list.	7.2	More Details
CVE-2024-10428	A vulnerability was found in WAVLINK WN530H4, WN530HG4 and WN572HG3 up to 20221028. It has been rated as critical. This issue affects the function set_ipv6 of the file firewall.cgi. The manipulation of the argument dhcpGateway leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.2	More Details
CVE-2024-49684	Deserialization of Untrusted Data vulnerability in Revmakx Backup and Staging by WP Time Capsule allows Object Injection.This issue affects Backup and Staging by WP Time Capsule: from n/a through 1.22.21.	7.2	More Details
CVE-2024-48700	Kliqqi-CMS has a background arbitrary code execution vulnerability that attackers can exploit to implant backdoors or getShell via the edit_page.php component.	7.2	More Details
CVE-2024-37845	MangoOS before 5.2.0 was discovered to contain an authenticated remote code execution (RCE) vulnerability via the Active Process Command feature.	7.2	More Details
CVE-2024-9927	The WooCommerce Order Proposal plugin for WordPress is vulnerable to privilege escalation via order proposal in all versions up to and including 2.0.5. This is due to the improper implementation of allow_payment_without_login function. This makes it possible for authenticated attackers, with Shop Manager-level access and above, to log in to WordPress as an arbitrary user account, including administrators.	7.2	More Details
CVE-2024-48223	Funadmin v5.0.2 has a SQL injection vulnerability in /curd/table/fieldlist.	7.2	More Details
CVE-2024-48222	Funadmin v5.0.2 has a SQL injection vulnerability in /curd/table/edit.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47902	A vulnerability has been identified in InterMesh 7177 Hybrid 2.0 Subscriber (All versions < V8.2.12), InterMesh 7707 Fire Subscriber (All versions < V7.2.12 only if the IP interface is enabled (which is not the default configuration)). The web server of affected devices does not authenticate GET requests that execute specific commands (such as `ping`) on operating system level.	7.2	More Details
CVE-2024-41153	Command injection vulnerability in the Edge Computing UI for the TRO600 series radios that allows for the execution of arbitrary system commands. If exploited, an attacker with write access to the web UI can execute commands on the device with root privileges, far more extensive than what the write privilege intends.	7.2	More Details
CVE-2024-50611	CycloneDX cdxgen through 10.10.7, when run against an untrusted codebase, may execute code contained within build-related files such as build.gradle.kts, a similar issue to CVE-2022-24441. cdxgen is used by, for example, OWASP dep-scan. NOTE: this has been characterized as a design limitation, rather than an implementation mistake.	7.2	More Details
CVE-2024-49672	Cross-Site Request Forgery (CSRF) vulnerability in Gifford Cheung, Brian Watanabe, Chongsun Ahn Google Docs RSVP allows Stored XSS.This issue affects Google Docs RSVP: from n/a through 2.0.1.	7.1	More Details
CVE-2024-47640	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in weDevs WP ERP allows Reflected XSS.This issue affects WP ERP: from n/a through 1.13.2.	7.1	More Details
CVE-2024-49673	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Van Abel LaTeX2HTML allows Reflected XSS.This issue affects LaTeX2HTML: from n/a through 2.5.4.	7.1	More Details
CVE-2024-44252	A logic issue was addressed with improved file handling. This issue is fixed in iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, visionOS 2.1, tvOS 18.1. Restoring a maliciously crafted backup file may lead to modification of protected system files.	7.1	More Details
CVE-2024-44159	A path deletion vulnerability was addressed by preventing vulnerable code from running with privileges. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to bypass Privacy preferences.	7.1	More Details
CVE-2024-49634	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Rimon Habib BP Member Type Manager allows Reflected XSS.This issue affects BP Member Type Manager: from n/a through 1.01.	7.1	More Details
CVE-2024-49663	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Elena Zhyvohliad uCAT – Next Story allows Reflected XSS.This issue affects uCAT – Next Story: from n/a through 2.0.0.	7.1	More Details
CVE-2024-44156	A path deletion vulnerability was addressed by preventing vulnerable code from running with privileges. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to bypass Privacy preferences.	7.1	More Details
CVE-2024-49646	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ioannup Code Generate allows Reflected XSS.This issue affects Code Generate: from n/a through 1.0.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49664	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in allows Reflected XSS.This issue affects chatplusjp: from n/a through 1.02.	7.1	More Details
CVE-2024-49643	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Abdullah Irfan Whitelist allows Reflected XSS.This issue affects Whitelist: from n/a through 3.5.	7.1	More Details
CVE-2024-49642	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Rafasashi Todo Custom Field allows Reflected XSS.This issue affects Todo Custom Field: from n/a through 3.0.4.	7.1	More Details
CVE-2024-49760	OpenRefine is a free, open source tool for working with messy data. The load-language command expects a `lang` parameter from which it constructs the path of the localization file to load, of the form `translations-$LANG.json`. But when doing so in versions prior to 3.8.3, it does not check that the resulting path is in the expected directory, which means that this command could be exploited to read other JSON files on the file system. Version 3.8.3 addresses this issue.	7.1	More Details
CVE-2024-49654	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Marian Heddesheimer Extra Privacy for Elementor allows Reflected XSS.This issue affects Extra Privacy for Elementor: from n/a through 0.1.3.	7.1	More Details
CVE-2024-49656	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Abdullah Irfan DocumentPress allows Reflected XSS.This issue affects DocumentPress: from n/a through 2.1.	7.1	More Details
CVE-2024-49645	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ilias Gomatos Affiliate Platform allows Reflected XSS.This issue affects Affiliate Platform: from n/a through 1.4.8.	7.1	More Details
CVE-2024-49650	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in xarbo BuddyPress Greeting Message allows Reflected XSS.This issue affects BuddyPress Greeting Message: from n/a through 1.0.3.	7.1	More Details
CVE-2024-49632	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Coral Web Design CWD 3D Image Gallery allows Reflected XSS.This issue affects CWD 3D Image Gallery: from n/a through 1.0.	7.1	More Details
CVE-2024-6674	A CORS misconfiguration in parisneo/lollms-webui prior to version 10 allows attackers to steal sensitive information such as logs, browser sessions, and settings containing private API keys from other services. This vulnerability can also enable attackers to perform actions on behalf of a user, such as deleting a project or sending a message. The issue impacts the confidentiality and integrity of the information.	7.1	More Details
CVE-2024-50448	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in YITH YITH WooCommerce Product Add-Ons allows Reflected XSS.This issue affects YITH WooCommerce Product Add-Ons: from n/a through 4.14.1.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49641	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tidaweb Tida URL Screenshot allows Reflected XSS.This issue affects Tida URL Screenshot: from n/a through 1.0.	7.1	More Details
CVE-2024-49640	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AmaderCode Lab ACL Floating Cart for WooCommerce allows Reflected XSS.This issue affects ACL Floating Cart for WooCommerce: from n/a through 0.9.	7.1	More Details
CVE-2024-49639	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Edward Stoever Monitor.Chat allows Reflected XSS.This issue affects Monitor.Chat: from n/a through 1.1.1.	7.1	More Details
CVE-2024-49678	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jinwen js allows Reflected XSS.This issue affects js paper: from n/a through 2.5.7.	7.1	More Details
CVE-2024-49638	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ali Azlan Risk Warning Bar allows Reflected XSS.This issue affects Risk Warning Bar: from n/a through 1.0.	7.1	More Details
CVE-2024-49637	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Foxskav Bet WC 2018 Russia allows Reflected XSS.This issue affects Bet WC 2018 Russia: from n/a through 2.1.	7.1	More Details
CVE-2024-50407	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kiboko Labs Namaste! LMS allows Reflected XSS.This issue affects Namaste! LMS: from n/a through 2.6.2.	7.1	More Details
CVE-2024-50438	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Andy Moyle Church Admin allows Reflected XSS.This issue affects Church Admin: from n/a before 5.0.0.	7.1	More Details
CVE-2024-44258	This issue was addressed with improved handling of symlinks. This issue is fixed in iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, visionOS 2.1, tvOS 18.1. Restoring a maliciously crafted backup file may lead to modification of protected system files.	7.1	More Details
CVE-2024-49670	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Sam Glover Client Power Tools Portal allows Reflected XSS.This issue affects Client Power Tools Portal: from n/a through 1.8.6.	7.1	More Details
CVE-2024-0128	NVIDIA vGPU software contains a vulnerability in the Virtual GPU Manager that allows a user of the guest OS to access global resources. A successful exploit of this vulnerability might lead to information disclosure, data tampering, and escalation of privileges.	7.1	More Details
CVE-2024-49648	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in rafasashi SVG Captcha allows Reflected XSS.This issue affects SVG Captcha: from n/a through 1.0.11.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49636	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Prashant Mavinkurve Agile Video Player Lite allows Reflected XSS.This issue affects Agile Video Player Lite: from n/a through 1.0.	7.1	More Details
CVE-2024-49660	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Campus Explorer Campus Explorer Widget allows Reflected XSS.This issue affects Campus Explorer Widget: from n/a through 1.4.	7.1	More Details
CVE-2024-49635	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Manzurul Haque Banner Slider allows Reflected XSS.This issue affects Banner Slider: from n/a through 2.1.	7.1	More Details
CVE-2024-46998	baserCMS is a website development framework. Versions prior to 5.1.2 have a cross-site scripting vulnerability in the Edit Email Form Settings Feature. Version 5.1.2 fixes the issue.	7.1	More Details
CVE-2024-49661	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Lew Ayotte leenk.Me allows Reflected XSS.This issue affects leenk.Me: from n/a through 2.16.0.	7.1	More Details
CVE-2024-49662	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Webgensis Simple Load More allows Reflected XSS.This issue affects Simple Load More: from n/a through 1.0.	7.1	More Details
CVE-2024-49647	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Carl Alberto Simple Custom Admin allows Reflected XSS.This issue affects Simple Custom Admin: from n/a through 1.2.	7.1	More Details
CVE-2024-49651	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Matt Royal WooCommerce Maintenance Mode allows Reflected XSS.This issue affects WooCommerce Maintenance Mode: from n/a through 2.0.1.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50066	In the Linux kernel, the following vulnerability has been resolved: mm/mremap: fix move_normal_pmd/retract_page_tables race In mremap(), move_page_tables() looks at the type of the PMD entry and the specified address range to figure out by which method the next chunk of page table entries should be moved. At that point, the mmap_lock is held in write mode, but no rmap locks are held yet. For PMD entries that point to page tables and are fully covered by the source address range, move_pgt_entry(NORMAL_PMD, ...) is called, which first takes rmap locks, then does move_normal_pmd(). move_normal_pmd() takes the necessary page table locks at source and destination, then moves an entire page table from the source to the destination. The problem is: The rmap locks, which protect against concurrent page table removal by retract_page_tables() in the THP code, are only taken after the PMD entry has been read and it has been decided how to move it. So we can race as follows (with two processes that have mappings of the same tmpfs file that is stored on a tmpfs mount with huge=advise); note that process A accesses page tables through the MM while process B does it through the file rmap: process A process B ========= ========= mremap mremap_to move_vma move_page_tables get_old_pmd alloc_new_pmd *** PREEMPT *** madvise(MADV_COLLAPSE) do_madvise madvise_walk_vmas madvise_vma_behavior madvise_collapse hpage_collapse_scan_file collapse_file retract_page_tables i_mmap_lock_read(mapping) pmdp_collapse_flush i_mmap_unlock_read(mapping) move_pgt_entry(NORMAL_PMD, ...) take_rmap_locks move_normal_pmd drop_rmap_locks When this happens, move_normal_pmd() can end up creating bogus PMD entries in the line `pmd_populate(mm, new_pmd, pmd_pgtable(pmd))`. The effect depends on arch-specific and machine-specific details; on x86, you can end up with physical page 0 mapped as a page table, which is likely exploitable for user->kernel privilege escalation. Fix the race by letting process B recheck that the PMD still points to a page table after the rmap locks have been taken. Otherwise, we bail and let the caller fall back to the PTE-level copying path, which will then bail immediately at the pmd_none() check. Bug reachability: Reaching this bug requires that you can create shmem/file THP mappings - anonymous THP uses different code that doesn't zap stuff under rmap locks. File THP is gated on an experimental config flag (CONFIG_READ_ONLY_THP_FOR_FS), so on normal distro kernels you need shmem THP to hit this bug. As far as I know, getting shmem THP normally requires that you can mount your own tmpfs with the right mount flags, which would require creating your own user+mount namespace; though I don't know if some distros maybe enable shmem THP by default or something like that. Bug impact: This issue can likely be used for user->kernel privilege escalation when it is reachable.	7.0	More Details
CVE-2024-50086	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix user-after-free from session log off There is racy issue between smb2 session log off and smb2 session setup. It will cause user-after-free from session log off. This add session_lock when setting SMB2_SESSION_EXPIRED and referece count to session struct not to free session while it is being used.	7.0	More Details
CVE-2024-44141	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.6. A person with physical access to an unlocked Mac may be able to gain root code execution.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20331	A vulnerability in the session authentication functionality of the Remote Access SSL VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to prevent users from authenticating. This vulnerability is due to insufficient entropy in the authentication process. An attacker could exploit this vulnerability by determining the handle of an authenticating user and using it to terminate their authentication session. A successful exploit could allow the attacker to force a user to restart the authentication process, preventing a legitimate user from establishing remote access VPN sessions.	6.8	More Details
CVE-2024-22065	There is a command injection vulnerability in ZTE MF258 Pro product. Due to insufficient validation of Ping Diagnosis interface parameter, an authenticated attacker could use the vulnerability to execute arbitrary commands.	6.8	More Details
CVE-2024-49676	Unrestricted Upload of File with Dangerous Type vulnerability in Michael Bourne Custom Icons for Elementor allows Upload a Web Shell to a Web Server.This issue affects Custom Icons for Elementor: from n/a through 0.3.3.	6.6	More Details
CVE-2024-50470	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themes4WP Themes4WP YouTube External Subtitles allows Stored XSS.This issue affects Themes4WP YouTube External Subtitles: from n/a through 1.0.	6.5	More Details
CVE-2024-50471	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Checklist Trip Plan allows Stored XSS.This issue affects Trip Plan: from n/a through 1.0.10.	6.5	More Details
CVE-2024-48225	Funadmin v5.0.2 has an arbitrary file deletion vulnerability in /curd/index/delfile.	6.5	More Details
CVE-2024-50501	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Climax Themes Kata Plus allows Stored XSS.This issue affects Kata Plus: from n/a through 1.4.7.	6.5	More Details
CVE-2024-49692	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AffiliateX allows Stored XSS.This issue affects AffiliateX: from n/a through 1.2.9.	6.5	More Details
CVE-2024-50472	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Martin Drapeau Amilia Store allows Stored XSS.This issue affects Amilia Store: from n/a through 2.9.8.	6.5	More Details
CVE-2024-50615	TinyXML2 through 10.0.0 has a reachable assertion for UINT_MAX/digit, that may lead to application exit, in tinyxml2.cpp XMLUtil::GetCharacterRef.	6.5	More Details
CVE-2024-49659	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Rami Yushuvaev Coub allows Stored XSS.This issue affects Coub: from n/a through 1.4.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48450	An arbitrary file upload vulnerability in Huly Platform v0.6.295 allows attackers to execute arbitrary code via uploading a crafted HTML file into chat group.	6.5	More Details
CVE-2024-49667	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NervyThemes Local Business Addons For Elementor allows Stored XSS.This issue affects Local Business Addons For Elementor: from n/a through 1.1.5.	6.5	More Details
CVE-2024-50442	Improper Restriction of XML External Entity Reference vulnerability in WP Royal Royal Elementor Addons allows XML Injection.This issue affects Royal Elementor Addons: from n/a through 1.3.980.	6.5	More Details
CVE-2024-48235	An issue in ofcms 1.1.2 allows a remote attacker to execute arbitrary code via the save method of the TemplateController.java file.	6.5	More Details
CVE-2024-48236	An issue in ofcms 1.1.2 allows a remote attacker to execute arbitrary code via the FileOutputStream function in the write String method of the ofcms-admin\src\main\java\com\ofsoft\cms\core\uitle\FileUtils.java file	6.5	More Details
CVE-2024-49665	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Web Bricks Web Bricks Addons for Elementor allows Stored XSS.This issue affects Web Bricks Addons for Elementor: from n/a through 1.1.1.	6.5	More Details
CVE-2024-50410	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kiboko Labs Namaste! LMS allows Stored XSS.This issue affects Namaste! LMS: from n/a through 2.6.4.	6.5	More Details
CVE-2024-50409	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kiboko Labs Namaste! LMS allows Stored XSS.This issue affects Namaste! LMS: from n/a through 2.6.2.	6.5	More Details
CVE-2024-50613	libsndfile through 1.2.2 has a reachable assertion, that may lead to application exit, in mpeg_l3_encode.c mpeg_l3_encoder_close.	6.5	More Details
CVE-2024-48743	Cross Site Scripting vulnerability in Sentry v.6.0.9 allows a remote attacker to execute arbitrary code via the z parameter.	6.5	More Details
CVE-2024-50458	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Codeus Advanced Sermons allows Stored XSS.This issue affects Advanced Sermons: from n/a through 3.4.	6.5	More Details
CVE-2024-49703	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MagePeople Team Event Manager for WooCommerce allows Stored XSS.This issue affects Event Manager for WooCommerce: from n/a through 4.2.5.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49693	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kraftplugins Mega Elements allows Stored XSS.This issue affects Mega Elements: from n/a through 1.2.6.	6.5	More Details
CVE-2024-49695	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Spiffy Plugins WP Flow Plus allows Stored XSS.This issue affects WP Flow Plus: from n/a through 5.2.3.	6.5	More Details
CVE-2024-50437	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AyeCode GeoDirectory allows Stored XSS.This issue affects GeoDirectory: from n/a through 2.3.80.	6.5	More Details
CVE-2024-49702	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in myCRED myCred Elementor allows Stored XSS.This issue affects myCred Elementor: from n/a through 1.2.6.	6.5	More Details
CVE-2024-50433	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in wowDevs Sky Addons for Elementor allows Stored XSS.This issue affects Sky Addons for Elementor: from n/a through 2.5.15.	6.5	More Details
CVE-2024-50432	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PickPlugins Post Grid and Gutenberg Blocks allows Stored XSS.This issue affects Post Grid and Gutenberg Blocks: from n/a through 2.2.93.	6.5	More Details
CVE-2024-50429	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPBlockArt Magazine Blocks allows Stored XSS.This issue affects Magazine Blocks: from n/a through 1.3.15.	6.5	More Details
CVE-2024-50469	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Team Bright Vessel Textboxes allows DOM-Based XSS.This issue affects Textboxes: from n/a through 0.1.3.1.	6.5	More Details
CVE-2024-7473	An IDOR vulnerability exists in the 'Evaluations' function of the 'umgws datasets' section in lunary-ai/lunary versions 1.3.2. This vulnerability allows an authenticated user to update other users' prompts by manipulating the 'id' parameter in the request. The issue is fixed in version 1.4.3.	6.5	More Details
CVE-2024-50468	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Michael Robinson Raptor Editor allows DOM-Based XSS.This issue affects Raptor Editor: from n/a through 1.0.20.	6.5	More Details
CVE-2024-50502	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CozyThemes Cozy Blocks allows Stored XSS.This issue affects Cozy Blocks: from n/a through 2.0.18.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7472	lunary-ai/lunary v1.2.26 contains an email injection vulnerability in the Send email verification API (/v1/users/send-verification) and Sign up API (/auth/signup). An unauthenticated attacker can inject data into outgoing emails by bypassing the extractFirstName function using a different whitespace character (e.g., \xa0). This vulnerability can be exploited to conduct phishing attacks, damage the application's brand, cause legal and compliance issues, and result in financial impact due to unauthorized email usage.	6.5	More Details
CVE-2024-50467	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WebXApp Scrollbar by webxapp – Best vertical/horizontal scrollbars plugin allows Stored XSS.This issue affects Scrollbar by webxapp – Best vertical/horizontal scrollbars plugin: from n/a through 1.3.0.	6.5	More Details
CVE-2024-50464	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pierre Lebedel Kodex Posts likes allows Stored XSS.This issue affects Kodex Posts likes: from n/a through 2.5.0.	6.5	More Details
CVE-2024-50462	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Fla-shop Interactive World Map allows Stored XSS.This issue affects Interactive World Map: from n/a through 3.4.4.	6.5	More Details
CVE-2024-45259	An issue was discovered on certain GL-iNet devices, including MT6000, MT3000, MT2500, AXT1800, and AX1800 4.6.2. By intercepting an HTTP request and changing the filename property in the download interface, any file on the device can be deleted.	6.5	More Details
CVE-2024-9650	The WP Recipe Maker plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘tooltip’ parameter in all versions up to, and including, 9.6.1 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.	6.5	More Details
CVE-2024-6826	An issue has been discovered in GitLab CE/EE affecting all versions from 11.2 before 17.3.6, 17.4 before 17.4.3, and 17.5 before 17.5.1. A denial of service could occur via importing a malicious crafted XML manifest file.	6.5	More Details
CVE-2024-40432	A lack of input validation in Realtek SD card reader driver before 10.0.26100.21374 through the implementation of the IOCTL_SFFDISK_DEVICE_COMMAND control of the SD card reader driver allows a privileged attacker to crash the OS.	6.5	More Details
CVE-2024-20340	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software, formerly Firepower Management Center Software, could allow an authenticated, remote attacker to perform an SQL injection attack against an affected device. To exploit this vulnerability, an attacker must have a valid account on the device with the role of Security Approver, Intrusion Admin, Access Admin, or Network Admin. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface of an affected device. A successful exploit could allow the attacker to read the contents of databases on the affected device and also obtain limited read access to the underlying operating system.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9829	The Download Plugin plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability checks on the 'dpwap_handle_download_user' and 'dpwap_handle_download_comment' functions in all versions up to, and including, 2.2.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to download any comment, and download metadata for any user including user PII and sensitive information including username, email, hashed passwords and application passwords, session token information and more depending on set up and additional plugins installed.	6.5	More Details
CVE-2024-48107	SparkShop <=1.1.7 is vulnerable to server-side request forgery (SSRF). This vulnerability allows attacks to scan ports on the Intranet or local network where the server resides, attack applications running on the Intranet or local network, or read metadata on the cloud server.	6.5	More Details
CVE-2024-44297	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. Processing a maliciously crafted message may lead to a denial-of-service.	6.5	More Details
CVE-2024-10280	A vulnerability was found in Tenda AC6, AC7, AC8, AC9, AC10, AC10U, AC15, AC18, AC500 and AC1206 up to 20241022. It has been rated as problematic. This issue affects the function websReadEvent of the file /goform/GetIPTV. The manipulation of the argument Content-Length leads to null pointer dereference. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.5	More Details
CVE-2024-50076	In the Linux kernel, the following vulnerability has been resolved: vt: prevent kernel-infoleak in con_font_get() font.data may not initialize all memory spaces depending on the implementation of vc->vc_sw->con_font_get. This may cause info-leak, so to prevent this, it is safest to modify it to initialize the allocated memory space to 0, and it generally does not affect the overall performance of the system.	6.5	More Details
CVE-2024-44294	A path deletion vulnerability was addressed by preventing vulnerable code from running with privileges. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An attacker with root privileges may be able to delete protected system files.	6.5	More Details
CVE-2024-5764	Use of Hard-coded Credentials vulnerability in Sonatype Nexus Repository has been discovered in the code responsible for encrypting any secrets stored in the Nexus Repository configuration database (SMTP or HTTP proxy credentials, user tokens, tokens, among others). The affected versions relied on a static hard-coded encryption passphrase. While it was possible for an administrator to define an alternate encryption passphrase, it could only be done at first boot and not updated. This issue affects Nexus Repository: from 3.0.0 through 3.72.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20374	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software, formerly Firepower Management Center Software, could allow an authenticated, remote attacker with Administrator-level privileges to execute arbitrary commands on the underlying operating system. This vulnerability is due to insufficient input validation of certain HTTP request parameters that are sent to the web-based management interface. An attacker could exploit this vulnerability by authenticating to the Cisco FMC web-based management interface and sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to execute commands as the root user on the affected device. To exploit this vulnerability, an attacker would need Administrator-level credentials.	6.5	More Details
CVE-2024-20482	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software, formerly Firepower Management Center Software, could allow an authenticated, remote attacker to elevate privileges on an affected device. To exploit this vulnerability, an attacker must have a valid account on the device that is configured with a custom read-only role. This vulnerability is due to insufficient validation of role permissions in part of the web-based management interface. An attacker could exploit this vulnerability by performing a write operation on the affected part of the web-based management interface. A successful exploit could allow the attacker to modify certain parts of the configuration.	6.5	More Details
CVE-2024-20379	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software, formerly Firepower Management Center Software, could allow an authenticated, remote attacker to read arbitrary files from the underlying operating system. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to read arbitrary files on the underlying operating system of the affected device. The attacker would need valid user credentials to exploit this vulnerability.	6.5	More Details
CVE-2024-44155	A custom URL scheme handling issue was addressed with improved input validation. This issue is fixed in Safari 18, iOS 17.7.1 and iPadOS 17.7.1, macOS Sequoia 15, watchOS 11, iOS 18 and iPadOS 18. Maliciously crafted web content may violate iframe sandboxing policy.	6.5	More Details
CVE-2024-50425	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Veribo, Roland Murg WP Booking System.This issue affects WP Booking System: from n/a through 2.0.19.10.	6.5	More Details
CVE-2024-50424	Missing Authorization vulnerability in Templately allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Templately: from n/a through 3.1.5.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20471	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface does not validate user input adequately. An attacker could exploit this vulnerability by authenticating to the application as an Administrator and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to obtain unauthorized data from the database and make changes to the system. To exploit this vulnerability, an attacker would need Administrator-level privileges.	6.5	More Details
CVE-2024-20472	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface does not validate user input adequately. An attacker could exploit this vulnerability by authenticating to the application as an Administrator and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to obtain unauthorized data from the database and make changes to the system. To exploit this vulnerability, an attacker would need Administrator-level privileges.	6.5	More Details
CVE-2024-20473	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface does not validate user input adequately. An attacker could exploit this vulnerability by authenticating to the application as an Administrator and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to obtain unauthorized data from the database and make changes to the system. To exploit this vulnerability, an attacker would need Administrator-level privileges.	6.5	More Details
CVE-2024-50461	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloper EmbedPress allows Stored XSS.This issue affects EmbedPress: from n/a through 4.0.14.	6.5	More Details
CVE-2024-48442	Incorrect access control in Shenzhen Tuoshi Network Communications Co.,Ltd 5G CPE Router NR500-EA RG500UEAABxCOMSLICv3.2.2543.12.18 allows attackers to access the SSH protocol without authentication.	6.5	More Details
CVE-2024-50451	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in realmag777 WordPress Meta Data and Taxonomies Filter (MDTF) allows Stored XSS.This issue affects WordPress Meta Data and Taxonomies Filter (MDTF): from n/a through 1.3.3.4.	6.5	More Details
CVE-2024-50445	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Merkulove Selection Lite allows Stored XSS.This issue affects Selection Lite: from n/a through 1.13.	6.5	More Details
CVE-2024-50443	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Post Grid Team by WPXPO PostX allows Stored XSS.This issue affects PostX: from n/a through 4.1.12.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10469	VINCE versions before 3.0.9 is vulnerable to exposure of User information to authenticated users.	6.5	More Details
CVE-2024-50418	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Time Slot Booking Time Slot allows Stored XSS.This issue affects Time Slot: from n/a through 1.3.6.	6.5	More Details
CVE-2024-10474	Focus was incorrectly allowing internal links to utilize the app scheme used for deeplinking, which could result in links potentially circumventing some URL safety checks This vulnerability affects Focus for iOS < 132.	6.5	More Details
CVE-2024-47481	Dell Data Lakehouse, version(s) 1.0.0.0, 1.1.0., contain(s) an Improper Access Control vulnerability. An unauthenticated attacker with adjacent network access could potentially exploit this vulnerability, leading to Denial of service.	6.5	More Details
CVE-2024-10341	The League of Legends Shortcodes plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 1.0.1 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.	6.5	More Details
CVE-2024-50439	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Brainstorm Force Astra Widgets allows Stored XSS.This issue affects Astra Widgets: from n/a through 1.2.14.	6.5	More Details
CVE-2024-10465	A clipboard "paste" button could persist across tabs which allowed a spoofing attack. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	6.5	More Details
CVE-2024-10464	Repeated writes to history interface attributes could have been used to cause a Denial of Service condition in the browser. This was addressed by introducing rate-limiting to this API. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	6.5	More Details
CVE-2024-50440	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Chris Coyier CodePen Embedded Pens Shortcode allows Stored XSS.This issue affects CodePen Embedded Pens Shortcode: from n/a through 1.0.2.	6.5	More Details
CVE-2024-50614	TinyXML2 through 10.0.0 has a reachable assertion for UINT_MAX/16, that may lead to application exit, in tinyxml2.cpp XMLUtil::GetCharacterRef.	6.5	More Details
CVE-2024-50447	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in EnvoThemes Envo's Elementor Templates & Widgets for WooCommerce allows Stored XSS.This issue affects Envo's Elementor Templates & Widgets for WooCommerce: from n/a through 1.4.19.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10462	Truncation of a long URL could have allowed origin spoofing in a permission prompt. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	6.5	More Details
CVE-2024-50449	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in RedefiningTheWeb PDF Generator Addon for Elementor Page Builder allows Stored XSS.This issue affects PDF Generator Addon for Elementor Page Builder: from n/a through 1.7.4.	6.5	More Details
CVE-2024-50446	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in FuturioWP Futurio Extra allows Stored XSS.This issue affects Futurio Extra: from n/a through 2.0.11.	6.5	More Details
CVE-2024-10463	Video frames could have been leaked between origins in some situations. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Firefox ESR < 115.17, Thunderbird < 128.4, and Thunderbird < 132.	6.5	More Details
CVE-2024-6673	A Cross-Site Request Forgery (CSRF) vulnerability exists in the `install_comfyui` endpoint of the `lollms_comfyui.py` file in the parisneo/lollms-webui repository, versions v9.9 to the latest. The endpoint uses the GET method without requiring a client ID, allowing an attacker to trick a victim into installing ComfyUI. If the victim's device does not have sufficient capacity, this can result in a crash.	6.5	More Details
CVE-2024-9505	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Button widget in all versions up to, and including, 2.8.4.2 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-10000	The Masteriyo LMS – eLearning and Online Course Builder for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the question's content parameter in all versions up to, and including, 1.13.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with student-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-2024-10266	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Video Box widget in all versions up to, and including, 4.10.60 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-10185	The StreamWeasels YouTube Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's sw-youtube-embed shortcode in all versions up to, and including, 1.3.2 due to insufficient input sanitization and output escaping on user supplied attributes. 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 Number	Description	Base Score	Reference
CVE-2024-9376	The Kata Plus – Addons for Elementor – Widgets, Extensions and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.4.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-10374	The WP-Members Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpmem_loginout shortcode in all versions up to, and including, 3.4.9.5 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-10227	The affiliate-toolkit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's atkp_product shortcode in all versions up to, and including, 3.6.5 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-10184	The StreamWeasels Kick Integration plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's sw-kick-embed shortcode in all versions up to, and including, 1.1.1 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-10226	The Arconix Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'box' shortcode in all versions up to, and including, 2.1.13 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-9585	The Image Map Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'save_project' function with an arbitrary shortcode in versions up to, and including, 6.0.20 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-2024-8666	The Shoutcast Icecast HTML5 Radio Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'html5radio' shortcode in all versions up to, and including, 2.1.6 due to insufficient input sanitization and output escaping on user supplied attributes. 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 Number	Description	Base Score	Reference
CVE-2024-10112	The Simple News plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'news' shortcode in all versions up to, and including, 2.8 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-10343	The Beek Widget Extention plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 0.9.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-10342	The League of Legends Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 1.0.1 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-2024-10233	The SMS Alert Order Notifications – WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's sa_subscribe shortcode in all versions up to, and including, 3.7.5 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-9454	The PriPre plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 0.4.11 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-10091	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Image Comparison Widget in all versions up to, and including, 3.2.9 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-9642	The Editor Custom Color Palette plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 3.3.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-9853	The ID-SK Toolkit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.7.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9967	The WP show more plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's show_more shortcode in all versions up to, and including, 1.0.7 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-9116	The Monkee-Boy Essentials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-10117	The WP Crowdfunding plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpcf_donate shortcode in all versions up to, and including, 2.1.11 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-10148	The Awesome buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's btn2 shortcode in all 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 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-2024-10150	The Bamazoo – Button Generator plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's dgs shortcode in all 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 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-2022-30360	OvalEdge 5.2.8.0 and earlier is affected by multiple Stored XSS (AKA Persistent or Type II) vulnerabilities via a POST request to /profile/updateProfile via the slackid or phone parameters. Authentication is required.	6.4	More Details
CVE-2024-10176	The Compact WP Audio Player plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's sc_embed_player shortcode in all versions up to, and including, 1.9.13 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-10181	The Newsletters plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's newsletters_video shortcode in all versions up to, and including, 4.9.9.4 due to insufficient input sanitization and output escaping on user supplied attributes. 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 Number	Description	Base Score	Reference
CVE-2024-10180	The Contact Form 7 – Repeatable Fields plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's field_group shortcode in all versions up to, and including, 2.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. 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-2024-8959	The WP Adminify – Custom WordPress Dashboard, Login and Admin Customizer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 4.0.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-10016	The File Upload Types by WPForms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.4.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-9456	The WP Awesome Login plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 0.4.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-10447	A vulnerability classified as critical was found in Project Worlds Online Time Table Generator 1.0. Affected by this vulnerability is an unknown functionality of the file /timetable/staff/staffdashboard.php?info=updateprofile. The manipulation of the argument n leads to sql injection. The attack can be launched remotely.	6.3	More Details
CVE-2024-48191	dingfanzu CMS 1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /admin/doAdminAction.php?act=delAdmin&id=17	6.3	More Details
CVE-2024-10450	A vulnerability has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /kortex_lite/control/edit_profile.php of the component POST Parameter Handler. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-48291	dingfanzu CMS 1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admin/doAdminAction.php?act=editAdmin&id=17	6.3	More Details
CVE-2024-10446	A vulnerability classified as critical has been found in Project Worlds Online Time Table Generator 1.0. Affected is an unknown function of the file /timetable/admin/admindashboard.php?info=add_course. The manipulation of the argument c leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10435	A vulnerability was found in didi Super-Jacoco 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /cov/triggerEnvCov. The manipulation of the argument uuid leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10416	A vulnerability was found in code-projects Blood Bank Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /file/cancel.php. The manipulation of the argument reqid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10353	A vulnerability classified as critical has been found in SourceCodester Online Exam System 1.0. Affected is an unknown function of the file /admin-dashboard. The manipulation leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This affects a different product and is a different issue than CVE-2024-40480.	6.3	More Details
CVE-2024-10376	A vulnerability was found in ESAFENET CDG 5. It has been declared as critical. This vulnerability affects the function actionPassOrNotAutoSign of the file /com/esafenet/servlet/service/processsign/AutoSignService.java. The manipulation of the argument UniqueId leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-10406	A vulnerability, which was classified as critical, has been found in SourceCodester Petrol Pump Management Software 1.0. Affected by this issue is some unknown functionality of the file /admin/edit_fuel.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10277	A vulnerability was found in ESAFENET CDG 5 and classified as critical. Affected by this issue is some unknown functionality of the file /com/esafenet/servlet/ajax/UsbKeyAjax.java. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-50583	Whale browser Installer before 3.1.0.0 allows an attacker to execute a malicious DLL in the user environment due to improper permission settings.	6.3	More Details
CVE-2024-10349	A vulnerability was found in SourceCodester Best House Rental Management System 1.0 and classified as critical. Affected by this issue is the function delete_tenant of the file /ajax.php?action=delete_tenant. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10291	A vulnerability has been found in ZZCMS 2023 and classified as critical. This vulnerability affects the function Ebak_DoExecSQL/Ebak_DotranExecutSQL of the file 3/Ebak5.1/upload/phome.php. The manipulation of the argument phome leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-50050	Llama Stack prior to revision 7a8aa775e5a267cf8660d83140011a0b7f91e005 used pickle as a serialization format for socket communication, potentially allowing for remote code execution. Socket communication has been changed to use JSON instead.	6.3	More Details
CVE-2024-9628	The WPS Telegram Chat plugin for WordPress is vulnerable to unauthorized modification of data and loss of data due to a missing capability check on the 'Wps_Telegram_Chat_Admin::checkConnection' function in versions up to, and including, 4.5.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to have full access to the Telegram Bot API endpoint and communicate with it.	6.3	More Details
CVE-2024-48343	A SQL Injection vulnerability in ESAFENET CDG 5 and earlier allows an attacker to execute arbitrary code via the id parameter of the dataSearch.jsp page.	6.3	More Details
CVE-2024-10331	A vulnerability, which was classified as critical, has been found in PHPGurukul Vehicle Record System 1.0. This issue affects some unknown processing of the file /admin/search-vehicle.php. The manipulation of the argument searchinputdata leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10377	A vulnerability was found in ESAFENET CDG 5. It has been rated as critical. This issue affects the function actionPassDecryptApplication1 of the file /com/esafenet/servlet/client/DecryptApplicationService.java. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This is a different issue than CVE-2024-10069. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-10278	A vulnerability was found in ESAFENET CDG 5. It has been classified as critical. This affects an unknown part of the file /com/esafenet/servlet/user/ReUserOrganiseService.java. The manipulation of the argument userId leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-46996	baserCMS is a website development framework. Versions prior to 5.1.2 have a cross-site scripting vulnerability in the Blog posts feature. Version 5.1.2 fixes this issue.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10279	A vulnerability was found in ESAFENET CDG 5. It has been declared as critical. This vulnerability affects unknown code of the file /com/esafenet/servlet/policy/PrintPolicyService.java. The manipulation of the argument policyId leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-9943	The MultiVendorX – The Ultimate WooCommerce Multivendor Marketplace Solution plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.2.4. This is due to missing or incorrect nonce validation on several functions in api/class-mvx-rest-controller.php. This makes it possible for unauthenticated attackers to update vendor account details, create vendor accounts, and delete arbitrary users via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.3	More Details
CVE-2024-10380	A vulnerability, which was classified as critical, has been found in SourceCodester Petrol Pump Management Software 1.0. Affected by this issue is some unknown functionality of the file /admin/ajax_product.php. The manipulation of the argument drop_services leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10378	A vulnerability classified as critical has been found in ESAFENET CDG 5. Affected is the function actionViewCDGRenewFile of the file /com/esafenet/servlet/client/CDGRenewApplicationService.java. The manipulation of the argument CDGRenewFileId leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-10407	A vulnerability, which was classified as critical, was found in SourceCodester Petrol Pump Management Software 1.0. This affects an unknown part of the file /admin/edit_customer.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10408	A vulnerability has been found in code-projects Blood Bank Management up to 1.0 and classified as critical. This vulnerability affects unknown code of the file /abs.php. The manipulation of the argument search leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10409	A vulnerability was found in code-projects Blood Bank Management 1.0 and classified as critical. This issue affects some unknown processing of the file /file/accept.php. The manipulation of the argument reqid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10410	A vulnerability classified as critical was found in SourceCodester Online Hotel Reservation System 1.0. Affected by this vulnerability is the function upload of the file /admin/mod_room/controller.php?action=add. The manipulation of the argument image leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10426	A vulnerability was found in Codezips Pet Shop Management System 1.0. It has been classified as critical. This affects an unknown part of the file /animalsadd.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions the parameter "refno" to be affected. But further inspection indicates that the name of the affected parameter is "id".	6.3	More Details
CVE-2024-10425	A vulnerability was found in Project Worlds Student Project Allocation System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /student/project_selection/move_up_project.php of the component Project Selection Page. The manipulation of the argument up leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10424	A vulnerability has been found in Project Worlds Student Project Allocation System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /student/project_selection/remove_project.php of the component Project Selection Page. The manipulation of the argument no leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10423	A vulnerability, which was classified as critical, was found in Project Worlds Student Project Allocation System 1.0. Affected is an unknown function of the file /student/project_selection/project_selection.php of the component Project Selection Page. The manipulation of the argument project_id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10371	A vulnerability classified as critical has been found in SourceCodester Payroll Management System 1.0. This affects the function login of the file main. The manipulation leads to buffer overflow. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10422	A vulnerability, which was classified as critical, has been found in SourceCodester Attendance and Payroll System 1.0. This issue affects some unknown processing of the file /admin/overtime_add.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10421	A vulnerability classified as critical was found in SourceCodester Attendance and Payroll System 1.0. This vulnerability affects unknown code of the file /admin/overtime_row.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10420	A vulnerability classified as critical has been found in SourceCodester Attendance and Payroll System 1.0. This affects the function upload of the file /marimar/guest/update.php. The manipulation of the argument image leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10293	A vulnerability was found in ZZCMS 2023. It has been classified as critical. Affected is the function Ebak_SetGotoPak of the file 3/Ebbak5.1/upload/class/functions.php. The manipulation of the argument file leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10418	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /file/infoAdd.php. The manipulation of the argument bg leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10417	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /file/delete.php. The manipulation of the argument bid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10415	A vulnerability has been found in code-projects Blood Bank Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /file/accept.php. The manipulation of the argument reqid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10413	A vulnerability, which was classified as critical, has been found in SourceCodester Online Hotel Reservation System 1.0. Affected by this issue is the function upload of the file /guest/update.php. The manipulation of the argument image leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10292	A vulnerability was found in ZZCMS 2023 and classified as critical. This issue affects some unknown processing of the file 3/Ebak5.1/upload/ChangeTable.php. The manipulation of the argument savefilename leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10411	A vulnerability was found in SourceCodester Online Hotel Reservation System 1.0. It has been classified as critical. Affected is the function doCancelRoom/doCancel/doConfirm/doCancel/doCheckin/doCheckout of the file /marimar/admin/mod_room/controller.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10427	A vulnerability was found in Codezips Pet Shop Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /deleteanimal.php. The manipulation of the argument t1 leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions the parameter "refno" to be affected. But further inspection indicates that the name of the affected parameter is "t1".	6.3	More Details
CVE-2024-48540	Incorrect access control in XIAO HE Smart 4.3.1 allows attackers to access sensitive information by analyzing the code and data within the APK file.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48870	Sharp and Toshiba Tec MFPs improperly validate input data in URI data registration, resulting in a stored cross-site scripting vulnerability. If crafted input is stored by an administrative user, malicious script may be executed on the web browsers of other victim users.	6.2	More Details
CVE-2024-48426	A segmentation fault (SEGV) was detected in the SortByPTypeProcess::Execute function in the Assimp library during fuzz testing with AddressSanitizer. The crash occurred due to a read access to an invalid memory address (0x1000c9714971).	6.2	More Details
CVE-2024-48195	Cross Site Scripting vulnerability in eyouCMS v.1.6.7 allows a remote attacker to obtain sensitive information via a crafted script to the post parameter.	6.1	More Details
CVE-2024-9214	The Extra Product Options Builder for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'RednaoSerializedFields' parameter during the creation of a signature file in all versions up to, and including, 1.2.133 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.1	More Details
CVE-2024-20275	A vulnerability in the cluster backup feature of Cisco Secure Firewall Management Center (FMC) Software, formerly Firepower Management Center Software, could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system. This vulnerability is due to insufficient validation of user data that is supplied through the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to execute arbitrary operating system commands on the affected device. To exploit this vulnerability, an attacker would need valid credentials for a user account with at least the role of Network Administrator. In addition, the attacker would need to persuade a legitimate user to initiate a cluster backup on the affected device.	6.1	More Details
CVE-2024-20341	A vulnerability in the VPN web client services feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a browser that is accessing an affected device. This vulnerability is due to improper validation of user-supplied input to application endpoints. An attacker could exploit this vulnerability by persuading a user to follow a link designed to submit malicious input to the affected application. A successful exploit could allow the attacker to execute arbitrary HTML or script code in the browser in the context of the web services page.	6.1	More Details
CVE-2024-20372	A vulnerability 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. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability 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.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51181	A Reflected Cross Site Scripting (XSS) vulnerability was found in /ifscfinder/admin/profile.php in PHPGurukul IFSC Code Finder Project v1.0, which allows remote attackers to execute arbitrary code via " searchifsccode" parameter.	6.1	More Details
CVE-2024-44145	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15, iOS 18 and iPadOS 18. An attacker with physical access to a macOS device with Sidecar enabled may be able to bypass the Lock Screen.	6.1	More Details
CVE-2024-20382	A vulnerability in the VPN web client services feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a browser that is accessing an affected device. This vulnerability is due to improper validation of user-supplied input to application endpoints. An attacker could exploit this vulnerability by persuading a user to follow a link designed to submit malicious input to the affected application. A successful exploit could allow the attacker to execute arbitrary HTML or script code in the browser in the context of the web services page.	6.1	More Details
CVE-2024-10250	The Nioland theme for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘s’ parameter in all versions up to, and including, 1.2.6 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-2024-25566	An Open-Redirect vulnerability exists in PingAM where well-crafted requests may cause improper validation of redirect URLs. This could allow an attacker to redirect end-users to malicious sites under their control, simplifying phishing attacks	6.1	More Details
CVE-2024-51180	A Reflected Cross Site Scripting (XSS) vulnerability was found in /ifscfinder/index.php in PHPGurukul IFSC Code Finder Project v1.0, which allows remote attackers to execute arbitrary code via the "searchifsccode" parameter.	6.1	More Details
CVE-2024-10289	Cross-Site Scripting (XSS) vulnerability affecting LocalServer 1.0.9 that could allow a remote user to send a specially crafted query to an authenticated user and steal their session details through /mlss/ManageSubscription, parameter MSubListName.	6.1	More Details
CVE-2024-51075	A Reflected Cross Site Scripting (XSS) vulnerability was found in /odms/admin/user-search.php in PHPGurukul Online DJ Booking Management System v1.0, which allows remote attackers to execute arbitrary code via the searchdata parameter.	6.1	More Details
CVE-2024-9374	The Terms descriptions plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.4.6. 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-2024-46995	baserCMS is a website development framework. Versions prior to 5.1.2 have a cross-site scripting vulnerability in HTTP 400 Bad Request. Version 5.1.2 fixes this issue.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9864	The EventPrime – Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via ticket names in all versions up to, and including, 4.0.4.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This is only exploitable when front-end users can submit new events with tickets.	6.1	More Details
CVE-2024-9865	The EventPrime – Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘ep_booking_attendee_fields’ fields in all versions up to, and including, 4.0.4.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses the transaction log for a booking.	6.1	More Details
CVE-2024-45031	When editing objects in the Syncope Console, incomplete HTML tags could be used to bypass HTML sanitization. This made it possible to inject stored XSS payloads which would trigger for other users during ordinary usage of the application. XSS payloads could also be injected in Syncope Enduser when editing “Personal Information” or “User Requests”: such payloads would trigger for administrators in Syncope Console, thus enabling session hijacking. Users are recommended to upgrade to version 3.0.9, which fixes this issue.	6.1	More Details
CVE-2024-10332	A Cross-Site Scripting vulnerability has been found in Janto v4.3r11 from Impronta. This vulnerability allows an attacker to execute JavaScript code in the victim's browser by sending the victim a malicious URL using the endpoint “/abonados/public/janto/main.php”.	6.1	More Details
CVE-2024-10048	The Post Status Notifier Lite and Premium plugins for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘page’ parameter in all versions up to, and including, 1.11.6 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-2024-42930	PbootCMS 3.2.8 is vulnerable to URL Redirect.	6.1	More Details
CVE-2024-51076	A Reflected Cross Site Scripting (XSS) vulnerability was found in /odms/admin/booking-search.php in PHPGurukul Online DJ Booking Management System 1.0, which allows remote attackers to execute arbitrary code via the "searchdata" parameter.	6.1	More Details
CVE-2024-8717	The PDF Flipbook, 3D Flipbook, PDF embed, PDF viewer – DearFlip plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'pdf_source' parameter in all versions up to, and including, 2.3.32 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 Number	Description	Base Score	Reference
CVE-2024-48396	AIML Chatbot 1.0 (fixed in 2.0) is vulnerable to Cross Site Scripting (XSS). The vulnerability is exploited through the message input field, where attackers can inject malicious HTML or JavaScript code. The chatbot fails to sanitize these inputs, leading to the execution of malicious scripts.	6.1	More Details
CVE-2024-10288	Cross-Site Scripting (XSS) vulnerability affecting LocalServer 1.0.9 that could allow a remote user to send a specially crafted query to an authenticated user and steal their session details through /mlss/SubscribeToList, parameter ListName.	6.1	More Details
CVE-2024-8870	The Forms for Mailchimp by Optin Cat – Grow Your MailChimp List plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.5.6. 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-2024-9613	The FormFacade – WordPress plugin for Google Forms plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'userId' and 'publishId' parameters in all versions up to, and including, 1.3.6 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-2024-48228	An issue was found in funadmin 5.0.2. The selectfiles method in \backend\controller\sys\Attachh.php directly stores the passed parameters and values into the param parameter without filtering, resulting in Cross Site Scripting (XSS).	6.1	More Details
CVE-2024-48448	An arbitrary file upload vulnerability in Huly Platform v0.6.295 allows attackers to execute arbitrary code via uploading a crafted HTML file into the tracker comments page.	6.1	More Details
CVE-2024-48654	Cross Site Scripting vulnerability in Blood Bank v.1 allows a remote attacker to execute arbitrary code via a crafted script to the login.php component.	6.1	More Details
CVE-2024-10286	Cross-Site Scripting (XSS) vulnerability affecting LocalServer 1.0.9 that could allow a remote user to send a specially crafted query to an authenticated user and steal their session details through /testmail/index.php, parameter to.	6.1	More Details
CVE-2024-10461	In multipart/x-mixed-replace responses, `Content-Disposition: attachment` in the response header was not respected and did not force a download, which could allow XSS attacks. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	6.1	More Details
CVE-2024-49378	smartUp, a web browser mouse gestures extension, has a universal cross-site scripting issue in the Edge and Firefox versions of smartUp 7.2.622.1170. The vulnerability allows another extension to execute arbitrary code in the context of the user's tab. As of time of publication, no known patches exist.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9438	The SEUR Oficial plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'change_service' parameter in all versions up to, and including, 2.2.11 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-2024-10287	Cross-Site Scripting (XSS) vulnerability affecting LocalServer 1.0.9 that could allow a remote user to send a specially crafted query to an authenticated user and steal their session details through /mlss/ForgotPassword, parameter ListName.	6.1	More Details
CVE-2024-20273	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability 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.	6.1	More Details
CVE-2024-9607	The 10Web Social Post Feed plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.2.9. 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. Please note this is only exploitable when the leave a review notice is present.	6.1	More Details
CVE-2024-20370	A vulnerability in the Cisco FXOS CLI feature on specific hardware platforms for Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to elevate their administrative privileges to root. The attacker would need valid administrative credentials on the device to exploit this vulnerability. This vulnerability exists because certain system configurations and executable files have insecure storage and permissions. An attacker could exploit this vulnerability by authenticating on the device and then performing a series of steps that includes downloading malicious system files and accessing the Cisco FXOS CLI to configure the attack. A successful exploit could allow the attacker to obtain root access on the device.	6.0	More Details
CVE-2024-20485	A vulnerability in the VPN web server of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an authenticated, local attacker to execute arbitrary code with root-level privileges. Administrator-level privileges are required to exploit this vulnerability. This vulnerability is due to improper validation of a specific file when it is read from system flash memory. An attacker could exploit this vulnerability by restoring a crafted backup file to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the affected device after the next reload of the device, which could alter system behavior. Because the injected code could persist across device reboots, Cisco has raised the Security Impact Rating (SIR) of this advisory from Medium to High.	6.0	More Details
CVE-2024-38314	IBM Maximo Application Suite - Monitor Component 8.10, 8.11, and 9.0 could disclose information in the form of the hard-coded cryptographic key to an attacker that has compromised environment.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49753	Zitadel is open-source identity infrastructure software. Versions prior to 2.64.1, 2.63.6, 2.62.8, 2.61.4, 2.60.4, 2.59.5, and 2.58.7 have a flaw in the URL validation mechanism of Zitadel actions allows bypassing restrictions intended to block requests to localhost (127.0.0.1). The isHostBlocked check, designed to prevent such requests, can be circumvented by creating a DNS record that resolves to 127.0.0.1. This enables actions to send requests to localhost despite the intended security measures. This vulnerability potentially allows unauthorized access to unsecured internal endpoints, which may contain sensitive information or functionalities. Versions 2.64.1, 2.63.6, 2.62.8, 2.61.4, 2.60.4, 2.59.5, and 2.58.7 contain a patch. No known workarounds are available.	5.9	More Details
CVE-2024-50624	ispdbservice.cpp in KDE Kmail before 6.2.0 allows man-in-the-middle attackers to trigger use of an attacker-controlled mail server because cleartext HTTP is used for a URL such as http://autoconfig.example.com or http://example.com/.well-known/autoconfig for retrieving the configuration. This is related to kmail-account-wizard.	5.9	More Details
CVE-2024-49679	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPKoi WPKoi Templates for Elementor allows Stored XSS.This issue affects WPKoi Templates for Elementor: from n/a through 3.1.0.	5.9	More Details
CVE-2024-50602	An issue was discovered in libexpat before 2.6.4. There is a crash within the XML_ResumeParser function because XML_StopParser can stop/suspend an unstarted parser.	5.9	More Details
CVE-2024-44213	An issue existed in the parsing of URLs. This issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An attacker in a privileged network position may be able to leak sensitive user information.	5.9	More Details
CVE-2024-50382	Botan before 3.6.0, when certain LLVM versions are used, has compiler-induced secret-dependent control flow in lib/utils/ghash/ghash.cpp in GHASH in AES-GCM. There is a branch instead of an XOR with carry. This was observed for Clang in LLVM 15 on RISC-V.	5.9	More Details
CVE-2024-50383	Botan before 3.6.0, when certain GCC versions are used, has a compiler-induced secret-dependent operation in lib/utils/donna128.h in donna128 (used in Chacha-Poly1305 and x25519). An addition can be skipped if a carry is not set. This was observed for GCC 11.3.0 with -O2 on MIPS, and GCC on x86-i386. (Only 32-bit processors can be affected.)	5.9	More Details
CVE-2024-7010	mudler/localai version 2.17.1 is vulnerable to a Timing Attack. This type of side-channel attack allows an attacker to compromise the cryptosystem by analyzing the time taken to execute cryptographic algorithms. Specifically, in the context of password handling, an attacker can determine valid login credentials based on the server's response time, potentially leading to unauthorized access.	5.9	More Details
CVE-2024-8036	ABB is aware of privately reported vulnerabilities in the product versions referenced in this CVE. An attacker could exploit these vulnerabilities by sending a specially crafted firmware or configuration to the system node, causing the node to stop, become inaccessible, or allowing the attacker to take control of the node.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50460	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in FirelightWP Firelight Lightbox allows Stored XSS.This issue affects Firelight Lightbox: from n/a through 2.3.3.	5.9	More Details
CVE-2024-47882	OpenRefine is a free, open source tool for working with messy data. Prior to version 3.8.3, the built-in "Something went wrong!" error page includes the exception message and exception traceback without escaping HTML tags, enabling injection into the page if an attacker can reliably produce an error with an attacker-influenced message. It appears that the only way to reach this code in OpenRefine itself is for an attacker to somehow convince a victim to import a malicious file, which may be difficult. However, out-of-tree extensions may add their own calls to `respondWithErrorPage`. Version 3.8.3 has a fix for this issue.	5.9	More Details
CVE-2024-50411	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Kevon Adonis WP Abstracts allows Stored XSS.This issue affects WP Abstracts: from n/a through 2.7.1.	5.9	More Details
CVE-2024-50413	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in codection Import and export users and customers allows Stored XSS.This issue affects Import and export users and customers: from n/a through 1.27.5.	5.9	More Details
CVE-2024-49696	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in RoboSoft Robo Gallery allows Stored XSS.This issue affects Robo Gallery: from n/a through 3.2.21.	5.9	More Details
CVE-2024-50412	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jules Colle Conditional Fields for Contact Form 7 allows Stored XSS.This issue affects Conditional Fields for Contact Form 7: from n/a through 2.4.15.	5.9	More Details
CVE-2024-50426	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Survey Maker team Survey Maker allows Stored XSS.This issue affects Survey Maker: from n/a through 5.0.2.	5.9	More Details
CVE-2024-50431	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Cloudways Breeze allows Stored XSS.This issue affects Breeze: from n/a through 2.1.14.	5.9	More Details
CVE-2024-50414	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in VirusTran Button contact VR allows Stored XSS.This issue affects Button contact VR: from n/a through 4.7.9.1.	5.9	More Details
CVE-2024-50415	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pagup Ads.Txt & App-ads.Txt Manager for WordPress allows Stored XSS.This issue affects Ads.Txt & App-ads.Txt Manager for WordPress: from n/a through 1.1.7.1.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20297	A vulnerability in the AnyConnect firewall for 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 have been denied to flow through an affected device. This vulnerability is due to a logic error in populating group ACLs when an AnyConnect client establishes a new session toward an affected device. An attacker could exploit this vulnerability by establishing an AnyConnect connection to the affected device. A successful exploit could allow the attacker to bypass configured ACL rules.	5.8	More Details
CVE-2024-47903	A vulnerability has been identified in InterMesh 7177 Hybrid 2.0 Subscriber (All versions < V8.2.12), InterMesh 7707 Fire Subscriber (All versions < V7.2.12 only if the IP interface is enabled (which is not the default configuration)). The web server of affected devices allows to write arbitrary files to the web server's DocumentRoot directory.	5.8	More Details
CVE-2024-20299	A vulnerability in the AnyConnect firewall for 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 have been denied to flow through an affected device. This vulnerability is due to a logic error in populating group ACLs when an AnyConnect client establishes a new session toward an affected device. An attacker could exploit this vulnerability by establishing an AnyConnect connection to the affected device. A successful exploit could allow the attacker to bypass configured ACL rules.	5.8	More Details
CVE-2024-20384	A vulnerability in the Network Service Group (NSG) 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. This vulnerability is due to a logic error that occurs when NSG ACLs are populated on an affected device. An attacker could exploit this vulnerability by establishing a connection to the affected device. A successful exploit could allow the attacker to bypass configured ACL rules.	5.8	More Details
CVE-2024-20342	Multiple Cisco products are affected by a vulnerability in the rate filtering feature of the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured rate limiting filter. This vulnerability is due to an incorrect connection count comparison. An attacker could exploit this vulnerability by sending traffic through an affected device at a rate that exceeds a configured rate filter. A successful exploit could allow the attacker to successfully bypass the rate filter. This could allow unintended traffic to enter the network protected by the affected device.	5.8	More Details
CVE-2024-20407	A vulnerability in the interaction between the TCP Intercept feature and the Snort 3 detection engine on Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass configured policies on an affected system. Devices that are configured with Snort 2 are not affected by this vulnerability. This vulnerability is due to a logic error when handling embryonic (half-open) TCP connections. An attacker could exploit this vulnerability by sending a crafted traffic pattern through an affected device. A successful exploit could allow unintended traffic to enter the network protected by the affected device.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30122	HCL Sametime is impacted by misconfigured security related HTTP headers. It was identified that some HTTP headers were missing on web service responses. This will lead to less secure browser default treatment for the policies controlled by these headers.	5.8	More Details
CVE-2024-20431	A vulnerability in the geolocation access control feature of Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass an access control policy. This vulnerability is due to improper assignment of geolocation data. An attacker could exploit this vulnerability by sending traffic through an affected device. A successful exploit could allow the attacker to bypass a geolocation-based access control policy and successfully send traffic to a protected device.	5.8	More Details
CVE-2024-20481	A vulnerability in the Remote Access VPN (RAVPN) service 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) of the RAVPN service. This vulnerability is due to resource exhaustion. An attacker could exploit this vulnerability by sending a large number of VPN authentication requests to an affected device. A successful exploit could allow the attacker to exhaust resources, resulting in a DoS of the RAVPN service on the affected device. Depending on the impact of the attack, a reload of the device may be required to restore the RAVPN service. Services that are not related to VPN are not affected. Cisco Talos discussed these attacks in the blog post Large-scale brute-force activity targeting VPNs, SSH services with commonly used login credentials.	5.8	More Details
CVE-2024-47827	Argo Workflows is an open source container-native workflow engine for orchestrating parallel jobs on Kubernetes. Due to a race condition in a global variable in 3.6.0-rc1, the argo workflows controller can be made to crash on-command by any user with access to execute a workflow. This vulnerability is fixed in 3.6.0-rc2.	5.7	More Details
CVE-2024-44275	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious application may be able to modify protected parts of the file system.	5.5	More Details
CVE-2024-50070	In the Linux kernel, the following vulnerability has been resolved: pinctrl: stm32: check devm_kasprintf() returned value devm_kasprintf() can return a NULL pointer on failure but this returned value is not checked. Fix this lack and check the returned value. Found by code review.	5.5	More Details
CVE-2024-44263	A logic issue was addressed with improved state management. This issue is fixed in iOS 18.1 and iPadOS 18.1. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-44302	The issue was addressed with improved checks. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. Processing a maliciously crafted font may result in the disclosure of process memory.	5.5	More Details
CVE-2024-44264	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious app may be able to create symlinks to protected regions of the disk.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44273	This issue was addressed with improved handling of symlinks. This issue is fixed in iOS 18.1 and iPadOS 18.1, visionOS 2.1, macOS Sonoma 14.7.1, watchOS 11.1, tvOS 18.1. A malicious app may be able to access private information.	5.5	More Details
CVE-2024-50077	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: Fix multiple init when debugfs is disabled If bt_debugfs is not created successfully, which happens if either CONFIG_DEBUG_FS or CONFIG_DEBUG_FS_ALLOW_ALL is unset, then iso_init() returns early and does not set iso_inited to true. This means that a subsequent call to iso_init() will result in duplicate calls to proto_register(), bt_sock_register(), etc. With CONFIG_LIST_HARDENED and CONFIG_BUG_ON_DATA_CORRUPTION enabled, the duplicate call to proto_register() triggers this BUG(): list_add double add: new=ffffffffc0b280d0, prev=ffffffffbab56250, next=ffffffffc0b280d0. ------------[cut here]------------ kernel BUG at lib/list_debug.c:35! Oops: invalid opcode: 0000 [#1] PREEMPT SMP PTI CPU: 2 PID: 887 Comm: bluetoothd Not tainted 6.10.11-1-ao-desktop #1 RIP: 0010:__list_add_valid_or_report+0x9a/0xa0 ... __list_add_valid_or_report+0x9a/0xa0 proto_register+0x2b5/0x340 iso_init+0x23/0x150 [bluetooth] set_iso_socket_func+0x68/0x1b0 [bluetooth] kmem_cache_free+0x308/0x330 hci_sock_sendmsg+0x990/0x9e0 [bluetooth] __sock_sendmsg+0x7b/0x80 sock_write_iter+0x9a/0x110 do_iter_readv_writev+0x11d/0x220 vfs_writev+0x180/0x3e0 do_writev+0xca/0x100 ... This change removes the early return. The check for iso_debugfs being NULL was unnecessary, it is always NULL when iso_inited is false.	5.5	More Details
CVE-2024-50078	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: Call iso_exit() on module unload If iso_init() has been called, iso_exit() must be called on module unload. Without that, the struct proto that iso_init() registered with proto_register() becomes invalid, which could cause unpredictable problems later. In my case, with CONFIG_LIST_HARDENED and CONFIG_BUG_ON_DATA_CORRUPTION enabled, loading the module again usually triggers this BUG(): list_add corruption. next->prev should be prev (ffffffffb5355fd0), but was 0000000000000068. (next=ffffffffc0a010d0). ------------[cut here]------------ kernel BUG at lib/list_debug.c:29! Oops: invalid opcode: 0000 [#1] PREEMPT SMP PTI CPU: 1 PID: 4159 Comm: modprobe Not tainted 6.10.11-4+bt2-ao-desktop #1 RIP: 0010:__list_add_valid_or_report+0x61/0xa0 ... __list_add_valid_or_report+0x61/0xa0 proto_register+0x299/0x320 hci_sock_init+0x16/0xc0 [bluetooth] bt_init+0x68/0xd0 [bluetooth] __pfx_bt_init+0x10/0x10 [bluetooth] do_one_initcall+0x80/0x2f0 do_init_module+0x8b/0x230 __do_sys_init_module+0x15f/0x190 do_syscall_64+0x68/0x110 ...	5.5	More Details
CVE-2024-44269	A logic issue was addressed with improved checks. This issue is fixed in iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. A malicious app may use shortcuts to access restricted files.	5.5	More Details
CVE-2024-44267	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious application may be able to modify protected parts of the file system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44301	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious application may be able to modify protected parts of the file system.	5.5	More Details
CVE-2024-44237	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. Processing a maliciously crafted file may lead to unexpected app termination.	5.5	More Details
CVE-2024-44280	A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2024-44278	An information disclosure issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. A sandboxed app may be able to access sensitive user data in system logs.	5.5	More Details
CVE-2024-44279	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. Parsing a file may lead to disclosure of user information.	5.5	More Details
CVE-2024-44240	The issue was addressed with improved checks. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. Processing a maliciously crafted font may result in the disclosure of process memory.	5.5	More Details
CVE-2024-44281	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. Parsing a file may lead to disclosure of user information.	5.5	More Details
CVE-2024-44282	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. Parsing a file may lead to disclosure of user information.	5.5	More Details
CVE-2024-44284	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. Parsing a maliciously crafted file may lead to an unexpected app termination.	5.5	More Details
CVE-2024-44283	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. Parsing a maliciously crafted file may lead to an unexpected app termination.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50072	In the Linux kernel, the following vulnerability has been resolved: x86/bugs: Use code segment selector for VERW operand Robert Gill reported below #GP in 32-bit mode when dosemu software was executing vm86() system call: general protection fault: 0000 [#1] PREEMPT SMP CPU: 4 PID: 4610 Comm: dosemu.bin Not tainted 6.6.21-gentoo-x86 #1 Hardware name: Dell Inc. PowerEdge 1950/0H723K, BIOS 2.7.0 10/30/2010 EIP: restore_all_switch_stack+0xbe/0xcf EAX: 00000000 EBX: 00000000 ECX: 00000000 EDX: 00000000 ESI: 00000000 EDI: 00000000 EBP: 00000000 ESP: ff8affdc DS: 0000 ES: 0000 FS: 0000 GS: 0033 SS: 0068 EFLAGS: 00010046 CR0: 80050033 CR2: 00c2101c CR3: 04b6d000 CR4: 000406d0 Call Trace: show_regs+0x70/0x78 die_addr+0x29/0x70 exc_general_protection+0x13c/0x348 exc_bounds+0x98/0x98 handle_exception+0x14d/0x14d exc_bounds+0x98/0x98 restore_all_switch_stack+0xbe/0xcf exc_bounds+0x98/0x98 restore_all_switch_stack+0xbe/0xcf This only happens in 32-bit mode when VERW based mitigations like MDS/RFDS are enabled. This is because segment registers with an arbitrary user value can result in #GP when executing VERW. Intel SDM vol. 2C documents the following behavior for VERW instruction: #GP(0) - If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. CLEAR_CPU_BUFFERS macro executes VERW instruction before returning to user space. Use %cs selector to reference VERW operand. This ensures VERW will not #GP for an arbitrary user %ds. [mingo: Fixed the SOB chain.]	5.5	More Details
CVE-2024-44257	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to access sensitive user data.	5.5	More Details
CVE-2024-44262	This issue was addressed with improved redaction of sensitive information. This issue is fixed in visionOS 2.1. A user may be able to view sensitive user information.	5.5	More Details
CVE-2024-50075	In the Linux kernel, the following vulnerability has been resolved: xhci: tegra: fix checked USB2 port number If USB virtualizatoin is enabled, USB2 ports are shared between all Virtual Functions. The USB2 port number owned by an USB2 root hub in a Virtual Function may be less than total USB2 phy number supported by the Tegra XUSB controller. Using total USB2 phy number as port number to check all PORTSC values would cause invalid memory access. [116.923438] Unable to handle kernel paging request at virtual address 006c622f7665642f ... [117.213640] Call trace: [117.216783] tegra_xusb_enter_elpg+0x23c/0x658 [117.222021] tegra_xusb_runtime_suspend+0x40/0x68 [117.227260] pm_generic_runtime_suspend+0x30/0x50 [117.232847] __rpm_callback+0x84/0x3c0 [117.237038] rpm_suspend+0x2dc/0x740 [117.241229] pm_runtime_work+0xa0/0xb8 [117.245769] process_scheduled_works+0x24c/0x478 [117.251007] worker_thread+0x23c/0x328 [117.255547] kthread+0x104/0x1b0 [117.259389] ret_from_fork+0x10/0x20 [117.263582] Code: 54000222 f9461ae8 f8747908 b4ffff48 (f9400100)	5.5	More Details
CVE-2024-44295	This issue was addressed with additional entitlement checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to modify protected parts of the file system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44216	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-44287	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious application may be able to modify protected parts of the file system.	5.5	More Details
CVE-2024-50612	libsndfile through 1.2.2 has an ogg_vorbis.c vorbis_analysis_wrote out-of-bounds read.	5.5	More Details
CVE-2024-44261	This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 17.7.1 and iPadOS 17.7.1, iOS 18.1 and iPadOS 18.1. An attacker may be able to view restricted content from the lock screen.	5.5	More Details
CVE-2024-47018	In pmucal_rae_handle_seq_int of flexpmu_cal_rae.c, there is a possible out of bounds read due to a buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-44185	The issue was addressed with improved checks. This issue is fixed in tvOS 17.6, visionOS 1.3, Safari 17.6, watchOS 10.6, iOS 17.6 and iPadOS 17.6, macOS Sonoma 14.6. Processing maliciously crafted web content may lead to an unexpected process crash.	5.5	More Details
CVE-2024-44205	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.6.8, macOS Monterey 12.7.6, iOS 16.7.9 and iPadOS 16.7.9, iOS 17.6 and iPadOS 17.6, macOS Sonoma 14.6. A sandboxed app may be able to access sensitive user data in system logs.	5.5	More Details
CVE-2024-47173	Aimeos is an e-commerce framework. All SaaS and marketplace setups using the Aimeos GraphQL API admin interface version from 2024.04 up to 2024.07.1 are affected by a potential denial of service attack. Version 2024.07.2 fixes the issue.	5.5	More Details
CVE-2024-48424	A heap-buffer-overflow vulnerability has been identified in the OpenDDLParser::parseStructure function within the Assimp library, specifically during the processing of OpenGEX files.	5.5	More Details
CVE-2024-48425	A segmentation fault (SEGV) was detected in the Assimp::SplitLargeMeshesProcess_Triangle::UpdateNode function within the Assimp library during fuzz testing using AddressSanitizer. The crash occurs due to a read access violation at address 0x000000000460, which points to the zero page, indicating a null or invalid pointer dereference.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49750	The Snowflake Connector for Python provides an interface for developing Python applications that can connect to Snowflake and perform all standard operations. Prior to version 3.12.3, when the logging level was set by the user to DEBUG, the Connector could have logged Duo passcodes (when specified via the `passcode` parameter) and Azure SAS tokens. Additionally, the SecretDetector logging formatter, if enabled, contained bugs which caused it to not fully redact JWT tokens and certain private key formats. Snowflake released version 3.12.3 of the Snowflake Connector for Python, which fixes the issue. In addition to upgrading, users should review their logs for any potentially sensitive information that may have been captured.	5.5	More Details
CVE-2024-44099	There is a possible Local bypass of user interaction due to an insecure default value. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-47015	In ProtocolMiscHwConfigChangeAdapter::GetData() of protocolmiscadapter.cpp, there is a possible out-of-bounds read due to a missing bounds check. This could lead to local information disclosure with baseband firmware compromise required. User Interaction is not needed for exploitation.	5.5	More Details
CVE-2024-47019	In ProtocolEmbmsSaiListAdapter::Init() of protocolembmsadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with baseband firmware compromise required. User Interaction is not needed for exploitation.	5.5	More Details
CVE-2024-20274	A vulnerability in the web-based management interface of Cisco Secure Firewall Management Center (FMC) Software, formerly Firepower Management Center Software, could allow an authenticated, remote attacker to inject arbitrary HTML content into a device-generated document. This vulnerability is due to improper validation of user-supplied data. An attacker could exploit this vulnerability by submitting malicious content to an affected device and using the device to generate a document that contains sensitive information. A successful exploit could allow the attacker to alter the standard layout of the device-generated documents, access arbitrary files from the underlying operating system, and conduct server-side request forgery (SSRF) attacks. To successfully exploit this vulnerability, an attacker would need valid credentials for a user account with policy-editing permissions, such as Network Admin, Intrusion Admin, or any custom user role with the same capabilities.	5.5	More Details
CVE-2024-47025	In ppmp_protect_buf of drm_fw.c, there is a possible information disclosure due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-47026	In gsc_gsa_rescue of gsc_gsa.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-47029	In TrustySharedMemoryManager::GetSharedMemory of ondevice/trusty/trusty_shared_memory_manager.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47034	there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-50068	In the Linux kernel, the following vulnerability has been resolved: mm/damon/tests/sysfs-kunit.h: fix memory leak in damon_sysfs_test_add_targets() The sysfs_target->regions allocated in damon_sysfs_regions_alloc() is not freed in damon_sysfs_test_add_targets(), which cause the following memory leak, free it to fix it. unreferenced object 0xffffff80c2a8db80 (size 96): comm "kunit_try_catch", pid 187, jiffies 4294894363 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace (crc 0): [<0000000001e3714d>] kmemleak_alloc+0x34/0x40 [<000000008e6835c1>] __kmalloc_cache_noprof+0x26c/0x2f4 [<000000001286d9f8>] damon_sysfs_test_add_targets+0x1cc/0x738 [<0000000032ef8f77>] kunit_try_run_case+0x13c/0x3ac [<00000000f3edea23>] kunit_generic_run_threadfn_adapter+0x80/0xec [<00000000adf936cf>] kthread+0x2e8/0x374 [<0000000041bb1628>] ret_from_fork+0x10/0x20	5.5	More Details
CVE-2024-9462	The Poll Maker – Versus Polls, Anonymous Polls, Image Polls plugin for WordPress is vulnerable to Stored Cross-Site Scripting via poll settings in all versions up to, and including, 5.4.6 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.	5.5	More Details
CVE-2017-20195	A vulnerability was found in LUNAD3v AreaLoad up to 1a1103182ed63a06dde63d1712f3262eda19c3ec. It has been rated as critical. This issue affects some unknown processing of the file request.php. The manipulation of the argument phone leads to sql injection. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. The patch is named 264813c546dba03989ac0fc365f2022bf65e3be2. It is recommended to apply a patch to fix this issue.	5.5	More Details
CVE-2024-50307	Use of potentially dangerous function issue exists in Chatwork Desktop Application (Windows) versions prior to 2.9.2. If a user clicks a specially crafted link in the application, an arbitrary file may be downloaded from an external website and executed. As a result, arbitrary code may be executed on the device that runs Chatwork Desktop Application (Windows).	5.5	More Details
CVE-2024-40810	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.6. An app may be able to cause a coprocessor crash.	5.5	More Details
CVE-2024-50087	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix uninitialized pointer free on read_alloc_one_name() error The function read_alloc_one_name() does not initialize the name field of the passed fscrypt_str struct if kmalloc fails to allocate the corresponding buffer. Thus, it is not guaranteed that fscrypt_str.name is initialized when freeing it. This is a follow-up to the linked patch that fixes the remaining instances of the bug introduced by commit e43eec81c516 ("btrfs: use struct qstr instead of name and namelen pairs").	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44215	This issue was addressed with improved checks. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. Processing an image may result in disclosure of process memory.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50084	In the Linux kernel, the following vulnerability has been resolved: net: microchip: vcap api: Fix memory leaks in vcap_api_encode_rule_test() Commit a3c1e45156ad ("net: microchip: vcap: Fix use-after-free error in kunit test") fixed the use-after-free error, but introduced below memory leaks by removing necessary vcap_free_rule(), add it to fix it. unreferenced object 0xffffff80ca58b700 (size 192): comm "kunit_try_catch", pid 1215, jiffies 4294898264 hex dump (first 32 bytes): 00 12 7a 00 05 00 00 00 0a 00 00 00 64 00 00 00 ..z.....d... 00 00 00 00 00 00 00 00 00 00 04 0b cc 80 ff ff ff ..... backtrace (crc 9c09c3fe): [<0000000052a0be73>] kmemleak_alloc+0x34/0x40 [<0000000043605459>] __kmalloc_cache_noprof+0x26c/0x2f4 [<0000000040a01b8d>] vcap_alloc_rule+0x3cc/0x9c4 [<000000003fe86110>] vcap_api_encode_rule_test+0x1ac/0x16b0 [<00000000b3595fc4>] kunit_try_run_case+0x13c/0x3ac [<0000000010f5d2bf>] kunit_generic_run_threadfn_adapter+0x80/0xec [<00000000c5d82c9a>] kthread+0x2e8/0x374 [<00000000f4287308>] ret_from_fork+0x10/0x20 unreferenced object 0xffffff80cc0b0400 (size 64): comm "kunit_try_catch", pid 1215, jiffies 4294898265 hex dump (first 32 bytes): 80 04 0b cc 80 ff ff ff 18 b7 58 ca 80 ff ff ff ....X..... 39 00 00 00 02 00 00 00 06 05 04 03 02 01 ff ff 9..... backtrace (crc daf014e9): [<0000000052a0be73>] kmemleak_alloc+0x34/0x40 [<0000000043605459>] __kmalloc_cache_noprof+0x26c/0x2f4 [<000000000ff63fd4>] vcap_rule_add_key+0x2cc/0x528 [<00000000dfdb1e81>] vcap_api_encode_rule_test+0x224/0x16b0 [<00000000b3595fc4>] kunit_try_run_case+0x13c/0x3ac [<0000000010f5d2bf>] kunit_generic_run_threadfn_adapter+0x80/0xec [<00000000c5d82c9a>] kthread+0x2e8/0x374 [<00000000f4287308>] ret_from_fork+0x10/0x20 unreferenced object 0xffffff80cc0b0700 (size 64): comm "kunit_try_catch", pid 1215, jiffies 4294898265 hex dump (first 32 bytes): 80 07 0b cc 80 ff ff ff 28 b7 58 ca 80 ff ff ff ....(.X..... 3c 00 00 00 00 00 00 00 01 2f 03 b3 ec ff ff ff <......../..... backtrace (crc 8d877792): [<0000000052a0be73>] kmemleak_alloc+0x34/0x40 [<0000000043605459>] __kmalloc_cache_noprof+0x26c/0x2f4 [<000000006eadfab7>] vcap_rule_add_action+0x2d0/0x52c [<00000000323475d1>] vcap_api_encode_rule_test+0x4d4/0x16b0 [<00000000b3595fc4>] kunit_try_run_case+0x13c/0x3ac [<0000000010f5d2bf>] kunit_generic_run_threadfn_adapter+0x80/0xec [<00000000c5d82c9a>] kthread+0x2e8/0x374 [<00000000f4287308>] ret_from_fork+0x10/0x20 unreferenced object 0xffffff80cc0b0900 (size 64): comm "kunit_try_catch", pid 1215, jiffies 4294898266 hex dump (first 32 bytes): 80 09 0b cc 80 ff ff ff 80 06 0b cc 80 ff ff ff ..... 7d 00 00 00 01 00 00 00 00 00 00 00 ff 00 00 00 }..... backtrace (crc 34181e56): [<0000000052a0be73>] kmemleak_alloc+0x34/0x40 [<0000000043605459>] __kmalloc_cache_noprof+0x26c/0x2f4 [<000000000ff63fd4>] vcap_rule_add_key+0x2cc/0x528 [<00000000991e3564>] vcap_val_rule+0xcf0/0x13e8 [<00000000fc9868e5>] vcap_api_encode_rule_test+0x678/0x16b0 [<00000000b3595fc4>] kunit_try_run_case+0x13c/0x3ac [<0000000010f5d2bf>] kunit_generic_run_threadfn_adapter+0x80/0xec [<00000000c5d82c9a>] kthread+0x2e8/0x374 [<00000000f4287308>] ret_from_fork+0x10/0x20 unreferenced object 0xffffff80cc0b0980 (size 64): comm "kunit_try_catch", pid 1215, jiffies 4294898266 hex dump (first 32 bytes): 18 b7 58 ca 80 ff ff ff 00 09 0b cc 80 ff ff ff ..X..... 67 00 00 00 00 00 00 00 01 01 74 88 c0 ff ff ff g.....t..... backtrace (crc 275fd9be): [<0000000052a0be73>] kmemleak_alloc+0x34/0x40 [<0000000043605459>] __kmalloc_cache_noprof+0x26c/0x2f4 [<000000000ff63fd4>]	5.5	More Details

CVE Number	Description	Base Score	Reference
	vcap_rule_add_key+0x2cc/0x528 [<000000001396a1a2>] test_add_de ---truncated---		
CVE-2024-44254	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 11.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, iOS 18.1 and iPadOS 18.1. An app may be able to access sensitive user data.	5.5	More Details
CVE-2024-44253	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2024-50079	In the Linux kernel, the following vulnerability has been resolved: io_uring/sqpoll: ensure task state is TASK_RUNNING when running task_work When the sqpoll is exiting and cancels pending work items, it may need to run task_work. If this happens from within io_uring_cancel_generic(), then it may be under waiting for the io_uring_task waitqueue. This results in the below splat from the scheduler, as the ring mutex may be attempted grabbed while in a TASK_INTERRUPTIBLE state. Ensure that the task state is set appropriately for that, just like what is done for the other cases in io_run_task_work(). do not call blocking ops when !TASK_RUNNING; state=1 set at [<0000000029387fd2>] prepare_to_wait+0x88/0x2fc WARNING: CPU: 6 PID: 59939 at kernel/sched/core.c:8561 __might_sleep+0xf4/0x140 Modules linked in: CPU: 6 UID: 0 PID: 59939 Comm: iou-sqp-59938 Not tainted 6.12.0-rc3-00113-g8d020023b155 #7456 Hardware name: linux,dummy-virt (DT) pstate: 61400005 (nZCv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=--) pc : __might_sleep+0xf4/0x140 lr : __might_sleep+0xf4/0x140 sp : ffff80008c5e7830 x29: ffff80008c5e7830 x28: ffff0000d93088c0 x27: ffff60001c2d7230 x26: dfff800000000000 x25: ffff0000e16b9180 x24: ffff80008c5e7a50 x23: 1ffff000118bcf4a x22: ffff0000e16b9180 x21: ffff0000e16b9180 x20: 000000000000011b x19: ffff80008310fac0 x18: 1ffff000118bcd90 x17: 30303c5b20746120 x16: 74657320313d6574 x15: 0720072007200720 x14: 0720072007200720 x13: 0720072007200720 x12: ffff600036c64f0b x11: 1fffe00036c64f0a x10: ffff600036c64f0a x9 : dfff800000000000 x8 : 00009fffc939b0f6 x7 : ffff0001b6327853 x6 : 0000000000000001 x5 : ffff0001b6327850 x4 : ffff600036c64f0b x3 : ffff8000803c35bc x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffff0000e16b9180 Call trace: __might_sleep+0xf4/0x140 mutex_lock+0x84/0x124 io_handle_tw_list+0xf4/0x260 tctx_task_work_run+0x94/0x340 io_run_task_work+0x1ec/0x3c0 io_uring_cancel_generic+0x364/0x524 io_sq_thread+0x820/0x124c ret_from_fork+0x10/0x20	5.5	More Details
CVE-2024-44247	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious application may be able to modify protected parts of the file system.	5.5	More Details
CVE-2024-50080	In the Linux kernel, the following vulnerability has been resolved: ublk: don't allow user copy for unprivileged device UBLK_F_USER_COPY requires userspace to call write() on ublk char device for filling request buffer, and unprivileged device can't be trusted. So don't allow user copy for unprivileged device.	5.5	More Details
CVE-2024-44239	An information disclosure issue was addressed with improved private data redaction for log entries. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. An app may be able to leak sensitive kernel state.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44236	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. Processing a maliciously crafted file may lead to unexpected app termination.	5.5	More Details
CVE-2024-50081	In the Linux kernel, the following vulnerability has been resolved: blk-mq: setup queue ->tag_set before initializing hctx Commit 7b815817aa58 ("blk-mq: add helper for checking if one CPU is mapped to specified hctx") needs to check queue mapping via tag set in hctx's cpuhp handler. However, q->tag_set may not be setup yet when the cpuhp handler is enabled, then kernel oops is triggered. Fix the issue by setup queue tag_set before initializing hctx.	5.5	More Details
CVE-2024-50069	In the Linux kernel, the following vulnerability has been resolved: pinctrl: apple: check devm_kasprintf() returned value devm_kasprintf() can return a NULL pointer on failure but this returned value is not checked. Fix this lack and check the returned value. Found by code review.	5.5	More Details
CVE-2024-40855	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sequoia 15, macOS Sonoma 14.7.1. A sandboxed app may be able to access sensitive user data.	5.5	More Details
CVE-2024-44197	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious app may be able to cause a denial-of-service.	5.5	More Details
CVE-2024-44196	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2024-44194	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 11.1, visionOS 2.1, iOS 18.1 and iPadOS 18.1. An app may be able to access sensitive user data.	5.5	More Details
CVE-2024-44175	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Sequoia 15, macOS Sonoma 14.7.1. An app may be able to access sensitive user data.	5.5	More Details
CVE-2024-44174	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15. An attacker may be able to view restricted content from the lock screen.	5.5	More Details
CVE-2024-44144	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 17.7.1 and iPadOS 17.7.1, macOS Sequoia 15, macOS Sonoma 14.7.1, tvOS 18, watchOS 11, visionOS 2, iOS 18 and iPadOS 18. Processing a maliciously crafted file may lead to unexpected app termination.	5.5	More Details
	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: fix UaF read in mptcp_pm_nl_rm_addr_or_subflow Syzkaller reported this splat: == BUG: KASAN: slab-use-after-free in mptcp_pm_nl_rm_addr_or_subflow+0xb44/0xcc0 net/mptcp/pm_netlink.c:881 Read of size 4 at addr ffff8880569ac858 by task syz.1.2799/14662 CPU: 0 UID: 0 PID: 14662 Comm: syz.1.2799 Not tainted 6.12.0-rc2-syzkaller-00307-g36c254515dc6 #0 Hardware name: QEMU Standard PC (Q35 +		

CVE Number	Description	Base Score	Reference
	ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2~bpo12+1 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:377 [inline]		
CVE-2024-50085	print_report+0xc3/0x620 mm/kasan/report.c:488 kasan_report+0xd9/0x110 mm/kasan/report.c:601 mptcp_pm_nl_rm_addr_or_subflow+0xb44/0xcc0 net/mptcp/pm_netlink.c:881 mptcp_pm_nl_rm_subflow_received net/mptcp/pm_netlink.c:914 [inline] mptcp_nl_remove_id_zero_address+0x305/0x4a0 net/mptcp/pm_netlink.c:1572 mptcp_pm_nl_del_addr_doit+0x5c9/0x770 net/mptcp/pm_netlink.c:1603 genl_family_rcv_msg_doit+0x202/0x2f0 net/netlink/genetlink.c:1115 genl_family_rcv_msg net/netlink/genetlink.c:1195 [inline] genl_rcv_msg+0x565/0x800 net/netlink/genetlink.c:1210 netlink_rcv_skb+0x165/0x410 net/netlink/af_netlink.c:2551 genl_rcv+0x28/0x40 net/netlink/genetlink.c:1219 netlink_unicast_kernel net/netlink/af_netlink.c:1331 [inline] netlink_unicast+0x53c/0x7f0 net/netlink/af_netlink.c:1357 netlink_sendmsg+0x8b8/0xd70 net/netlink/af_netlink.c:1901 sock_sendmsg_nosec net/socket.c:729 [inline] __sock_sendmsg net/socket.c:744 [inline] ____sys_sendmsg+0x9ae/0xb40 net/socket.c:2607 ___sys_sendmsg+0x135/0x1e0 net/socket.c:2661 __sys_sendmsg+0x117/0x1f0 net/socket.c:2690 do_syscall_32_irqs_on arch/x86/entry/common.c:165 [inline] __do_fast_syscall_32+0x73/0x120 arch/x86/entry/common.c:386 do_fast_syscall_32+0x32/0x80 arch/x86/entry/common.c:411 entry_SYSENTER_compat_after_hwframe+0x84/0x8e RIP: 0023:0xf7fe4579 Code: b8 01 10 06 03 74 b4 01 10 07 03 74 b0 01 10 08 03 74 d8 01 00 00 00 00 00 00 00 00 00 00 00 00 51 52 55 89 e5 0f 34 cd 80 <5d> 5a 59 c3 90 90 90 90 8d b4 26 00 00 00 00 8d b4 26 00 00 00 00 RSP: 002b:00000000f574556c EFLAGS: 00000296 ORIG_RAX: 0000000000000172 RAX: ffffffffffffffda RBX: 000000000000000b RCX: 0000000020000140 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: 0000000000000000 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000296 R12: 0000000000000000 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 </TASK> Allocated by task 5387: kasan_save_stack+0x33/0x60 mm/kasan/common.c:47 kasan_save_track+0x14/0x30 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0xaa/0xb0 mm/kasan/common.c:394 kmalloc_noprof include/linux/slab.h:878 [inline] kzalloc_noprof include/linux/slab.h:1014 [inline] subflow_create_ctx+0x87/0x2a0 net/mptcp/subflow.c:1803 subflow_ulp_init+0xc3/0x4d0 net/mptcp/subflow.c:1956 __tcp_set_ulp net/ipv4/tcp_ulp.c:146 [inline] tcp_set_ulp+0x326/0x7f0 net/ipv4/tcp_ulp.c:167 mptcp_subflow_create_socket+0x4ae/0x10a0 net/mptcp/subflow.c:1764 __mptcp_subflow_connect+0x3cc/0x1490 net/mptcp/subflow.c:1592 mptcp_pm_create_subflow_or_signal_addr+0xbda/0x23a0 net/mptcp/pm_netlink.c:642 mptcp_pm_nl_fully_established net/mptcp/pm_netlink.c:650 [inline] mptcp_pm_nl_work+0x3a1/0x4f0 net/mptcp/pm_netlink.c:943 mptcp_worker+0x15a/0x1240 net/mptcp/protocol.c:2777 process_one_work+0x958/0x1b30 kernel/workqueue.c:3229 process_scheduled_works kernel/workqueue.c:3310 [inline] worker_thread+0x6c8/0xf00 kernel/workqueue.c:3391 kthread+0x2c1/0x3a0 kernel/kthread.c:389 ret_from_fork+0x45/0x80 arch/x86/ke ---truncated---	5.5	More Details
CVE-2024-50423	Missing Authorization vulnerability in Templately allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Templately: from n/a through 3.1.5.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50456	Missing Authorization vulnerability in The SEO Guys at SEOPress SEOPress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SEOPress: from n/a through 8.1.1.	5.4	More Details
CVE-2024-50348	InstantCMS is a free and open source content management system. In photo upload function in the photo album page there is no input validation taking place. Due to this attackers are able to inject the XSS (Cross Site Scripting) payload and execute. This vulnerability is fixed in 2.16.3.	5.4	More Details
CVE-2024-20387	A vulnerability in the web-based management interface of Cisco FMC Software could allow an authenticated, remote attacker to store malicious content for use in XSS attacks. This vulnerability is due to improper input sanitization in the web-based management interface of Cisco FMC Software. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to conduct a stored XSS attack on an affected device.	5.4	More Details
CVE-2024-20377	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to the web-based management interface not properly validating user-supplied input. An attacker could exploit this vulnerability by by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	5.4	More Details
CVE-2024-9629	The Contact Form 7 + Telegram plugin for WordPress is vulnerable to unauthorized modification of data and loss of data due to a missing capability check on the 'wpcf7_Telegram::ajax' function in versions up to, and including, 0.8.5. This makes it possible for authenticated attackers, with subscriber-level access and above, to approve, pause and refuse subscriptions.	5.4	More Details
CVE-2024-37844	A stored cross-site scripting (XSS) vulnerability in MangoOS before 5.2.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2024-9825	The Chef Habitat builder-api on-prem-builder package with any version lower than habitat/builder-api/10315/20240913162802 is vulnerable to indirect object reference (IDOR) by un-authorized deletion of personal token. Habitat builder consumes builder-api habitat package as a dependency and the vulnerability was specifically due to builder-api habitat package. The fix was made available in habitat/builder-api/10315/20240913162802 and all the subsequent versions after that. We would recommend user to always use on-prem stable channel.	5.4	More Details
CVE-2024-9584	The Image Map Pro plugin for WordPress is vulnerable to unauthorized modification of data and loss of data due to a missing capability check on the AJAX functions in versions up to, and including, 6.0.20. This makes it possible for authenticated attackers with contributor-level privileges or above, to add, update or delete map projects.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9630	The WPS Telegram Chat plugin for WordPress is vulnerable to authorization bypass due to a missing capability check when accessing messages in versions up to, and including, 4.5.4. This makes it possible for unauthenticated attackers to view the messages that are sent through the Telegram Bot API.	5.4	More Details
CVE-2024-47158	N-LINE 2.0.6 and prior versions contain a code injection vulnerability. If this vulnerability is exploited, arbitrary code may be executed on the instructor's browser, or the instructor may be directed to a malicious website.	5.4	More Details
CVE-2024-8500	The WP Shortcodes Plugin — Shortcodes Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the several parameters in all versions up to, and including, 7.2.2 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.	5.4	More Details
CVE-2024-46994	baserCMS is a website development framework. Versions prior to 5.1.2 have a cross-site scripting vulnerability in Blog posts and Contents list Feature. Version 5.1.2 fixes this issue.	5.4	More Details
CVE-2024-50575	In JetBrains YouTrack before 2024.3.47707 reflected XSS was possible in Widget API	5.4	More Details
CVE-2024-44296	The issue was addressed with improved checks. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, watchOS 11.1, visionOS 2.1, macOS Sequoia 15.1, Safari 18.1. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.	5.4	More Details
CVE-2024-20410	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability 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.	5.4	More Details
CVE-2024-50459	Missing Authorization vulnerability in HM Plugin WordPress Stripe Donation and Payment Plugin allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WordPress Stripe Donation and Payment Plugin: from n/a through 3.2.3.	5.3	More Details
CVE-2023-26248	The Kademlia DHT (go-libp2p-kad-dht 0.20.0 and earlier) used in IPFS (0.18.1 and earlier) assigns routing information for content (i.e., information about who holds the content) to be stored by peers whose peer IDs have a small DHT distance from the content ID. This allows an attacker to censor content by generating many Sybil peers whose peer IDs have a small distance from the content ID, thus hijacking the content resolution process.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20388	A vulnerability in the password change feature of Cisco Firepower Management Center (FMC) software could allow an unauthenticated, remote attacker to determine valid user names on an affected device. This vulnerability is due to improper authentication of password update responses. An attacker could exploit this vulnerability by forcing a password reset on an affected device. A successful exploit could allow the attacker to determine valid user names in the unauthenticated response to a forced password reset.	5.3	More Details
CVE-2024-50574	In JetBrains YouTrack before 2024.3.47707 potential ReDoS exploit was possible via email header parsing in Helpdesk functionality	5.3	More Details
CVE-2024-10439	The eHRD CTMS from Sunnet has an Insecure Direct Object Reference (IDOR) vulnerability, allowing unauthenticated remote attackers to modify a specific parameter to access arbitrary files uploaded by any user.	5.3	More Details
CVE-2024-10290	A vulnerability, which was classified as problematic, was found in ZZCMS 2023. This affects an unknown part of the file 3/qq-connect2.0/API/com/inc.php. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2024-50422	Missing Authorization vulnerability in Cloudways Breeze allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Breeze: from n/a through 2.1.14.	5.3	More Details
CVE-2024-50421	Missing Authorization vulnerability in WP Overnight WooCommerce PDF Invoices & Packing Slips allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WooCommerce PDF Invoices & Packing Slips: from n/a through 3.8.6.	5.3	More Details
CVE-2022-30361	OvalEdge 5.2.8.0 and earlier is affected by a Sensitive Data Exposure vulnerability via a GET request to /user/getUserType. No authentication is required. The information disclosed is associated with the registered user ID, status, email address, role(s), user type, license type, and personal details such as first name, last name, gender, and user preferences.	5.3	More Details
CVE-2024-10460	The origin of an external protocol handler prompt could have been obscured using a data: URL within an `iframe`. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49756	AshPostgres is the PostgreSQL data layer for Ash Framework. Starting in version 2.0.0 and prior to version 2.4.10, in certain very specific situations, it was possible for the policies of an update action to be skipped. This occurred only on "empty" update actions (no changing fields), and would allow their hooks (side effects) to be performed when they should not have been. Note that this does not allow reading new data that the user should not have had access to, only triggering a side effect a user should not have been able to trigger. To be vulnerable, an affected user must have an update action that is on a resource with no attributes containing an "update default" (updated_at timestamp, for example); can be performed atomically; does not have `require_atomic? false`; has at least one authorizer (typically `Ash.Policy.Authorizer`); and has at least one `change` (on the resource's `changes` block or in the action itself). This is where the side-effects would be performed when they should not have been. This problem has been patched in `2.4.10` of `ash_postgres`. Several workarounds are available. Potentially affected users may determine that none of their actions are vulnerable using a script the maintainers provide in the GitHub Security Advisory, add `require_atomic? false` to any potentially affected update action, replace any usage of `Ash.update` with `Ash.bulk_update` for an affected action, and/or add an update timestamp to their action.	5.3	More Details
CVE-2024-50334	Scoold is a Q&A and a knowledge sharing platform for teams. A semicolon path injection vulnerability was found on the /api;/config endpoint. By appending a semicolon in the URL, attackers can bypass authentication and gain unauthorised access to sensitive configuration data. Furthermore, PUT requests on the /api;/config endpoint while setting the Content-Type: application/hocon header allow unauthenticated attackers to file reading via HOCON file inclusion. This allows attackers to retrieve sensitive information such as configuration files from the server, which can be leveraged for further exploitation. The vulnerability has been fixed in Scoold 1.64.0. A workaround would be to disable the Scoold API with scoold.api_enabled = false.	5.3	More Details
CVE-2024-10468	Potential race conditions in IndexedDB could have caused memory corruption, leading to a potentially exploitable crash. This vulnerability affects Firefox < 132 and Thunderbird < 132.	5.3	More Details
CVE-2024-20493	A vulnerability in the login authentication functionality of the Remote Access SSL VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to deny further VPN user authentications for several minutes, resulting in a temporary denial of service (DoS) condition. This vulnerability is due to ineffective handling of memory resources during the authentication process. An attacker could exploit this vulnerability by sending crafted packets, which could cause resource exhaustion of the authentication process. A successful exploit could allow the attacker to deny authentication for Remote Access SSL VPN users for several minutes, resulting in a temporary DoS condition.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20526	A vulnerability in the SSH server of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition for the SSH server of an affected device. This vulnerability is due to a logic error when an SSH session is established. An attacker could exploit this vulnerability by sending crafted SSH messages to an affected device. A successful exploit could allow the attacker to exhaust available SSH resources on the affected device so that new SSH connections to the device are denied, resulting in a DoS condition. Existing SSH connections to the device would continue to function normally. The device must be rebooted manually to recover. However, user traffic would not be impacted and could be managed using a remote application such as Cisco Adaptive Security Device Manager (ASDM).	5.3	More Details
CVE-2024-45842	Sharp and Toshiba Tec MFPs improperly process URI data in HTTP PUT requests resulting in a path Traversal vulnerability. Unintended internal files may be retrieved when processing crafted HTTP requests.	5.3	More Details
CVE-2024-9686	The Order Notification for Telegram plugin for WordPress is vulnerable to unauthorized test message sending due to a missing capability check on the 'nktgnfw_send_test_message' function in versions up to, and including, 1.0.1. This makes it possible for unauthenticated attackers to send a test message via the Telegram Bot API to the user configured in the settings.	5.3	More Details
CVE-2024-48932	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In version 1.2.4 and all prior versions, the API endpoint `http://<Server-ip>/v1/users/name` allows unauthenticated users to access sensitive information, such as usernames, without any authorization. This vulnerability could be exploited by an attacker to enumerate usernames and leverage them for further attacks, such as brute-force or phishing campaigns. As of time of publication, no known patched versions are available.	5.3	More Details
CVE-2024-50454	Missing Authorization vulnerability in The SEO Guys at SEOPress SEOPress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SEOPress: from n/a through 8.1.1.	5.3	More Details
CVE-2024-49683	Missing Authorization vulnerability in Schema & Structured Data for WP & AMP allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Schema & Structured Data for WP & AMP: from n/a through 1.3.5.	5.3	More Details
CVE-2024-40595	An authentication-bypass issue in the RDP component of One Identity Safeguard for Privileged Sessions (SPS) On Premise before 7.5.1 (and LTS before 7.0.5.1) allows man-in-the-middle attackers to obtain access to privileged sessions on target resources by intercepting cleartext RDP protocol information.	5.3	More Details
CVE-2024-49358	ZimaOS is a fork of CasaOS, an operating system for Zima devices and x86-64 systems with UEFI. In version 1.2.4 and all prior versions, the API endpoint `http://<Server-IP>/v1/users/login` in ZimaOS returns distinct responses based on whether a username exists or the password is incorrect. This behavior can be exploited for username enumeration, allowing attackers to determine whether a user exists in the system or not. Attackers can leverage this information in further attacks, such as credential stuffing or targeted password brute-forcing. As of time of publication, no known patched versions are available.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31880	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to a denial of service, under specific configurations, as the server may crash when using a specially crafted SQL statement by an authenticated user.	5.3	More Details
CVE-2024-44229	An information leakage was addressed with additional validation. This issue is fixed in visionOS 2.1, iOS 18.1 and iPadOS 18.1, macOS Sequoia 15.1, Safari 18.1. Private browsing may leak some browsing history.	5.3	More Details
CVE-2024-43924	Missing Authorization vulnerability in dFactory Responsive Lightbox allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Responsive Lightbox: from n/a through 2.4.7.	5.3	More Details
CVE-2024-49771	MPXJ is an open source library to read and write project plans from a variety of file formats and databases. The patch for the historical vulnerability CVE-2020-35460 in MPXJ is incomplete as there is still a possibility that a malicious path could be constructed which would not be picked up by the original fix and allow files to be written to arbitrary locations. The issue is addressed in MPXJ version 13.5.1.	5.3	More Details
CVE-2024-47030	Android before 2024-10-05 on Google Pixel devices allows information disclosure in the ACPM component, A-315191818.	5.1	More Details
CVE-2024-48936	SchedMD Slurm before 24.05.4 has Incorrect Authorization. A mistake in authentication handling in stepmgr could permit an attacker to execute processes under other users' jobs. This is limited to jobs explicitly running with --stepmgr, or on systems that have globally enabled stepmgr via SlurmctldParameters=enable_stepmgr in their configuration.	5.0	More Details
CVE-2024-34537	TYPO3 before 13.3.1 allows denial of service (interface error) in the Bookmark Toolbar (ext:backend), exploitable by an administrator-level backend user account via manipulated data saved in the bookmark toolbar of the backend user interface. The fixed versions are 10.4.46 ELTS, 11.5.40 LTS, 12.4.21 LTS, and 13.3.1.	4.9	More Details
CVE-2024-45829	Sharp and Toshiba Tec MFPs provide the web page to download data, where query parameters in HTTP requests are improperly processed and resulting in an Out-of-bounds Read vulnerability. Crafted HTTP requests may cause affected products crashed.	4.9	More Details
CVE-2023-50310	IBM CICS Transaction Gateway for Multiplatforms 9.2 and 9.3 transmits or stores authentication credentials, but it uses an insecure method that is susceptible to unauthorized interception and/or retrieval.	4.9	More Details
CVE-2024-48224	Funadmin v5.0.2 has an arbitrary file read vulnerability in /curd/index/editfile.	4.9	More Details
CVE-2024-48227	Funadmin 5.0.2 has a logical flaw in the Curd one click command deletion function, which can result in a Denial of Service (DOS).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48234	An issue was discovered in mipjz 5.0.5. In the push method of app\tag\controller\ApiAdminTag.php the value of the postAddress parameter is not processed and is directly passed into curl_exec execution and output, resulting in Server-side request forgery (SSRF) vulnerability that can read server files.	4.9	More Details
CVE-2024-9475	The Poll Maker – Versus Polls, Anonymous Polls, Image Polls plugin for WordPress is vulnerable to generic SQL Injection via the order_by parameter in all versions up to, and including, 5.4.6 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 administrator-level permissions and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	4.9	More Details
CVE-2024-49370	Pimcore is an open source data and experience management platform. When a PortalUserObject is connected to a PimcoreUser and "Use Pimcore Backend Password" is set to true, the change password function in Portal Profile sets the new password. Prior to Pimcore portal engine versions 4.1.7 and 3.1.16, the password is then set without hashing so it can be read by everyone. Everyone who combines PortalUser to PimcoreUsers and change passwords via profile settings could be affected. Versions 4.1.7 and 3.1.16 of the Pimcore portal engine fix the issue.	4.9	More Details
CVE-2024-48232	An issue was found in mipjz 5.0.5. In the mipPost method of \app\setting\controller\ApiAdminTool.php, the value of the postAddress parameter is not processed and is directly passed into curl_exec execution and output, resulting in a Server-side request forgery (SSRF) vulnerability that can read server files.	4.9	More Details
CVE-2024-20300	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability 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.	4.8	More Details
CVE-2024-51506	Tiki through 27.0 allows users who have certain permissions to insert a "Create a Wiki Pages" stored XSS payload in the description.	4.8	More Details
CVE-2024-20364	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability 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.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20269	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability 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.	4.8	More Details
CVE-2024-20264	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability 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.	4.8	More Details
CVE-2024-20298	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability 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.	4.8	More Details
CVE-2024-48233	mipjz 5.0.5 is vulnerable to Cross Site Scripting (XSS) in \app\setting\controller\ApiAdminSetting.php via the ICP parameter.	4.8	More Details
CVE-2024-48461	Cross Site Scripting vulnerability in TeslaLogger Admin Panel before v.1.59.6 allows a remote attacker to execute arbitrary code via the New Journey field.	4.8	More Details
CVE-2024-20415	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability 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.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20409	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability 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.	4.8	More Details
CVE-2024-20403	A vulnerability in the web-based management interface of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability 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.	4.8	More Details
CVE-2024-51507	Tiki through 27.0 allows users who have certain permissions to insert a "Create/Edit External Wiki" stored XSS payload in the Name.	4.8	More Details
CVE-2024-20386	A vulnerability 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. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability 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.	4.8	More Details
CVE-2024-51508	Tiki through 27.0 allows users who have certain permissions to insert a "Create/Edit External Wiki" stored XSS payload in the Index.	4.8	More Details
CVE-2024-51509	Tiki through 27.0 allows users who have certain permissions to insert a "Modules" (aka tiki-admin_modules.php) stored XSS payload in the Name.	4.8	More Details
CVE-2024-48239	An issue was discovered in WTCMS 1.0. In the plupload method in \AssetController.class.php, the app parameters aren't processed, resulting in Cross Site Scripting (XSS).	4.8	More Details
CVE-2024-10337	A vulnerability classified as critical has been found in SourceCodeHero Clothes Recommendation System 1.0. Affected is an unknown function of the file /admin/home.php?con=add. The manipulation of the argument cat/subcat/ t1/t2/text leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10297	A vulnerability was found in PHPGurukul Medical Card Generation System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/changeimage.php of the component Managecard Edit Image Page. The manipulation of the argument editid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-50463	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in WP Sunshine Sunshine Photo Cart.This issue affects Sunshine Photo Cart: from n/a through 3.2.9.	4.7	More Details
CVE-2024-10338	A vulnerability classified as critical was found in SourceCodeHero Clothes Recommendation System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/home.php. The manipulation of the argument view/view1 leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2022-30356	OvalEdge 5.2.8.0 and earlier is affected by a Privilege Escalation vulnerability via a POST request to /user/assignuserrole via the userid and role parameters . Authentication is required with OE_ADMIN role privilege.	4.7	More Details
CVE-2024-10350	A vulnerability was found in code-projects Hospital Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/add-doctor.php. The manipulation of the argument docname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-10354	A vulnerability classified as critical was found in SourceCodester Petrol Pump Management Software 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/print.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-10355	A vulnerability, which was classified as critical, has been found in SourceCodester Petrol Pump Management Software 1.0. Affected by this issue is some unknown functionality of the file /admin/invoice.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50082	In the Linux kernel, the following vulnerability has been resolved: blk-rq-qos: fix crash on rq_qos_wait vs. rq_qos_wake_function race We're seeing crashes from rq_qos_wake_function that look like this: BUG: unable to handle page fault for address: ffffafe180a40084 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 100000067 P4D 100000067 PUD 10027c067 PMD 10115d067 PTE 0 Oops: Oops: 0002 [#1] PREEMPT SMP PTI CPU: 17 UID: 0 PID: 0 Comm: swapper/17 Not tainted 6.12.0-rc3-00013-geca631b8fe80 #11 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 RIP: 0010:_raw_spin_lock_irqsave+0x1d/0x40 Code: 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa 0f 1f 44 00 00 41 54 9c 41 5c fa 65 ff 05 62 97 30 4c 31 c0 ba 01 00 00 00 <f0> 0f b1 17 75 0a 4c 89 e0 41 5c c3 cc cc cc cc 89 c6 e8 2c 0b 00 RSP: 0018:ffffafe180580ca0 EFLAGS: 00010046 RAX: 0000000000000000 RBX: ffffafe180a3f7a8 RCX: 0000000000000011 RDX: 0000000000000001 RSI: 0000000000000003 RDI: ffffafe180a40084 RBP: 0000000000000000 R08: 00000000001e7240 R09: 0000000000000011 R10: 0000000000000028 R11: 0000000000000888 R12: 0000000000000002 R13: ffffafe180a40084 R14: 0000000000000000 R15: 0000000000000003 FS: 0000000000000000(0000) GS:ffff9aaf1f280000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffafe180a40084 CR3: 000000010e428002 CR4: 0000000000770ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <IRQ> try_to_wake_up+0x5a/0x6a0 rq_qos_wake_function+0x71/0x80 __wake_up_common+0x75/0xa0 __wake_up+0x36/0x60 scale_up.part.0+0x50/0x110 wb_timer_fn+0x227/0x450 ... So rq_qos_wake_function() calls wake_up_process(data->task), which calls try_to_wake_up(), which faults in raw_spin_lock_irqsave(&p->pi_lock). p comes from data->task, and data comes from the waitqueue entry, which is stored on the waiter's stack in rq_qos_wait(). Analyzing the core dump with drgn, I found that the waiter had already woken up and moved on to a completely unrelated code path, clobbering what was previously data->task. Meanwhile, the waker was passing the clobbered garbage in data->task to wake_up_process(), leading to the crash. What's happening is that in between rq_qos_wake_function() deleting the waitqueue entry and calling wake_up_process(), rq_qos_wait() is finding that it already got a token and returning. The race looks like this: rq_qos_wait() rq_qos_wake_function() == prepare_to_wait_exclusive() data->got_token = true; list_del_init(&curr->entry); if (data.got_token) break; finish_wait(&rqw->wait, &data.wq); ^- returns immediately because list_empty_careful(&wq_entry->entry) is true ... return, go do something else ... wake_up_process(data->task) (NO LONGER VALID!)-^ Normally, finish_wait() is supposed to synchronize against the waker. But, as noted above, it is returning immediately because the waitqueue entry has already been removed from the waitqueue. The bug is that rq_qos_wake_function() is accessing the waitqueue entry AFTER deleting it. Note that autoremove_wake_function() wakes the waiter and THEN deletes the waitqueue entry, which is the proper order. Fix it by swapping the order. We also need to use list_del_init_careful() to match the list_empty_careful() in finish_wait().	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48238	WTCMS 1.0 is vulnerable to SQL Injection in the edit_post method of /Admin\Controller\NavControl.class.php via the parentid parameter.	4.7	More Details
CVE-2024-49682	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in smp7, wp.Insider Simple Membership allows Phishing.This issue affects Simple Membership: from n/a through 4.5.3.	4.7	More Details
CVE-2024-10301	A vulnerability, which was classified as critical, was found in PHPGurukul Medical Card Generation System 1.0. Affected is an unknown function of the file /admin/search-medicalcard.php of the component Search. The manipulation of the argument searchdata leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-10300	A vulnerability, which was classified as critical, has been found in PHPGurukul Medical Card Generation System 1.0. This issue affects some unknown processing of the file /admin/view-enquiry.php of the component View Enquiry Page. The manipulation of the argument viewid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-10299	A vulnerability classified as critical was found in PHPGurukul Medical Card Generation System 1.0. This vulnerability affects unknown code of the file /admin/view-card-detail.php of the component Managecard View Detail Page. The manipulation of the argument viewid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-10298	A vulnerability classified as critical has been found in PHPGurukul Medical Card Generation System 1.0. This affects an unknown part of the file /admin/edit-card-detail.php of the component Managecard Edit Card Detail Page. The manipulation of the argument editid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-10296	A vulnerability was found in PHPGurukul Medical Card Generation System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/card-bwdates-reports-details.php of the component Report of Medical Card Page. The manipulation of the argument fromdate/todate leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-10041	A vulnerability was found in PAM. The secret information is stored in memory, where the attacker can trigger the victim program to execute by sending characters to its standard input (stdin). As this occurs, the attacker can train the branch predictor to execute an ROP chain speculatively. This flaw could result in leaked passwords, such as those found in /etc/shadow while performing authentications.	4.7	More Details
CVE-2024-44235	The issue was addressed with improved checks. This issue is fixed in iOS 18.1 and iPadOS 18.1. An attacker may be able to view restricted content from the lock screen.	4.6	More Details
CVE-2024-50579	In JetBrains YouTrack before 2024.3.47707 reflected XSS due to insecure link sanitization was possible	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44137	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sequoia 15, macOS Sonoma 14.7.1. An attacker with physical access may be able to share items from the lock screen.	4.6	More Details
CVE-2024-49762	Pterodactyl is a free, open-source game server management panel. When a user disables two-factor authentication via the Panel, a `DELETE` request with their current password in a query parameter will be sent. While query parameters are encrypted when using TLS, many webservers (including ones officially documented for use with Pterodactyl) will log query parameters in plain-text, storing a user's password in plain text. Prior to version 1.11.8, if a malicious user obtains access to these logs they could potentially authenticate against a user's account; assuming they are able to discover the account's email address or username separately. This problem has been patched in version 1.11.8. There are no workarounds at this time. There is not a direct vulnerability within the software as it relates to logs generated by intermediate components such as web servers or Layer 7 proxies. Updating to `v1.11.8` or adding the linked patch manually are the only ways to avoid this problem. As this vulnerability relates to historical logging of sensitive data, users who have ever disabled 2FA on a Panel (self-hosted or operated by a company) should change their passwords and consider enabling 2FA if it was left disabled. While it's unlikely that their account swill be compromised by this vulnerability, it's not impossible. Panel administrators should consider clearing any access logs that may contain sensitive data.	4.6	More Details
CVE-2024-44274	The issue was addressed with improved authentication. This issue is fixed in iOS 17.7.1 and iPadOS 17.7.1, watchOS 11.1, iOS 18.1 and iPadOS 18.1. An attacker with physical access to a locked device may be able to view sensitive user information.	4.6	More Details
CVE-2024-50581	In JetBrains YouTrack before 2024.3.47707 improper HTML sanitization could lead to XSS attack via comment tag	4.6	More Details
CVE-2024-50580	In JetBrains YouTrack before 2024.3.47707 multiple XSS were possible due to insecure markdown parsing and custom rendering rule	4.6	More Details
CVE-2024-50582	In JetBrains YouTrack before 2024.3.47707 stored XSS was possible due to improper HTML sanitization in markdown elements	4.6	More Details
CVE-2024-50577	In JetBrains YouTrack before 2024.3.47707 stored XSS was possible via Angular template injection in Hub settings	4.6	More Details
CVE-2024-46872	Mattermost versions 9.10.x <= 9.10.2, 9.11.x <= 9.11.1, 9.5.x <= 9.5.9 fail to sanitize user inputs in the frontend that are used for redirection which allows for a one-click client-side path traversal that is leading to CSRF in Playbooks	4.6	More Details
CVE-2024-50578	In JetBrains YouTrack before 2024.3.47707 stored XSS was possible via sprint value on agile boards page	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45477	Apache NiFi 1.10.0 through 1.27.0 and 2.0.0-M1 through 2.0.0-M3 support a description field for Parameters in a Parameter Context configuration that is vulnerable to cross-site scripting. An authenticated user, authorized to configure a Parameter Context, can enter arbitrary JavaScript code, which the client browser will execute within the session context of the authenticated user. Upgrading to Apache NiFi 1.28.0 or 2.0.0-M4 is the recommended mitigation.	4.6	More Details
CVE-2024-37846	MangoOS before 5.2.0 was discovered to contain a Client-Side Template Injection (CSTI) vulnerability via the Platform Management Edit page.	4.6	More Details
CVE-2024-50576	In JetBrains YouTrack before 2024.3.47707 stored XSS was possible via vendor URL in App manifest	4.6	More Details
CVE-2024-10372	A vulnerability classified as problematic was found in chidiwilliams buzz 1.1.0. This vulnerability affects the function download_model of the file buzz/model_loader.py. The manipulation leads to insecure temporary file. It is possible to launch the attack on the local host. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.5	More Details
CVE-2024-47028	In ffu_flash_pack of ffu.c, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	4.4	More Details
CVE-2024-44260	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious app with root privileges may be able to modify the contents of system files.	4.4	More Details
CVE-2024-10092	The Download Monitor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ajax_handle_api_key_actions function in all versions up to, and including, 5.0.12. This makes it possible for authenticated attackers, with Subscriber-level access and above, to revoke existing API keys and generate new ones.	4.3	More Details
CVE-2024-10437	The WPC Smart Messages for WooCommerce plugin for WordPress is vulnerable to unauthorized Smar Message activation/deactivation due to a missing capability check on the ajax_enable function in all versions up to, and including, 4.2.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to activate or deactivate smart messages.	4.3	More Details
CVE-2024-44244	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 18.1 and iPadOS 18.1, watchOS 11.1, visionOS 2.1, tvOS 18.1, macOS Sequoia 15.1, Safari 18.1. Processing maliciously crafted web content may lead to an unexpected process crash.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10045	The Transients Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.6. This is due to missing or incorrect nonce validation on the process_actions function. This makes it possible for unauthenticated attackers to delete transients 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-2024-9626	The Editorial Assistant by Sovrn plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ajax_zemanta_set_featured_image' function in versions up to, and including, 1.3.3. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload attachment files (such as jpg, png, txt, zip), and set the post featured image.	4.3	More Details
CVE-2024-9583	The RSS Aggregator – RSS Import, News Feeds, Feed to Post, and Autoblogging plugin for WordPress is vulnerable to unauthorized use of functionality due to a missing capability check on the wprss_ajax_send_premium_support function in all versions up to, and including, 4.23.12. This makes it possible for authenticated attackers, with Subscriber-level access and above, to send premium support requests with an attacker-controlled subject line and email address to support allowing them to impersonate the site owner. License information may also be leaked.	4.3	More Details
CVE-2024-10357	The Clever Addons for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.2.1 via the getTemplateContent function in src/widgets/class-clever-widget-base.php. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft template data.	4.3	More Details
CVE-2024-9531	The MultiVendorX – The Ultimate WooCommerce Multivendor Marketplace Solution plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'mvx_sent_deactivation_request' function in all versions up to, and including, 4.2.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to send a canned email to the site's administrator asking to delete the profile of an arbitrary vendor.	4.3	More Details
CVE-2024-50466	Cross-Site Request Forgery (CSRF) vulnerability in DarkMySite DarkMySite – Advanced Dark Mode Plugin for WordPress darkmysite allows Cross Site Request Forgery.This issue affects DarkMySite – Advanced Dark Mode Plugin for WordPress: from n/a through 1.2.8.	4.3	More Details
CVE-2024-47401	Mattermost versions 9.10.x <= 9.10.2, 9.11.x <= 9.11.1 and 9.5.x <= 9.5.9 fail to prevent detailed error messages from being displayed in Playbooks which allows an attacker to generate a large response and cause an amplified GraphQL response which in turn could cause the application to crash by sending a specially crafted request to Playbooks.	4.3	More Details
CVE-2024-50455	Missing Authorization vulnerability in The SEO Guys at SEOPress SEOPress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SEOPress: from n/a through 8.1.1.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20474	A vulnerability in Internet Key Exchange version 2 (IKEv2) processing of Cisco Secure Client Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) of Cisco Secure Client. This vulnerability is due to an integer underflow condition. An attacker could exploit this vulnerability by sending a crafted IKEv2 packet to an affected system. A successful exploit could allow the attacker to cause Cisco Secure Client Software to crash, resulting in a DoS condition on the client software. Note: Cisco Secure Client Software releases 4.10 and earlier were known as Cisco AnyConnect Secure Mobility Client.	4.3	More Details
CVE-2024-50428	Missing Authorization vulnerability in Mondula GmbH Multi Step Form allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Multi Step Form: from n/a through 1.7.21.	4.3	More Details
CVE-2024-10360	The Move Addons for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.3.5 via the render function in includes/widgets/accordion/widget.php, includes/widgets/remote-template/widget.php, and other widget.php files. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft template data.	4.3	More Details
CVE-2024-8667	The HurryTimer – An Scarcity and Urgency Countdown Timer for WordPress & WooCommerce plugin for WordPress is vulnerable to unauthorized post publication due to a missing capability check on the activateCampaign() function in all versions up to, and including, 2.10.0. This makes it possible for authenticated attackers, with contributor-level access and above, to publish arbitrary posts like ones they have submitted for review, or a site administrator has in draft.	4.3	More Details
CVE-2024-10448	A vulnerability, which was classified as problematic, has been found in code-projects Blood Bank Management System 1.0. Affected by this issue is some unknown functionality of the file /file/delete.php. The manipulation of the argument bid leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other endpoints might be affected as well.	4.3	More Details
CVE-2024-10050	The Elementor Header & Footer Builder plugin for WordPress is vulnerable to Information Disclosure in all versions up to, and including, 1.6.43 via the hfe_template shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to view the contents of Draft, Private and Password-protected posts they do not own.	4.3	More Details
CVE-2024-10241	Mattermost versions 9.5.x <= 9.5.9 fail to properly filter the channel data when ElasticSearch is enabled which allows a user to get private channel names by using cmd+K/ctrl+K.	4.3	More Details
CVE-2024-9530	The Qi Addons For Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.8.0 via private templates. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive data including the contents of templates that are private.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9109	The WooCommerce UPS Shipping – Live Rates and Access Points plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the delete_oauth_data function in all versions up to, and including, 2.3.11. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete the plugin's API key.	4.3	More Details
CVE-2024-50573	In JetBrains Hub before 2024.3.47707 improper access control allowed users to generate permanent tokens for unauthorized services	4.3	More Details
CVE-2024-10379	A vulnerability classified as problematic was found in ESAFENET CDG 5. Affected by this vulnerability is the function actionViewDecyptFile of the file /com/esafenet/servlet/client/DecryptApplicationService.java. The manipulation of the argument decryptFileId with the input ../../../Windows/System32/drivers/etc/hosts leads to path traversal: '../filedir'. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The affected function has a typo and is missing an R. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-8143	In the latest version (20240628) of gaizhenbiao/chuanhuchatgpt, an issue exists in the /file endpoint that allows authenticated users to access the chat history of other users. When a user logs in, a directory is created in the history folder with the user's name. By manipulating the /file endpoint, an authenticated user can enumerate and access files in other users' directories, leading to unauthorized access to private chat histories. This vulnerability can be exploited to read any user's private chat history.	4.3	More Details
CVE-2022-30359	OvalEdge 5.2.8.0 and earlier is affected by a Sensitive Data Exposure vulnerability via a GET request to /user/getUserList. Authentication is required. The information disclosed is associated with the all registered users, including user ID, status, email address, role(s), user type, license type, and personal details such as first name, last name, gender, and user preferences.	4.3	More Details
CVE-2024-48213	RockOA v2.6.5 is vulnerable to Directory Traversal in webmain/system/beifen/beifenAction.php.	4.3	More Details
CVE-2024-10312	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.7.4 via the render function in elements/tabs/tabs.php. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft template data.	4.3	More Details
CVE-2024-50052	Mattermost versions 9.10.x <= 9.10.2, 9.11.x <= 9.11.1, 9.5.x <= 9.5.9 fail to check that the origin of the message in an integration action matches with the original post metadata which allows an authenticated user to delete an arbitrary post.	4.3	More Details
CVE-2024-30124	HCL Sametime is impacted by insecure services in-use on the UIM client by default. An unused legacy REST service was enabled by default using the HTTP protocol. An attacker could potentially use this service endpoint maliciously.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10491	A vulnerability has been identified in the Express response.links function, allowing for arbitrary resource injection in the Link header when unsanitized data is used. The issue arises from improper sanitization in `Link` header values, which can allow a combination of characters like `,`, `;`, and `<>` to preload malicious resources. This vulnerability is especially relevant for dynamic parameters.	4.0	More Details
CVE-2024-10228	The Vagrant VMWare Utility Windows installer targeted a custom location with a non-protected path that could be modified by an unprivileged user, introducing potential for unauthorized file system writes. This vulnerability, CVE-2024-10228, was fixed in Vagrant VMWare Utility 1.0.23	3.8	More Details
CVE-2024-50610	GSL (GNU Scientific Library) through 2.8 has an integer signedness error in gsl_siman_solve_many in siman/siman.c. When params.n_tries is negative, incorrect memory allocation occurs.	3.6	More Details
CVE-2023-50355	HCL Sametime is impacted by the error messages containing sensitive information. An attacker can use this information to launch another, more focused attack.	3.6	More Details
CVE-2024-10214	Mattermost versions 9.11.X <= 9.11.1, 9.5.x <= 9.5.9 icorrectly issues two sessions when using desktop SSO - one in the browser and one in desktop with incorrect settings.	3.5	More Details
CVE-2024-30106	HCL Connections is vulnerable to an information disclosure vulnerability, due to an IBM WebSphere Application Server error, which could allow a user to obtain sensitive information they are not entitled to due to the improper handling of request data.	3.5	More Details
CVE-2024-10433	A vulnerability was found in Project Worlds Simple Web-Based Chat Application 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /index.php. The manipulation of the argument Name/Comment leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions different parameters to be affected which do not correlate with the screenshots of a successful attack.	3.5	More Details
CVE-2024-10276	A vulnerability has been found in Telestream Sentry 6.0.9 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /?page=reports of the component Reports Page. The manipulation of the argument z leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-10348	A vulnerability was found in SourceCodester Best House Rental Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /index.php?page=tenants of the component Manage Tenant Details. The manipulation of the argument Last Name/First Name/Middle Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only shows the field "Last Name" to be affected. Other fields might be affected as well.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10412	A vulnerability was found in Poco-z Guns-Medical 1.0. It has been declared as problematic. Affected by this vulnerability is the function upload of the file /mgr/upload of the component File Upload. The manipulation of the argument picture leads to cross site scripting. The attack can be launched remotely.	3.5	More Details
CVE-2024-10419	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /bloodrequest.php. The manipulation of the argument msg leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-40792	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. A malicious app may be able to change network settings.	3.3	More Details
CVE-2024-40853	This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 18 and iPadOS 18. An attacker may be able to use Siri to enable Auto-Answer Calls.	3.3	More Details
CVE-2024-44222	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to read sensitive location information.	3.3	More Details
CVE-2024-27849	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sequoia 15. An app may be able to read sensitive location information.	3.3	More Details
CVE-2024-49755	Duende IdentityServer is an OpenID Connect and OAuth 2.x framework for ASP.NET Core. IdentityServer's local API authentication handler performs insufficient validation of the cnf claim in DPoP access tokens. This allows an attacker to use leaked DPoP access tokens at local api endpoints even without possessing the private key for signing proof tokens. Note that this only impacts custom endpoints within an IdentityServer implementation that have explicitly used the LocalApiAuthenticationHandler for authentication. This vulnerability is patched in IdentityServer 7.0.8. Version 6.3 and below are unaffected, as they do not support DPoP in Local APIs.	3.1	More Details
CVE-2024-47483	Dell Data Lakehouse, version(s) 1.0.0.0 and 1.1.0.0, contain(s) an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2.9	More Details
CVE-2024-48921	Kyverno is a policy engine designed for Kubernetes. A kyverno ClusterPolicy, ie. "disallow-privileged-containers," can be overridden by the creation of a PolicyException in a random namespace. By design, PolicyExceptions are consumed from any namespace. Administrators may not recognize that this allows users with privileges to non-kyverno namespaces to create exceptions. This vulnerability is fixed in 1.13.0.	2.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41156	Profile files from TRO600 series radios are extracted in plain-text and encrypted file formats. Profile files provide potential attackers valuable configuration information about the Tropos network. Profiles can only be exported by authenticated users with higher privilege of write access.	2.7	More Details
CVE-2024-10478	A vulnerability, which was classified as problematic, has been found in LinZhaoguan pb-cms up to 2.0.1. This issue affects some unknown processing of the file /admin#article/edit?id=2 of the component Edit Article Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2024-44265	The issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An attacker with physical access can input Game Controller events to apps running on a locked device.	2.4	More Details
CVE-2024-44251	This issue was addressed through improved state management. This issue is fixed in iOS 18.1 and iPadOS 18.1. An attacker may be able to view restricted content from the lock screen.	2.4	More Details
CVE-2024-10477	A vulnerability classified as problematic was found in LinZhaoguan pb-cms up to 2.0.1. This vulnerability affects unknown code of the file /admin#permissions of the component Permission Management Page. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2024-40851	This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 18.1 and iPadOS 18.1. An attacker with physical access may be able to access contact photos from the lock screen.	2.4	More Details
CVE-2024-10479	A vulnerability, which was classified as problematic, was found in LinZhaoguan pb-cms up to 2.0.1. Affected is an unknown function of the file /admin#themes of the component Theme Management Module. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2024-10414	A vulnerability, which was classified as problematic, was found in PHPGurukul Vehicle Record System 1.0. This affects an unknown part of the file /admin/edit-brand.php. The manipulation of the argument Brand Name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions the parameter "phone_number" to be affected. But this might be a mistake because the textbox field label is "Brand Name".	2.4	More Details
CVE-2024-44123	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15, iOS 18 and iPadOS 18. A malicious app with root privileges may be able to access keyboard input and location information without user consent.	2.3	More Details
CVE-2024-10452	Organization admins can delete pending invites created in an organization they are not part of.	2.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8013	A bug in query analysis of certain complex self-referential $lookup subpipelines may result in literal values in expressions for encrypted fields to be sent to the server as plaintext instead of ciphertext. Should this occur, no documents would be returned or written. This issue affects mongocryptd binary (v5.0 versions prior to 5.0.29, v6.0 versions prior to 6.0.17, v7.0 versions prior to 7.0.12 and v7.3 versions prior to 7.3.4) and mongo_crypt_v1.so shared libraries (v6.0 versions prior to 6.0.17, v7.0 versions prior to 7.0.12 and v7.3 versions prior to 7.3.4) released alongside MongoDB Enterprise Server versions.	2.2	More Details
CVE-2024-23843	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Genians Genian NAC V5.0, Genians Genian NAC LTS V5.0.This issue affects Genian NAC V5.0: from V5.0.0 through V5.0.60; Genian NAC LTS V5.0: from 5.0.0 LTS through 5.0.55 LTS(Revision 125558), from 5.0.0 LTS through 5.0.56 LTS(Revision 125560).	2.2	More Details
CVE-2024-48572	A User enumeration vulnerability in AquilaCMS 1.409.20 and prior allows unauthenticated attackers to obtain email addresses via the "Add a user" feature. The vulnerability occurs due to insufficiently validated user input being processed as a regular expression, which is then matched against email addresses to find duplicate entries.	N/A	More Details
CVE-2020-26310	Validate.js provides a declarative way of validating javascript objects. All versions as of 30 November 2020 contain one or more regular expressions that are vulnerable to Regular Expression Denial of Service (ReDoS). As of time of publication, it is unknown if any patches are available.	N/A	More Details
CVE-2024-5532	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in OpenText™ Operations Agent. The XSS vulnerability could allow an attacker with local admin permissions to manipulate the content of the internal status page of the Agent on the local system. This issue affects Operations Agent: 12.20, 12.21, 12.22, 12.23, 12.24, 12.25, 12.26.	N/A	More Details
CVE-2020-26309	Validate.js provides a declarative way of validating javascript objects. Versions 0.11.3 and prior contain one or more regular expressions that are vulnerable to Regular Expression Denial of Service (ReDoS). As of time of publication, it is unknown if any patches are available.	N/A	More Details
CVE-2024-9949	Denial of Service in Forescout SecureConnector 11.1.02.1019 on Windows allows Unprivileged user to corrupt the configuration file and cause Denial of Service in the application.	N/A	More Details
CVE-2024-49751	Press, a Frappe custom app that runs Frappe Cloud, manages infrastructure, subscription, marketplace, and software-as-a-service (SaaS). Prior to commit 5d118a902872d7941f099ad1fb918e2421e79ccd, a user could inject HTML through SaaS signup inputs. The user who injected the unsafe HTML code would only affect themselves and would not affect other users. Commit 5d118a902872d7941f099ad1fb918e2421e79ccd patches this bug.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26308	Validate.js provides a declarative way of validating javascript objects. Versions 0.13.1 and prior contain one or more regular expressions that are vulnerable to Regular Expression Denial of Service (ReDoS). As of time of publication, no known patches are available.	N/A	More Details
CVE-2020-26307	HTML2Markdown is a Javascript implementation for converting HTML to Markdown text. All available versions contain one or more regular expressions that are vulnerable to Regular Expression Denial of Service (ReDoS). As of time of publication, no known patches are available.	N/A	More Details
CVE-2020-26306	Knwl.js is a Javascript library that parses through text for dates, times, phone numbers, emails, places, and more. Versions 1.0.2 and prior contain one or more regular expressions that are vulnerable to Regular Expression Denial of Service (ReDoS). As of time of publication, no known patches are available.	N/A	More Details
CVE-2024-49766	Werkzeug is a Web Server Gateway Interface web application library. On Python < 3.11 on Windows, os.path.isabs() does not catch UNC paths like //server/share. Werkzeug's safe_join() relies on this check, and so can produce a path that is not safe, potentially allowing unintended access to data. Applications using Python >= 3.11, or not using Windows, are not vulnerable. Werkzeug version 3.0.6 contains a patch.	N/A	More Details
CVE-2024-49380	Plenti, a static site generator, has an arbitrary file write vulnerability in versions prior to 0.7.2. The `/postLocal` endpoint is vulnerable to an arbitrary file write vulnerability when a plenti user serves their website. This issue may lead to Remote Code Execution. Version 0.7.2 fixes the vulnerability.	N/A	More Details
CVE-2024-9692	VIMESA VHF/FM Transmitter Blue Plus is suffering from a Denial-of-Service (DoS) vulnerability. An unauthenticated attacker can issue an unauthorized HTTP GET request to the unprotected endpoint 'doreboot' and restart the transmitter operations.	N/A	More Details
CVE-2024-9899	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-2143. Reason: This candidate is a reservation duplicate of CVE-2023-2143. Notes: All CVE users should reference CVE-2023-2143 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-9991	This vulnerability exists in Philips lighting devices due to storage of Wi-Fi credentials in plain text within the device firmware. An attacker with physical access could exploit this by extracting the firmware and analyzing the binary data to obtain the plaintext Wi-Fi credentials stored on the vulnerable device. Successful exploitation of this vulnerability could allow an attacker to gain unauthorized access to the Wi-Fi network to which vulnerable device is connected.	N/A	More Details