SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 02 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-2024-8940	Vulnerability in the Scriptcase application version 9.4.019, which involves the arbitrary upload of a file via /scriptcase/devel/lib/third/jquery_plugin/jQuery-File-Upload/server/php/ via a POST request. An attacker could upload malicious files to the server due to the application not properly verifying user input.	10.0	More Details
CVE-2024-43693	A specially crafted POST request to the ProGauge MAGLINK LX CONSOLE UTILITY sub-menu can allow a remote attacker to inject arbitrary commands.	10.0	More Details
CVE-2024-45066	A specially crafted POST request to the ProGauge MAGLINK LX CONSOLE IP sub-menu can allow a remote attacker to inject arbitrary commands.	10.0	More Details
CVE-2024-8353	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.16.1 via deserialization of untrusted input via several parameters like 'give_title' and 'card_address'. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain allows attackers to delete arbitrary files and achieve remote code execution. This is essentially the same vulnerability as CVE-2024-5932, however, it was discovered the the presence of stripslashes_deep on user_info allows the is_serialized check to be bypassed. This issue was mostly patched in 3.16.1, but further hardening was added in 3.16.2.	10.0	More Details
CVE-2024-42017	An issue was discovered in Atos Eviden iCare 2.7.1 through 2.7.11. The application exposes a web interface locally. In the worst-case scenario, if the application is remotely accessible, it allows an attacker to execute arbitrary commands with system privilege on the endpoint hosting the application, without any authentication.	10.0	More Details
CVE-2024-8621	The Daily Prayer Time plugin for WordPress is vulnerable to SQL Injection via the 'max_word' attribute of the 'quran_verse' shortcode in all versions up to, and including, 2024.08.26 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 access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.9	More Details
CVE-2024-8436	The WP Easy Gallery – WordPress Gallery Plugin plugin for WordPress is vulnerable to SQL Injection via the 'edit_imageId' and 'edit_imageDelete' parameters in all versions up to, and including, 4.8.5 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 subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26686	File Upload vulnerability in CS-Cart MultiVendor 4.16.1 allows remote attackers to run arbitrary code via the image upload feature when customizing a shop.	9.8	More Details
CVE-2024-8607	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Oceanic Software ValeApp allows SQL Injection.This issue affects ValeApp: before v2.0.0.	9.8	More Details
CVE-2024-8643	Session Fixation vulnerability in Oceanic Software ValeApp allows Brute Force, Session Hijacking.This issue affects ValeApp: before v2.0.0.	9.8	More Details
CVE-2024-6981	OMNTEC Proteus Tank Monitoring OEL8000III Series could allow an attacker to perform administrative actions without proper authentication.	9.8	More Details
CVE-2024-8310	OPW Fuel Management Systems SiteSentinel could allow an attacker to bypass authentication to the server and obtain full admin privileges.	9.8	More Details
CVE-2024-46256	A Command injection vulnerability in requestLetsEncryptSsl in NginxProxyManager 2.11.3 allows an attacker to RCE via Add Let's Encrypt Certificate.	9.8	More Details
CVE-2024-8456	Certain switch models from PLANET Technology lack proper access control in firmware upload and download functionality, allowing unauthenticated remote attackers to download and upload firmware and system configurations, ultimately gaining full control of the devices.	9.8	More Details
CVE-2024-46293	Sourcecodester Online Medicine Ordering System 1.0 is vulnerable to Incorrect Access Control. There is a lack of authorization checks for admin operations. Specifically, an attacker can perform admin-level actions without possessing a valid session token. The application does not verify whether the user is logged in as an admin or even check for a session token at all.	9.8	More Details
CVE-2024-9106	The Wechat Social login plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 1.3.0. This is due to insufficient verification on the user being supplied during the social login. 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 user id. This is only exploitable if the app secret is not set, so it has a default empty value.	9.8	More Details
CVE-2023-26689	An issue discovered in CS-Cart MultiVendor 4.16.1 allows attackers to alter arbitrary user account profiles via crafted post request.	9.8	More Details
CVE-2024-9108	The Wechat Social login plugin for WordPress is vulnerable to arbitrary file uploads due to insufficient file type validation in the 'convert_remoteimage_to_local' function in versions up to, and including, 1.3.0. 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-2024-9265	The Echo RSS Feed Post Generator plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 5.4.6. This is due to the plugin not properly restricting the roles that can set during registration through the echo_check_post_header_sent() function. This makes it possible for unauthenticated attackers to register as an administrator.	9.8	More Details
CVE-2024-9289	The WordPress & WooCommerce Affiliate Program plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 8.4.1. This is due to the rtwwwap_login_request_callback() function not properly validating a user's identity prior to authenticating them to the site. This makes it possible for unauthenticated attackers to log in as any user, including administrators, granted they have access to the administrator's email.	9.8	More Details
CVE-2024-41276	A vulnerability in Kaiten version 57.131.12 and earlier allows attackers to bypass the PIN code authentication mechanism. The application requires users to input a 6-digit PIN code sent to their email for authorization after entering their login credentials. However, the request limiting mechanism can be easily bypassed, enabling attackers to perform a brute force attack to guess the correct PIN and gain unauthorized access to the application.	9.8	More Details
CVE-2024-9392	A compromised content process could have allowed for the arbitrary loading of cross-origin pages. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9401	Memory safety bugs present in Firefox 130, Firefox ESR 115.15, Firefox ESR 128.2, and Thunderbird 128.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131.	9.8	More Details
CVE-2024-9402	Memory safety bugs present in Firefox 130, Firefox ESR 128.2, and Thunderbird 128.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	9.8	More Details
CVE-2024-47608	Logicytics is designed to harvest and collect data for forensic analysis. Logicytics has a basic vuln affecting compromised devices from shell injections. This vulnerability is fixed in 2.3.2.	9.8	More Details
CVE-2024-46628	Tenda G3 Router firmware v15.03.05.05 was discovered to contain a remote code execution (RCE) vulnerability via the usbPartitionName parameter in the formSetUSBPartitionUmount function.	9.8	More Details
CVE-2024-7108	Incorrect Authorization vulnerability in National Keep Cyber Security Services CyberMath allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects CyberMath: before CYBM.240816253.	9.8	More Details
CVE-2024-45999	A SQL Injection vulnerability was discovered in Cloudlog 2.6.15, specifically within the get_station_info()function located in the file /application/models/Oqrs_model.php. The vulnerability is exploitable via the station_id parameter.	9.8	More Details
CVE-2024-8878	The password recovery mechanism for the forgotten password in Riello Netman 204 allows an attacker to reset the admin password and take over control of the device.This issue affects Netman 204: through 4.05.	9.8	More Details
CVE-2024-7772	The Jupiter X Core plugin for WordPress is vulnerable to arbitrary file uploads due to a mishandled file type validation in the 'validate' function in all versions up to, and including, 4.6.5. 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-2024-42505	Command injection vulnerabilities in the underlying CLI service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2024-42506	Command injection vulnerabilities in the underlying CLI service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2024-42507	Command injection vulnerabilities in the underlying CLI service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2024-42797	An Incorrect Access Control vulnerability was found in /music/ajax.php?action=delete_playlist in Kashipara Music Management System v1.0. This vulnerability allows an unauthenticated attacker to delete the valid music playlist entries.	9.8	More Details
CVE-2024-43423	The web application for ProGauge MAGLINK LX4 CONSOLE contains an administrative-level user account with a password that cannot be changed.	9.8	More Details
CVE-2024-8275	The The Events Calendar plugin for WordPress is vulnerable to SQL Injection via the 'order' parameter of the 'tribe_has_next_event' function in all versions up to, and including, 6.6.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database. Only sites that have manually added tribe_has_next_event() will be vulnerable to this SQL injection.	9.8	More Details
CVE-2024-43692	An attacker can directly request the ProGauge MAGLINK LX CONSOLE resource sub page with full privileges by requesting the URL directly.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46612	IceCMS v3.4.7 and before was discovered to contain a hardcoded JWT key, allowing an attacker to forge JWT authentication information.	9.8	More Details
CVE-2024-46957	Mellium mellium.im/xmpp 0.0.1 through 0.21.4 allows response spoofing if the implementation uses predictable IDs because the stanza type is not checked. This is fixed in 0.22.0.	9.8	More Details
CVE-2024-8485	The REST API TO MiniProgram plugin for WordPress is vulnerable to privilege escalation via account takeovr in all versions up to, and including, 4.7.1 via the updateUserInfo() due to missing validation on the 'openid' user controlled key that determines what user will be updated. This makes it possible for unauthenticated attackers to update arbitrary user's accounts, including their email to a @weixin.com email, which can the be leveraged to reset the password of the user's account, including administrators.	9.8	More Details
CVE-2024-8877	Improper neutralization of special elements results in a SQL Injection vulnerability in Riello Netman 204. It is only limited to the SQLite database of measurement data.This issue affects Netman 204: through 4.05.	9.8	More Details
CVE-2024-9142	External Control of File Name or Path, : Incorrect Permission Assignment for Critical Resource vulnerability in Olgu Computer Systems e-Belediye allows Manipulating Web Input to File System Calls.This issue affects e-Belediye: before 2.0.642.	9.8	More Details
CVE-2024-9148	Flowise < 2.1.1 suffers from a Stored Cross-Site vulnerability due to a lack of input sanitization in Flowise Chat Embed < 2.0.0.	9.6	More Details
CVE-2024-46367	A Stored Cross-Site Scripting (XSS) vulnerability in Webkul Krayin CRM 1.3.0 allows remote attackers to inject arbitrary JavaScript code by submitting a malicious payload within the username field. This can lead to privilege escalation when the payload is executed, granting the attacker elevated permissions within the CRM system.	9.6	More Details
CVE-2024-8630	Alisonic Sibylla devices are vulnerable to SQL injection attacks, which could allow complete access to the database.	9.4	More Details
CVE-2024-46627	Incorrect access control in BECN DATAGERRY v2.2 allows attackers to execute arbitrary commands via crafted web requests.	9.1	More Details
CVE-2024-7385	The WordPress Simple HTML Sitemap plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 3.1 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 Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.1	More Details
CVE-2024-8514	The Prisna GWT – Google Website Translator plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.4.11 via deserialization of untrusted input from the 'prisna_import' parameter. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	9.1	More Details
CVE-2024-6592	Incorrect Authorization vulnerability in the protocol communication between the WatchGuard Authentication Gateway (aka Single Sign-On Agent) on Windows and the WatchGuard Single Sign-On Client on Windows and MacOS allows Authentication Bypass.This issue affects the Authentication Gateway: through 12.10.2; Windows Single Sign-On Client: through 12.7; MacOS Single Sign-On Client: through 12.5.4.	9.1	More Details
CVE-2024-6593	Incorrect Authorization vulnerability in WatchGuard Authentication Gateway (aka Single Sign-On Agent) on Windows allows an attacker with network access to execute restricted management commands. This issue affects Authentication Gateway: through 12.10.2.	9.1	More Details
CVE-2024-25660	The WebDAV service in Infinera TNMS (Transcend Network Management System) 19.10.3 allows a low-privileged remote attacker to conduct unauthorized file operations, because of execution with unnecessary privileges.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47070	authentik is an open-source identity provider. A vulnerability that exists in versions prior to 2024.8.3 and 2024.6.5 allows bypassing password login by adding X-Forwarded-For header with an unparsable IP address, e.g. `a`. This results in a possibility of logging into any account with a known login or email address. The vulnerability requires the authentik instance to trust X-Forwarded-For header provided by the attacker, thus it is not reproducible from external hosts on a properly configured environment. The issue occurs due to the password stage having a policy bound to it, which skips the password stage if the Identification stage is setup to also contain a password stage. Due to the invalid X-Forwarded-For header, which does not get validated to be an IP Address early enough, the exception happens later and the policy fails. The default blueprint doesn't correctly set `failure_result` to `True` on the policy binding meaning that due to this exception the policy returns false and the password stage is skipped. Versions 2024.8.3 and 2024.6.5 fix this issue.	9.0	More Details
CVE-2024-47177	CUPS is a standards-based, open-source printing system, and cups-filters provides backends, filters, and other software for CUPS 2.x to use on non-Mac OS systems. Any value passed to `FoomaticRIPCommandLine` via a PPD file will be executed as a user controlled command. When combined with other logic bugs as described in CVE_2024-47176, this can lead to remote command execution.	9.0	More Details
CVE-2024-0132	NVIDIA Container Toolkit 1.16.1 or earlier contains a Time-of-check Time-of-Use (TOCTOU) vulnerability when used with default configuration where a specifically crafted container image may gain access to the host file system. This does not impact use cases where CDI is used. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-7481	Improper verification of cryptographic signature during installation of a Printer driver via the TeamViewer_service.exe component of TeamViewer Remote Clients prior version 15.58.4 for Windows allows an attacker with local unprivileged access on a Windows system to elevate their privileges and install drivers.	8.8	More Details
CVE-2024-8448	Certain switch models from PLANET Technology have a hard-coded credential in the specific command-line interface, allowing remote attackers with regular privilege to log in with this credential and obtain a Linux root shell.	8.8	More Details
CVE-2024-45981	A host header injection vulnerability in BookReviewLibrary 1.0 allows attackers to obtain the password reset token via user interaction with a crafted password reset link.	8.8	More Details
CVE-2024-9120	Use after free in Dawn in Google Chrome on Windows prior to 129.0.6668.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-9121	Inappropriate implementation in V8 in Google Chrome prior to 129.0.6668.70 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-9122	Type Confusion in V8 in Google Chrome prior to 129.0.6668.70 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-9123	Integer overflow in Skia in Google Chrome prior to 129.0.6668.70 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-7479	Improper verification of cryptographic signature during installation of a VPN driver via the TeamViewer_service.exe component of TeamViewer Remote Clients prior version 15.58.4 for Windows allows an attacker with local unprivileged access on a Windows system to elevate their privileges and install drivers.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28812	An issue was discovered in Infinera hiT 7300 5.60.50. A hidden SSH service (on the local management network interface) with hardcoded credentials allows attackers to access the appliance operating system (with highest privileges) via an SSH connection.	8.8	More Details
CVE-2024-28809	An issue was discovered in Infinera hiT 7300 5.60.50. Cleartext storage of sensitive password in firmware update packages allows attackers to access various appliance services via hardcoded credentials.	8.8	More Details
CVE-2024-45982	A host header injection vulnerability in scheduleR v0.0.18 allows attackers to obtain the password reset token via user interaction with a crafted password reset link. This allows attackers to arbitrarily reset other users' passwords and compromise their accounts.	8.8	More Details
CVE-2024-46280	PIX-LINK LV-WR22 RE3002-P1-01_V117.0 is vulnerable to Improper Access Control. The TELNET service is enabled with weak credentials for a root-level account, without the possibility of changing them.	8.8	More Details
CVE-2024-8458	Certain switch models from PLANET Technology have a web application that is vulnerable to Cross-Site Request Forgery (CSRF). An unauthenticated remote attacker can trick a user into visiting a malicious website, allowing the attacker to impersonate the user and perform actions on their behalf, such as creating accounts.	8.8	More Details
CVE-2024-47180	Shields.io is a service for concise, consistent, and legible badges in SVG and raster format. Shields.io and users self-hosting their own instance of shields using version < `server-2024-09-25` are vulnerable to a remote execution vulnerability via the JSONPath library used by the Dynamic JSON/Toml/Yaml badges. This vulnerability would allow any user with access to make a request to a URL on the instance to the ability to execute code by crafting a malicious JSONPath expression. All users who self-host an instance are vulnerable. This problem was fixed in server-2024-09-25. Those who follow the tagged releases should update to `server-2024-09-25` or later. Those who follow the rolling tag on DockerHub, `docker pull shieldsio/shields:next` to update to the latest version. As a workaround, blocking access to the endpoints `/badge/dynamic/json`, `/badge/dynamic/toml`, and `/badge/dynamic/yaml` (e.g: via a firewall or reverse proxy in front of your instance) would prevent the exploitable endpoints from being accessed.	8.8	More Details
CVE-2024-8290	The WCFM – Frontend Manager for WooCommerce along with Bookings Subscription Listings Compatible plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 6.7.12 via the WCFM_Customers_Manage_Controller::processing function due to missing validation on the ID user controlled key. This makes it possible for authenticated attackers, with subscriber/customer-level access and above, to change the email address of administrator user accounts which allows them to reset the password and access the administrator account.	8.8	More Details
CVE-2024-47130	The goTenna Pro App allows unauthenticated attackers to remotely update the local public keys used for P2P and group messages. It is advised to update your app to the current release for enhanced encryption protocols.	8.8	More Details
CVE-2024-47169	Agnai is an artificial-intelligence-agnostic multi-user, mult-bot roleplaying chat system. A vulnerability in versions prior to 1.0.330 permits attackers to upload arbitrary files to attacker-chosen locations on the server, including JavaScript, enabling the execution of commands within those files. This issue could result in unauthorized access, full server compromise, data leakage, and other critical security threats. This does not affect `agnai.chat`, installations using S3-compatible storage, or self-hosting that is not publicly exposed. This does affect publicly hosted installs without S3-compatible storage. Version 1.0.330 fixes this vulnerability.	8.8	More Details
CVE-2024-7149	The Event Manager, Events Calendar, Tickets, Registrations – Eventin plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 4.0.8 via multiple style parameters. This makes it possible for authenticated attackers, with Contributor-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-2024-23923	Alpine Halo9 prh_l2_sar_data_ind Use-After-Free Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Alpine Halo9 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the prh_l2_sar_data_ind function. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-22945	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23957	Autel MaxiCharger AC Elite Business C50 DLB_HostHeartBeat Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Autel MaxiCharger AC Elite Business C50 charging stations. Authentication is not required to exploit this vulnerability. The specific flaw exists within the DLB_HostHeartBeat handler of the DLB protocol implementation. When parsing an AES key, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-23241	8.8	More Details
CVE-2024-23938	Silicon Labs Gecko OS Debug Interface Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Silicon Labs Gecko OS. Authentication is not required to exploit this vulnerability. The specific flaw exists within the debug interface. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-23184	8.8	More Details
CVE-2024-33369	Directory Traversal vulnerability in Plasmoapp RPShare Fabric mod v.1.0.0 allows a remote attacker to execute arbitrary code via the getFileNameFromConnection method in DownloadTask	8.8	More Details
CVE-2024-33368	An issue in Plasmoapp RPShare Fabric mod v.1.0.0 allows a remote attacker to execute arbitrary code via the build method in DonwloadPromptScreen	8.8	More Details
CVE-2024-47179	RSSHub is an RSS network. Prior to commit 64e00e7, RSSHub's `docker-test-cont.yml` workflow is vulnerable to Artifact Poisoning, which could have lead to a full repository takeover. Downstream users of RSSHub are not vulnerable to this issue, and commit 64e00e7 fixed the underlying issue and made the repository no longer vulnerable. The `docker-test-cont.yml` workflow gets triggered when the `PR - Docker build test` workflow completes successfully. It then collects some information about the Pull Request that triggered the triggering workflow and set some labels depending on the PR body and sender. If the PR also contains a `routes` markdown block, it will set the `TEST_CONTINUE` environment variable to `true`. The workflow then downloads and extracts an artifact uploaded by the triggering workflow which is expected to contain a single `rsshub.tar.zst` file. However, prior to commit 64e00e7, it did not validate and the contents were extracted in the root of the workspace overriding any existing files. Since the contents of the artifact were not validated, it is possible for a malicious actor to send a Pull Request which uploads, not just the `rsshub.tar.zst` compressed docker image, but also a malicious `package.json` file with a script to run arbitrary code in the context of the privileged workflow. As of commit 64e00e7, this scenario has been addressed and the RSSHub repository is no longer vulnerable.	8.8	More Details
CVE-2024-38308	Advantech ADAM 5550's web application includes a "logs" page where all the HTTP requests received are displayed to the user. The device doesn't correctly neutralize malicious code when parsing HTTP requests to generate page output.	8.8	More Details
CVE-2024-46489	A remote command execution (RCE) vulnerability in promptr v6.0.7 allows attackers to execute arbitrary commands via a crafted URL.	8.8	More Details
CVE-2024-45980	A host header injection vulnerability in MEANStore 1.0 allows attackers to obtain the password reset token via user interaction with a crafted password reset link. This allows attackers to arbitrarily reset other users' passwords and compromise their accounts.	8.8	More Details
CVE-2024-45979	A host header injection vulnerability in Lines Police CAD 1.0 allows attackers to obtain the password reset token via user interaction with a crafted password reset link. This allows attackers to arbitrarily reset other users' passwords and compromise their accounts.	8.8	More Details
CVE-2024-46366	A Client-side Template Injection (CSTI) vulnerability in Webkul Krayin CRM 1.3.0 allows remote attackers to execute arbitrary client-side template code by injecting a malicious payload during the lead creation process. This can lead to privilege escalation when the payload is executed, granting the attacker elevated permissions within the CRM system.	8.8	More Details
CVE-2024-46441	An arbitrary file upload vulnerability in YPay 1.2.0 allows attackers to execute arbitrary code via a ZIP archive to themePutFile in app/common/util/Upload.php (called from app/admin/controller/ypay/Home.php). The file extension of an uncompressed file is not checked.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9400	A potential memory corruption vulnerability could be triggered if an attacker had the ability to trigger an OOM at a specific moment during JIT compilation. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	8.8	More Details
CVE-2024-9396	It is currently unknown if this issue is exploitable but a condition may arise where the structured clone of certain objects could lead to memory corruption. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	8.8	More Details
CVE-2024-41725	ProGauge MAGLINK LX CONSOLE does not have sufficient filtering on input fields that are used to render pages which may allow cross site scripting.	8.8	More Details
CVE-2024-45373	Once logged in to ProGauge MAGLINK LX4 CONSOLE, a valid user can change their privileges to administrator.	8.8	More Details
CVE-2023-26687	Directory Traversal vulnerability in CS-Cart MultiVendor 4.16.1 allows remote attackers to obtain sensitive information via the product_data parameter in the PDF Add-on.	8.8	More Details
CVE-2024-8922	The Product Enquiry for WooCommerce, WooCommerce product catalog plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.2.33.32 via deserialization of untrusted input in enquiry_detail.php. This makes it possible for authenticated attackers, with Author-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details
CVE-2023-26690	File Upload vulnerability in CS-Cart MultiVendor 4.16.1 allows remote attackers to run arbitrary code via File Manager/Editor component in the vendor or admin menu.	8.8	More Details
CVE-2024-7432	The Unseen Blog theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.0.0 via deserialization of untrusted input. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details
CVE-2024-9018	The WP Easy Gallery – WordPress Gallery Plugin plugin for WordPress is vulnerable to time-based SQL Injection via the 'key' parameter in all versions up to, and including, 4.8.5 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 access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2024-7433	The Empowerment theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.0.2 via deserialization of untrusted input. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details
CVE-2024-7434	The UltraPress theme for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.2.1 via deserialization of untrusted input. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details
CVE-2024-20436	A vulnerability in the HTTP Server feature of Cisco IOS XE Software when the Telephony Service feature is enabled could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to a null pointer dereference when accessing specific URLs. An attacker could exploit this vulnerability by sending crafted HTTP traffic to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, causing a DoS condition on the affected device.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8450	Certain switch models from PLANET Technology have a Hard-coded community string in the SNMPv1 service, allowing unauthorized remote attackers to use this community string to access the SNMPv1 service with read-write privileges.	8.6	More Details
CVE-2024-20433	A vulnerability in the Resource Reservation Protocol (RSVP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to a buffer overflow when processing crafted RSVP packets. An attacker could exploit this vulnerability by sending RSVP traffic to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	8.6	More Details
CVE-2024-46472	CodeAstro Membership Management System 1.0 is vulnerable to SQL Injection via the parameter 'email' in the Login Page.	8.6	More Details
CVE-2024-25632	eLabFTW is an open source electronic lab notebook for research labs. In the context of eLabFTW, an administrator is a user account with certain privileges to manage users and content in their assigned team/teams. A user may be an administrator in one team and a regular user in another. The vulnerability allows a regular user to become administrator of a team where they are a member, under a reasonable configuration. Additionally, in eLabFTW versions subsequent to v5.0.0, the vulnerability may allow an initially unauthenticated user to gain administrative privileges over an arbitrary team. The vulnerability does not affect system administrator status. Users should upgrade to version 5.1.0. System administrators are advised to turn off local user registration, saml_team_create and not allow administrators to import users into teams, unless strictly required.	8.6	More Details
CVE-2024-20480	A vulnerability in the DHCP Snooping feature of Cisco IOS XE Software on Software-Defined Access (SD-Access) fabric edge nodes could allow an unauthenticated, remote attacker to cause high CPU utilization on an affected device, resulting in a denial of service (DoS) condition that requires a manual reload to recover. This vulnerability is due to improper handling of IPv4 DHCP packets. An attacker could exploit this vulnerability by sending certain IPv4 DHCP packets to an affected device. A successful exploit could allow the attacker to cause the device to exhaust CPU resources and stop processing traffic, resulting in a DoS condition that requires a manual reload to recover.	8.6	More Details
CVE-2024-47076	CUPS is a standards-based, open-source printing system, and `libcupsfilters` contains the code of the filters of the former `cups-filters` package as library functions to be used for the data format conversion tasks needed in Printer Applications. The `cfGetPrinterAttributes5` function in `libcupsfilters` does not sanitize IPP attributes returned from an IPP server. When these IPP attributes are used, for instance, to generate a PPD file, this can lead to attacker controlled data to be provided to the rest of the CUPS system.	8.6	More Details
CVE-2024-47175	CUPS is a standards-based, open-source printing system, and `libppd` can be used for legacy PPD file support. The `libppd` function `ppdCreatePPDFromIPP2` does not sanitize IPP attributes when creating the PPD buffer. When used in combination with other functions such as `cfGetPrinterAttributes5`, can result in user controlled input and ultimately code execution via Foomatic. This vulnerability can be part of an exploit chain leading to remote code execution (RCE), as described in CVE-2024-47176.	8.6	More Details
CVE-2024-20467	A vulnerability in the implementation of the IPv4 fragmentation reassembly code in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper management of resources during fragment reassembly. An attacker could exploit this vulnerability by sending specific sizes of fragmented packets to an affected device or through a Virtual Fragmentation Reassembly (VFR)-enabled interface on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: This vulnerability affects Cisco ASR 1000 Series Aggregation Services Routers and Cisco cBR-8 Converged Broadband Routers if they are running Cisco IOS XE Software Release 17.12.1 or 17.12.1a.	8.6	More Details
CVE-2024-30128	HCL Nomad server on Domino is affected by an open proxy vulnerability in which an unauthenticated attacker can mask their original source IP address. This may enable an attacker to trick the user into exposing sensitive information.	8.6	More Details
CVE-2024-20464	A vulnerability in the Protocol Independent Multicast (PIM) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of received IPv4 PIMv2 packets. An attacker could exploit this vulnerability by sending a crafted PIMv2 packet to a PIM-enabled interface on an affected device. A successful exploit could allow the attacker to cause an affected device to reload, resulting in a DoS condition. Note: This vulnerability can be exploited with either an IPv4 multicast or unicast packet.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20455	A vulnerability in the process that classifies traffic that is going to the Unified Threat Defense (UTD) component of Cisco IOS XE Software in controller mode could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because UTD improperly handles certain packets as those packets egress an SD-WAN IPsec tunnel. An attacker could exploit this vulnerability by sending crafted traffic through an SD-WAN IPsec tunnel that is configured on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: SD-WAN tunnels that are configured with Generic Routing Encapsulation (GRE) are not affected by this vulnerability.	8.6	More Details
CVE-2024-41605	In Foxit PDF Reader before 2024.3, and PDF Editor before 2024.3 and 13.x before 13.1.4, an attacker can replace an update file with a Trojan horse via side loading, because the update service lacks integrity validation for the updater. Attacker-controlled code may thus be executed.	8.4	More Details
CVE-2024-28813	An issue was discovered in Infinera hiT 7300 5.60.50. Undocumented privileged functions in the @CT management application allow an attacker to activate remote SSH access to the appliance via an unexpected network interface.	8.4	More Details
CVE-2024-9158	A stored cross site scripting vulnerability exists in Nessus Network Monitor where an authenticated, privileged local attacker could inject arbitrary code into the NNM UI via the local CLI.	8.4	More Details
CVE-2024-39431	In UMTS RLC driver, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with System execution privileges needed.	8.3	More Details
CVE-2024-39432	In UMTS RLC driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with System execution privileges needed.	8.3	More Details
CVE-2024-40510	Cross Site Scripting vulnerability in openPetra v.2023.02 allows a remote attacker to obtain sensitive information via the serverMCommon.asmx function.	8.2	More Details
CVE-2024-21545	Proxmox Virtual Environment is an open-source server management platform for enterprise virtualization. Insufficient safeguards against malicious API response values allow authenticated attackers with 'Sys.Audit' or 'VM.Monitor' privileges to download arbitrary host files via the API. When handling the result from a request handler before returning it to the user, the handle_api2_request function will check for the ‘download’ or ‘data’->’download’ objects inside the request handler call response object. If present, handle_api2_request will read a local file defined by this object and return it to the user. Two endpoints were identified which can control the object returned by a request handler sufficiently that the ’download’ object is defined and user controlled. This results in arbitrary file read. The privileges of this file read can result in full compromise of the system by various impacts such as disclosing sensitive files allowing for privileged session forgery.	8.2	More Details
CVE-2023-52946	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in vss service component in Synology Drive Client before 3.5.0-16084 allows remote attackers to overwrite trivial buffers and crash the client via unspecified vectors.	8.2	More Details
CVE-2024-47604	NuGet Gallery is a package repository that powers nuget.org. The NuGetGallery has a security vulnerability in its handling of HTML element attributes, which allows an attacker to execute arbitrary HTML or Javascript code in a victim's browser.	8.2	More Details
CVE-2024-21489	Versions of the package uplot before 1.6.31 are vulnerable to Prototype Pollution via the uplot.assign function due to missing check if the attribute resolves to the object prototype.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47078	Meshtastic is an open source, off-grid, decentralized, mesh network. Meshtastic uses MQTT to communicate over an internet connection to a shared or private MQTT Server. Nodes can communicate directly via an internet connection or proxied through a connected phone (i.e., via bluetooth). Prior to version 2.5.1, multiple weaknesses in the MQTT implementation allow for authentication and authorization bypasses resulting in unauthorized control of MQTT-connected nodes. Version 2.5.1 contains a patch.	8.1	More Details
CVE-2024-46097	TestLink 1.9.20 is vulnerable to Incorrect Access Control in the TestPlan editing section. When a new TestPlan is created, an ID with an incremental value is automatically generated. Using the edit function you can change the tplan_id parameter to another ID. The application does not carry out a check on the user's permissions maing it possible to recover the IDs of all the TestPlans (even the administrative ones) and modify them even with minimal privileges.	8.1	More Details
CVE-2024-47125	The goTenna Pro App does not authenticate public keys which allows an unauthenticated attacker to manipulate messages. It is advised to update your app to the current release for enhanced encryption protocols.	8.1	More Details
CVE-2024-8455	The swctrl service is used to detect and remotely manage PLANET Technology devices. For certain switch models, the authentication tokens used during communication with this service are encoded user passwords. Due to insufficient strength, unauthorized remote attackers who intercept the packets can directly crack them to obtain plaintext passwords.	8.1	More Details
CVE-2024-47295	Insecure initial password configuration issue in SEIKO EPSON Web Config allows a remote unauthenticated attacker to set an arbitrary password and operate the device with an administrative privilege. As for the details of the affected versions, see the information provided by the vendor under [References].	8.1	More Details
CVE-2024-8548	The KB Support – WordPress Help Desk and Knowledge Base plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check on several functions in all versions up to, and including, 1.6.6. This makes it possible for authenticated attackers, with Subscriber-level access and above, to perform multiple administrative actions, such as replying to arbitrary tickets, updating the status of any post, deleting any post, adding notes to tickets, flagging or unflagging tickets, and adding or removing ticket participants.	8.1	More Details
CVE-2024-20437	A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an unauthenticated, remote attacker to perform a cross-site request forgery (CSRF) attack and execute commands on the CLI of an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an already authenticated user to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on the affected device with the privileges of the targeted user.	8.1	More Details
CVE-2024-42514	A vulnerability in the legacy chat component of Mitel MiContact Center Business through 10.1.0.4 could allow an unauthenticated attacker to conduct an unauthorized access attack due to inadequate access control checks. A successful exploit requires user interaction and could allow an attacker to access sensitive information and send unauthorized messages during an active chat session.	8.1	More Details
CVE-2024-7781	The Jupiter X Core plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 4.7.5. This is due to improper authentication via the Social Login widget. This makes it possible for unauthenticated attackers to log in as the first user to have logged in with a social media account, including administrator accounts. Attackers can exploit the vulnerability even if the Social Login element has been disabled, as long as it was previously enabled and used. The vulnerability was partially patched in version 4.7.5, and fully patched in version 4.7.8.	8.1	More Details
CVE-2024-46461	VLC media player 3.0.20 and earlier is vulnerable to denial of service through an integer overflow which could be triggered with a maliciously crafted mms stream (heap based overflow). If successful, a malicious third party could trigger either a crash of VLC or an arbitrary code execution with the target user's privileges.	8.0	More Details
CVE-2024-46329	VONETS VAP11G-300 v3.3.23.6.9 was discovered to contain a command injection vulnerability via the SystemCommand object.	8.0	More Details
CVE-2024-46328	VONETS VAP11G-300 v3.3.23.6.9 was discovered to contain hardcoded credentials for several different privileged accounts, including root.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38963	IBM Aspera Console 3.4.0 through 3.4.4 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by a CSV injection vulnerability. By persuading a victim to open a specially crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system.	8.0	More Details
CVE-2024-28948	Advantech ADAM-5630 contains a cross-site request forgery (CSRF) vulnerability. It allows an attacker to partly circumvent the same origin policy, which is designed to prevent different websites from interfering with each other.	8.0	More Details
CVE-2024-23967	Autel MaxiCharger AC Elite Business C50 WebSocket Base64 Decoding Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Autel MaxiCharger AC Elite Business C50 chargers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of base64-encoded data within WebSocket messages. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-23230	8.0	More Details
CVE-2024-39275	Cookies of authenticated Advantech ADAM-5630 users remain as active valid cookies when a session is closed. Forging requests with a legitimate cookie, even if the session was terminated, allows an unauthorized attacker to act with the same level of privileges of the legitimate user.	8.0	More Details
CVE-2024-46084	Scriptcase 9.10.023 and before is vulnerable to Remote Code Execution (RCE) via the nm_unzip function.	8.0	More Details
CVE-2024-46080	Scriptcase v9.10.023 and before is vulnerable to Remote Code Execution (RCE) via the nm_zip function.	8.0	More Details
CVE-2024-46313	TP-Link WR941ND V6 has a stack overflow vulnerability in the ssid parameter in /userRpm/popupSiteSurveyRpm.htm.	8.0	More Details
CVE-2024-23959	Autel MaxiCharger AC Elite Business C50 BLE AppChargingControl Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Autel MaxiCharger AC Elite Business C50 charging stations. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of the AppChargingControl BLE command. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-23194	8.0	More Details
CVE-2024-23935	Alpine Halo9 DecodeUTF7 Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Alpine Halo9 devices. An attacker must first obtain the ability to pair a malicious Bluetooth device with the target system in order to exploit this vulnerability. The specific flaw exists within the DecodeUTF7 function. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-23249	8.0	More Details
CVE-2024-44678	Gigastone TR1 Travel Router R101 v1.0.2 is vulnerable to Command Injection. This allows an authenticated attacker to execute arbitrary commands on the device by sending a crafted HTTP request to the ssid parameter in the request.	8.0	More Details
CVE-2024-46812	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Skip inactive planes within ModeSupportAndSystemConfiguration [Why] Coverity reports Memory - illegal accesses. [How] Skip inactive planes.	7.8	More Details
CVE-2024-7672	A maliciously crafted DWF file, when parsed in dwfcore.dll through Autodesk Navisworks, can force an Out-of-Bounds Write. 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-2024-7674	A maliciously crafted DWF file, when parsed in dwfcore.dll through Autodesk Navisworks, can force a Heap-based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash or execute arbitrary code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7675	A maliciously crafted DWF file, when parsed in w3dtk.dll through Autodesk Navisworks, can force a Use-After-Free. A malicious actor can leverage this vulnerability to cause a crash or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-46258	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_load_png_mem() function at cute_png.h.	7.8	More Details
CVE-2024-46259	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_unfilter() function at cute_png.h.	7.8	More Details
CVE-2024-46261	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_make32() function at cute_png.h.	7.8	More Details
CVE-2024-46263	cute_png v1.05 was discovered to contain a stack overflow via the cp_dynamic() function at cute_png.h.	7.8	More Details
CVE-2024-46264	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_find() function at cute_png.h.	7.8	More Details
CVE-2024-46267	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_block() function at cute_png.h.	7.8	More Details
CVE-2024-46274	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_stored() function at cute_png.h.	7.8	More Details
CVE-2024-46276	cute_png v1.05 was discovered to contain a heap buffer overflow via the cp_chunk() function at cute_png.h.	7.8	More Details
CVE-2024-46831	In the Linux kernel, the following vulnerability has been resolved: net: microchip: vcap: Fix use-after-free error in kunit test This is a clear use-after-free error. We remove it, and rely on checking the return code of vcap_del_rule.	7.8	More Details
CVE-2024-47045	Privilege chaining issue exists in the installer of e-Tax software(common program). If this vulnerability is exploited, a malicious DLL prepared by an attacker may be executed with higher privileges than the application privilege.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46830	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Acquire kvm->srcu when handling KVM_SET_VCPU_EVENTS Grab kvm->srcu when processing KVM_SET_VCPU_EVENTS, as KVM will forcibly leave nested VMX/SVM if SMM mode is being toggled, and leaving nested VMX reads guest memory. Note, kvm_vcpu_ioctl_x86_set_vcpu_events() can also be called from KVM_RUN via sync_regs(), which already holds SRCU. I.e. trying to precisely use kvm_vcpu_srcu_read_lock() around the problematic SMM code would cause problems. Acquiring SRCU isn't all that expensive, so for simplicity, grab it unconditionally for KVM_SET_VCPU_EVENTS. ============================= WARNING: suspicious RCU usage 6.10.0-rc7-332d2c1d713e-next-vm #552 Not tainted ----------------------------- include/linux/kvm_host.h:1027 suspicious rcu_dereference_check() usage! other info that might help us debug this: rcu_scheduler_active = 2, debug_locks = 1 1 lock held by repro/1071: #0: ffff88811e424430 (&vcpu->mutex){+.+.}-{3:3}, at: kvm_vcpu_ioctl+0x7d/0x970 [kvm] stack backtrace: CPU: 15 PID: 1071 Comm: repro Not tainted 6.10.0-rc7-332d2c1d713e-next-vm #552 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 0.0.0 02/06/2015 Call Trace: <TASK> dump_stack_lvl+0x7f/0x90 lockdep_rcu_suspicious+0x13f/0x1a0 kvm_vcpu_gfn_to_memslot+0x168/0x190 [kvm] kvm_vcpu_read_guest+0x3e/0x90 [kvm] nested_vmx_load_msr+0x6b/0x1d0 [kvm_intel] load_vmcs12_host_state+0x432/0xb40 [kvm_intel] vmx_leave_nested+0x30/0x40 [kvm_intel] kvm_vcpu_ioctl_x86_set_vcpu_events+0x15d/0x2b0 [kvm] kvm_arch_vcpu_ioctl+0x1107/0x1750 [kvm] ? mark_held_locks+0x49/0x70 ? kvm_vcpu_ioctl+0x7d/0x970 [kvm] ? kvm_vcpu_ioctl+0x497/0x970 [kvm] kvm_vcpu_ioctl+0x497/0x970 [kvm] ? lock_acquire+0xba/0x2d0 ? find_held_lock+0x2b/0x80 ? do_user_addr_fault+0x40c/0x6f0 ? lock_release+0xb7/0x270 __x64_sys_ioctl+0x82/0xb0 do_syscall_64+0x6c/0x170 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x7ff11eb1b539 </TASK>	7.8	More Details
CVE-2022-49038	Inclusion of functionality from untrusted control sphere vulnerability in OpenSSL DLL component in Synology Drive Client before 3.3.0-15082 allows local users to execute arbitrary code via unspecified vectors.	7.8	More Details
CVE-2024-8404	An arbitrary file deletion vulnerability exists in PaperCut NG/MF, specifically affecting Windows servers with Web Print enabled. To exploit this vulnerability, an attacker must first obtain local login access to the Windows Server hosting PaperCut NG/MF and be capable of executing low-privilege code directly on the server via the web-print-hot-folder. Important: In most installations, this risk is mitigated by the default Windows Server configuration, which restricts local login access to Administrators only. However, this vulnerability could pose a risk to customers who allow non-administrative users to log into the local console of the Windows environment hosting the PaperCut NG/MF application server. Note: This CVE has been split from CVE-2024-3037.	7.8	More Details
CVE-2024-7673	A maliciously crafted DWFX file, when parsed in w3dtk.dll through Autodesk Navisworks, can force a Heap-based Buffer Overflow. A malicious actor can leverage this vulnerability to cause a crash or execute arbitrary code in the context of the current process.	7.8	More Details
CVE-2024-7671	A maliciously crafted DWFX file, when parsed in dwfcore.dll through Autodesk Navisworks, can force an Out-of-Bounds Write. 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-2024-46811	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix index may exceed array range within fpu_update_bw_bounding_box [Why] Coverity reports OVERRUN warning. soc.num_states could be 40. But array range of bw_params->clk_table.entries is 8. [How] Assert if soc.num_states greater than 8.	7.8	More Details
CVE-2024-7670	A maliciously crafted DWFX file, when parsed in w3dtk.dll through Autodesk Navisworks, can force an Out-of-Bounds Read. 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-2024-46804	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add array index check for hdcp ddc access [Why] Coverity reports OVERRUN warning. Do not check if array index valid. [How] Check msg_id valid and valid array index.	7.8	More Details
CVE-2024-46833	In the Linux kernel, the following vulnerability has been resolved: net: hns3: void array out of bound when loop tnl_num When query reg inf of SSU, it loops tnl_num times. However, tnl_num comes from hardware and the length of array is a fixed value. To void array out of bound, make sure the loop time is not greater than the length of array	7.8	More Details
CVE-2024-46836	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: aspeed_udc: validate endpoint index for ast udc We should verify the bound of the array to assure that host may not manipulate the index to point past endpoint array. Found by static analysis.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46844	In the Linux kernel, the following vulnerability has been resolved: um: line: always fill *error_out in setup_one_line() The pointer isn't initialized by callers, but I have encountered cases where it's still printed; initialize it in all possible cases in setup_one_line().	7.8	More Details
CVE-2024-46845	In the Linux kernel, the following vulnerability has been resolved: tracing/timerlat: Only clear timer if a kthread exists The timerlat tracer can use user space threads to check for osnoise and timer latency. If the program using this is killed via a SIGTERM, the threads are shutdown one at a time and another tracing instance can start up resetting the threads before they are fully closed. That causes the hrtimer assigned to the kthread to be shutdown and freed twice when the dying thread finally closes the file descriptors, causing a use-after-free bug. Only cancel the hrtimer if the associated thread is still around. Also add the interface_lock around the resetting of the tlat_var->kthread. Note, this is just a quick fix that can be backported to stable. A real fix is to have a better synchronization between the shutdown of old threads and the starting of new ones.	7.8	More Details
CVE-2024-46849	In the Linux kernel, the following vulnerability has been resolved: ASoC: meson: axg-card: fix 'use-after-free' Buffer 'card->dai_link' is reallocated in 'meson_card_reallocate_links()', so move 'pad' pointer initialization after this function when memory is already reallocated. Kasan bug report: == BUG: KASAN: slab-use-after-free in axg_card_add_link+0x76c/0x9bc Read of size 8 at addr ffff000000e8b260 by task modprobe/356 CPU: 0 PID: 356 Comm: modprobe Tainted: G O 6.9.12-sdkernel #1 Call trace: dump_backtrace+0x94/0xec show_stack+0x18/0x24 dump_stack_lvl+0x78/0x90 print_report+0xfc/0x5c0 kasan_report+0xb8/0xfc __asan_load8+0x9c/0xb8 axg_card_add_link+0x76c/0x9bc [snd_soc_meson_axg_sound_card] meson_card_probe+0x344/0x3b8 [snd_soc_meson_card_utils] platform_probe+0x8c/0xf4 really_probe+0x110/0x39c __driver_probe_device+0xb8/0x18c driver_probe_device+0x108/0x1d8 __driver_attach+0xd0/0x25c bus_for_each_dev+0xe0/0x154 driver_attach+0x34/0x44 bus_add_driver+0x134/0x294 driver_register+0xa8/0x1e8 __platform_driver_register+0x44/0x54 axg_card_pdrv_init+0x20/0x1000 [snd_soc_meson_axg_sound_card] do_one_initcall+0xdc/0x25c do_init_module+0x10c/0x334 load_module+0x24c4/0x26cc init_module_from_file+0xd4/0x128 __arm64_sys_finit_module+0x1f4/0x41c invoke_syscall+0x60/0x188 el0_svc_common.constprop.0+0x78/0x13c do_el0_svc+0x30/0x40 el0_svc+0x38/0x78 el0t_64_sync_handler+0x100/0x12c el0t_64_sync+0x190/0x194	7.8	More Details
CVE-2024-46852	In the Linux kernel, the following vulnerability has been resolved: dma-buf: heaps: Fix off-by-one in CMA heap fault handler Until VM_DONTEXPAND was added in commit 1c1914d6e8c6 ("dma-buf: heaps: Don't track CMA dma-buf pages under RssFile") it was possible to obtain a mapping larger than the buffer size via mremap and bypass the overflow check in dma_buf_mmap_internal. When using such a mapping to attempt to fault past the end of the buffer, the CMA heap fault handler also checks the fault offset against the buffer size, but gets the boundary wrong by 1. Fix the boundary check so that we don't read off the end of the pages array and insert an arbitrary page in the mapping.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46853	In the Linux kernel, the following vulnerability has been resolved: spi: nxp-fspi: fix the KASAN report out-of-bounds bug Change the memcpy length to fix the out-of-bounds issue when writing the data that is not 4 byte aligned to TX FIFO. To reproduce the issue, write 3 bytes data to NOR chip. dd if=3b of=/dev/mtd0 [36.926103] == [36.933409] BUG: KASAN: slab-out-of-bounds in nxp_fspi_exec_op+0x26ec/0x2838 [36.940514] Read of size 4 at addr ffff00081037c2a0 by task dd/455 [36.946721] [36.948235] CPU: 3 UID: 0 PID: 455 Comm: dd Not tainted 6.11.0-rc5-gc7b0e37c8434 #1070 [36.956185] Hardware name: Freescale i.MX8QM MEK (DT) [36.961260] Call trace: [36.963723] dump_backtrace+0x90/0xe8 [36.967414] show_stack+0x18/0x24 [36.970749] dump_stack_lvl+0x78/0x90 [36.974451] print_report+0x114/0x5cc [36.978151] kasan_report+0xa4/0xf0 [36.981670] __asan_report_load_n_noabort+0x1c/0x28 [36.986587] nxp_fspi_exec_op+0x26ec/0x2838 [36.990800] spi_mem_exec_op+0x8ec/0xd30 [36.994762] spi_mem_no_dirmap_read+0x190/0x1e0 [36.999323] spi_mem_dirmap_write+0x238/0x32c [37.003710] spi_nor_write_data+0x220/0x374 [37.007932] spi_nor_write+0x110/0x2e8 [37.011711] mtd_write_oob_std+0x154/0x1f0 [37.015838] mtd_write_oob+0x104/0x1d0 [37.019617] mtd_write+0xb8/0x12c [37.022953] mtdchar_write+0x224/0x47c [37.026732] vfs_write+0x1e4/0x8c8 [37.030163] ksys_write+0xec/0x1d0 [37.033586] __arm64_sys_write+0x6c/0x9c [37.037539] invoke_syscall+0x6c/0x258 [37.041327] el0_svc_common.constprop.0+0x160/0x22c [37.046244] do_el0_svc+0x44/0x5c [37.049589] el0_svc+0x38/0x78 [37.052681] el0t_64_sync_handler+0x13c/0x158 [37.057077] el0t_64_sync+0x190/0x194 [37.060775] [37.062274] Allocated by task 455: [37.065701] kasan_save_stack+0x2c/0x54 [37.069570] kasan_save_track+0x20/0x3c [37.073438] kasan_save_alloc_info+0x40/0x54 [37.077736] __kasan_kmalloc+0xa0/0xb8 [37.081515] __kmalloc_noprof+0x158/0x2f8 [37.085563] mtd_kmalloc_up_to+0x120/0x154 [37.089690] mtdchar_write+0x130/0x47c [37.093469] vfs_write+0x1e4/0x8c8 [37.096901] ksys_write+0xec/0x1d0 [37.100332] __arm64_sys_write+0x6c/0x9c [37.104287] invoke_syscall+0x6c/0x258 [37.108064] el0_svc_common.constprop.0+0x160/0x22c [37.112972] do_el0_svc+0x44/0x5c [37.116319] el0_svc+0x38/0x78 [37.119401] el0t_64_sync_handler+0x13c/0x158 [37.123788] el0t_64_sync+0x190/0x194 [37.127474] [37.128977] The buggy address belongs to the object at ffff00081037c2a0 [37.128977] which belongs to the cache kmalloc-8 of size 8 [37.141177] The buggy address is located 0 bytes inside of [37.141177] allocated 3-byte region [ffff00081037c2a0, ffff00081037c2a3) [37.153465] [37.154971] The buggy address belongs to the physical page: [37.160559] page: refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x89037c [37.168596] flags: 0xbfffe0000000000(node=0|zone=2|lastcpupid=0x1ffff) [37.175149] page_type: 0xfdffffff(slab) [37.179021] raw: 0bfffe0000000000 ffff000800002500 dead000000000122 0000000000000000 [37.186788] raw: 0000000000000000 0000000080800080 00000001fdffffff 0000000000000000 [37.194553] page dumped because: kasan: bad access detected [37.200144] [37.201647] Memory state around the buggy address: [37.206460] ffff00081037c180: fa fc fc fc fa fc fc fc fa fc fc fc fa fc fc fc [37.213701] ffff00081037c200: fa fc fc fc 05 fc fc fc 03 fc fc fc 02 fc fc fc [37.220946] >ffff00081037c280: 06 fc fc fc 03 fc fc fc fc fc fc fc fc fc fc fc [37.228186] ^ [37.232473] ffff00081037c300: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [37.239718] ffff00081037c380: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [37.246962] == ---truncated---	7.8	More Details
CVE-2024-46859	In the Linux kernel, the following vulnerability has been resolved: platform/x86: panasonic-laptop: Fix SINF array out of bounds accesses The panasonic laptop code in various places uses the SINF array with index values of 0 - SINF_CUR_BRIGHT(0x0d) without checking that the SINF array is big enough. Not all panasonic laptops have this many SINF array entries, for example the Toughbook CF-18 model only has 10 SINF array entries. So it only supports the AC+DC brightness entries and mute. Check that the SINF array has a minimum size which covers all AC+DC brightness entries and refuse to load if the SINF array is smaller. For higher SINF indexes hide the sysfs attributes when the SINF array does not contain an entry for that attribute, avoiding show()/store() accessing the array out of bounds and add bounds checking to the probe() and resume() code accessing these.	7.8	More Details
CVE-2024-46813	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check link_index before accessing dc->links[] [WHY & HOW] dc->links[] has max size of MAX_LINKS and NULL is return when trying to access with out-of-bound index. This fixes 3 OVERRUN and 1 RESOURCE_LEAK issues reported by Coverity.	7.8	More Details
CVE-2024-46814	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check msg_id before processing transcation [WHY & HOW] HDCP_MESSAGE_ID_INVALID (-1) is not a valid msg_id nor is it a valid array index, and it needs checking before used. This fixes 4 OVERRUN issues reported by Coverity.	7.8	More Details
CVE-2024-46815	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check num_valid_sets before accessing reader_wm_sets[] [WHY & HOW] num_valid_sets needs to be checked to avoid a negative index when accessing reader_wm_sets[num_valid_sets - 1]. This fixes an OVERRUN issue reported by Coverity.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46820	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/vcn: remove irq disabling in vcn 5 suspend We do not directly enable/disable VCN IRQ in vcn 5.0.0. And we do not handle the IRQ state as well. So the calls to disable IRQ and set state are removed. This effectively gets rid of the warining of "WARN_ON(!amdgpu_irq_enabled(adev, src, type))" in amdgpu_irq_put().	7.8	More Details
CVE-2024-9325	A vulnerability classified as critical has been found in Intelbras InControl up to 2.21.56. This affects an unknown part of the file C:\Program Files (x86)\Intelbras\Incontrol Cliente\incontrol_webcam\incontrol-service-watchdog.exe. The manipulation leads to unquoted search path. It is possible to launch the attack on the local host. Upgrading to version 2.21.58 is able to address this issue. It is recommended to upgrade the affected component. The vendor was informed early on 2024-08-05 about this issue. The release of a fixed version 2.21.58 was announced for the end of August 2024 but then was postponed until 2024-09-20.	7.8	More Details
CVE-2024-46818	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check gpio_id before used as array index [WHY & HOW] GPIO_ID_UNKNOWN (-1) is not a valid value for array index and therefore should be checked in advance. This fixes 5 OVERRUN issues reported by Coverity.	7.8	More Details
CVE-2024-46828	In the Linux kernel, the following vulnerability has been resolved: sched: sch_cake: fix bulk flow accounting logic for host fairness In sch_cake, we keep track of the count of active bulk flows per host, when running in dst/src host fairness mode, which is used as the round-robin weight when iterating through flows. The count of active bulk flows is updated whenever a flow changes state. This has a peculiar interaction with the hash collision handling: when a hash collision occurs (after the set-associative hashing), the state of the hash bucket is simply updated to match the new packet that collided, and if host fairness is enabled, that also means assigning new per-host state to the flow. For this reason, the bulk flow counters of the host(s) assigned to the flow are decremented, before new state is assigned (and the counters, which may not belong to the same host anymore, are incremented again). Back when this code was introduced, the host fairness mode was always enabled, so the decrement was unconditional. When the configuration flags were introduced the *increment* was made conditional, but the *decrement* was not. Which of course can lead to a spurious decrement (and associated wrap-around to U16_MAX). AFAICT, when host fairness is disabled, the decrement and wrap-around happens as soon as a hash collision occurs (which is not that common in itself, due to the set-associative hashing). However, in most cases this is harmless, as the value is only used when host fairness mode is enabled. So in order to trigger an array overflow, sch_cake has to first be configured with host fairness disabled, and while running in this mode, a hash collision has to occur to cause the overflow. Then, the qdisc has to be reconfigured to enable host fairness, which leads to the array out-of-bounds because the wrapped-around value is retained and used as an array index. It seems that syzbot managed to trigger this, which is quite impressive in its own right. This patch fixes the issue by introducing the same conditional check on decrement as is used on increment. The original bug predates the upstreaming of cake, but the commit listed in the Fixes tag touched that code, meaning that this patch won't apply before that.	7.8	More Details
CVE-2024-46821	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: Fix negative array index read Avoid using the negative values for clk_idex as an index into an array pptable->DpmDescriptor. V2: fix clk_index return check (Tim Huang)	7.8	More Details
CVE-2024-7679	In Progress Telerik UI for WinForms versions prior to 2024 Q3 (2024.3.924), a command injection attack is possible through improper neutralization of hyperlink elements.	7.8	More Details
CVE-2024-7575	In Progress Telerik UI for WPF versions prior to 2024 Q3 (2024.3.924), a command injection attack is possible through improper neutralization of hyperlink elements.	7.8	More Details
CVE-2024-7576	In Progress Telerik UI for WPF versions prior to 2024 Q3 (2024.3.924), a code execution attack is possible through an insecure deserialization vulnerability.	7.8	More Details
CVE-2024-8316	In Progress Telerik UI for WPF versions prior to 2024 Q3 (2024.3.924), a code execution attack is possible through an insecure deserialization vulnerability.	7.8	More Details
CVE-2024-25661	In Infinera TNMS (Transcend Network Management System) 19.10.3, cleartext storage of sensitive information in memory of the desktop application TNMS Client allows guest OS administrators to obtain various users' passwords by reading memory dumps of the desktop application.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9198	Vulnerability in Clibo Manager v1.1.9.1 that could allow an attacker to execute an stored Cross-Site Scripting (stored XSS) by uploading a malicious .svg image in the section: Profile > Profile picture.	7.6	More Details
CVE-2024-46607	Incorrect access control in IceCMS v3.4.7 and before allows attackers to authenticate by entering any arbitrary values as the username and password via the loginAdmin method in the UserController.java file.	7.6	More Details
CVE-2024-46510	ESAFENET CDG v5 was discovered to contain a SQL injection vulnerability via the id parameter in the NavigationAjax interface	7.6	More Details
CVE-2024-46549	An issue in the TP-Link MQTT Broker and API gateway of TP-Link Kasa KP125M v1.0.3 allows attackers to establish connections by impersonating devices owned by other users.	7.6	More Details
CVE-2024-6594	Improper Handling of Exceptional Conditions vulnerability in the WatchGuard Single Sign-On Client on Windows causes the client to crash while handling malformed commands. An attacker with network access to the client could create a denial of service condition for the Single Sign-On service by repeatedly issuing malformed commands. This issue affects Single Sign-On Client: through 12.7.	7.5	More Details
CVE-2024-31146	When multiple devices share resources and one of them is to be passed through to a guest, security of the entire system and of respective guests individually cannot really be guaranteed without knowing internals of any of the involved guests. Therefore such a configuration cannot really be security-supported, yet making that explicit was so far missing. Resources the sharing of which is known to be problematic include, but are not limited to - - PCI Base Address Registers (BARs) of multiple devices mapping to the same page (4k on x86), - - INTx lines.	7.5	More Details
CVE-2024-44910	NASA CryptoLib v1.3.0 was discovered to contain an Out-of-Bounds read via the AOS subsystem (crypto_aos.c).	7.5	More Details
CVE-2024-8175	An unauthenticated remote attacker can causes the CODESYS web server to access invalid memory which results in a DoS.	7.5	More Details
CVE-2024-45773	A use-after-free vulnerability involving upgradeToRocket requests can cause the application to crash or potentially result in code execution or other undesirable effects. This issue affects Facebook Thrift prior to v2024.09.09.00.	7.5	More Details
CVE-2024-47197	Exposure of Sensitive Information to an Unauthorized Actor, Insecure Storage of Sensitive Information vulnerability in Maven Archetype Plugin. This issue affects Maven Archetype Plugin: from 3.2.1 before 3.3.0. Users are recommended to upgrade to version 3.3.0, which fixes the issue. Archetype integration testing creates a file called ./target/classes/archetype-it/archetype-settings.xml This file contains all the content from the users ~/.m2/settings.xml file, which often contains information they do not want to publish. We expect that on many developer machines, this also contains credentials. When the user runs mvn verify again (without a mvn clean), this file becomes part of the final artifact. If a developer were to publish this into Maven Central or any other remote repository (whether as a release or a snapshot) their credentials would be published without them knowing.	7.5	More Details
CVE-2024-44911	NASA CryptoLib v1.3.0 was discovered to contain an Out-of-Bounds read via the TC subsystem (crypto_aos.c).	7.5	More Details
CVE-2024-37125	Dell SmartFabric OS10 Software, versions 10.5.6.x, 10.5.5.x, 10.5.4.x,10.5.3.x, contains an Uncontrolled Resource Consumption vulnerability. A remote unauthenticated host could potentially exploit this vulnerability leading to a denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31145	Certain PCI devices in a system might be assigned Reserved Memory Regions (specified via Reserved Memory Region Reporting, "RMRR") for Intel VT-d or Unity Mapping ranges for AMD-Vi. These are typically used for platform tasks such as legacy USB emulation. Since the precise purpose of these regions is unknown, once a device associated with such a region is active, the mappings of these regions need to remain continuouly accessible by the device. In the logic establishing these mappings, error handling was flawed, resulting in such mappings to potentially remain in place when they should have been removed again. Respective guests would then gain access to memory regions which they aren't supposed to have access to.	7.5	More Details
CVE-2024-8644	Cleartext Storage of Sensitive Information in a Cookie vulnerability in Oceanic Software ValeApp allows Protocol Manipulation, : JSON Hijacking (aka JavaScript Hijacking).This issue affects ValeApp: before v2.0.0.	7.5	More Details
CVE-2024-8126	The Advanced File Manager plugin for WordPress is vulnerable to arbitrary file uploads via the 'class_fma_connector.php' file in all versions up to, and including, 5.2.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, and granted permissions by an Administrator, to upload a new .htaccess file allowing them to subsequently upload arbitrary files on the affected site's server which may make remote code execution possible.	7.5	More Details
CVE-2024-9301	A path traversal issue in E2Nest prior to commit 8a41948e553c89c56b14410c6ed395e9cfb9250a	7.5	More Details
CVE-2024-8609	Insertion of Sensitive Information into Log File vulnerability in Oceanic Software ValeApp allows Query System for Information.This issue affects ValeApp: before v2.0.0.	7.5	More Details
CVE-2024-7107	Files or Directories Accessible to External Parties vulnerability in National Keep Cyber Security Services CyberMath allows Collect Data from Common Resource Locations.This issue affects CyberMath: before CYBM.240816253.	7.5	More Details
CVE-2024-9029	A flaw was found in the freeimage library. Processing a crafted image can cause a buffer over-read of 1 byte in the read_iptc_profile function in the Source/Metadata/IPTC.cpp file because the size of the profile is not being sanitized, causing a crash in the application linked to the library, resulting in a denial of service.	7.5	More Details
CVE-2024-22892	OpenSlides 4.0.15 was discovered to be using a weak hashing algorithm to store passwords.	7.5	More Details
CVE-2024-7714	The AI ChatBot with ChatGPT and Content Generator by AYS WordPress plugin before 2.1.0 lacks sufficient access controls allowing an unauthenticated user to disconnect the AI ChatBot with ChatGPT and Content Generator by AYS WordPress plugin before 2.1.0 from OpenAI, thereby disabling the AI ChatBot with ChatGPT and Content Generator by AYS WordPress plugin before 2.1.0. Multiple actions are accessible: 'ays_chatgpt_disconnect', 'ays_chatgpt_connect', and 'ays_chatgpt_save_feedback'	7.5	More Details
CVE-2024-7713	The AI ChatBot with ChatGPT and Content Generator by AYS WordPress plugin before 2.1.0 discloses the Open AI API Key, allowing unauthenticated users to obtain it	7.5	More Details
CVE-2024-22893	OpenSlides 4.0.15 verifies passwords by comparing password hashes using a function with content-dependent runtime. This can allow attackers to obtain information about the password hash using a timing attack.	7.5	More Details
CVE-2024-7594	Vault’s SSH secrets engine did not require the valid_principals list to contain a value by default. If the valid_principals and default_user fields of the SSH secrets engine configuration are not set, an SSH certificate requested by an authorized user to Vault’s SSH secrets engine could be used to authenticate as any user on the host. Fixed in Vault Community Edition 1.17.6, and in Vault Enterprise 1.17.6, 1.16.10, and 1.15.15.	7.5	More Details
CVE-2024-44825	Directory Traversal vulnerability in Centro de Tecnologia da Informaco Renato Archer InVesalius3 v3.1.99995 allows attackers to write arbitrary files unto the system via a crafted .inv3 file.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20350	A vulnerability in the SSH server of Cisco Catalyst Center, formerly Cisco DNA Center, could allow an unauthenticated, remote attacker to impersonate a Cisco Catalyst Center appliance. This vulnerability is due to the presence of a static SSH host key. An attacker could exploit this vulnerability by performing a machine-in-the-middle attack on SSH connections, which could allow the attacker to intercept traffic between SSH clients and a Cisco Catalyst Center appliance. A successful exploit could allow the attacker to impersonate the affected appliance, inject commands into the terminal session, and steal valid user credentials.	7.5	More Details
CVE-2024-46471	The Directory Listing in /uploads/ Folder in CodeAstro Membership Management System 1.0 exposes the structure and contents of directories, potentially revealing sensitive information.	7.5	More Details
CVE-2024-44912	NASA CryptoLib v1.3.0 was discovered to contain an Out-of-Bounds read via the TM subsystem (crypto_tm.c).	7.5	More Details
CVE-2024-8484	The REST API TO MiniProgram plugin for WordPress is vulnerable to SQL Injection via the 'order' parameter of the /wp-json/watch-life-net/v1/comment/getcomments REST API endpoint in all versions up to, and including, 4.7.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2024-8497	Franklin Fueling Systems TS-550 EVO versions prior to 2.26.4.8967 possess a file that can be read arbitrarily that could allow an attacker obtain administrator credentials.	7.5	More Details
CVE-2024-47527	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Device Dependencies" feature allows authenticated users to inject arbitrary JavaScript through the device name ("hostname" parameter). This vulnerability can lead to the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and allowing unauthorized actions. This vulnerability is fixed in 24.9.0.	7.5	More Details
CVE-2024-47525	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Alert Rules" feature allows authenticated users to inject arbitrary JavaScript through the "Title" field. This vulnerability can lead to the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and allowing unauthorized actions. This vulnerability is fixed in 24.9.0.	7.5	More Details
CVE-2024-47523	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Alert Transports" feature allows authenticated users to inject arbitrary JavaScript through the "Details" section (which contains multiple fields depending on which transport is selected at that moment). This vulnerability can lead to the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and allowing unauthorized actions. This vulnerability is fixed in 24.9.0.	7.5	More Details
CVE-2024-9399	A website configured to initiate a specially crafted WebTransport session could crash the Firefox process leading to a denial of service condition. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	7.5	More Details
CVE-2024-39928	In Apache Linkis <= 1.5.0, a Random string security vulnerability in Spark EngineConn, random string generated by the Token when starting Py4j uses the Commons Lang's RandomStringUtils. Users are recommended to upgrade to version 1.6.0, which fixes this issue.	7.5	More Details
CVE-2024-9394	An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the `resource://devtools` origin. This could allow them to access cross-origin JSON content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47083	Power Platform Terraform Provider allows managing environments and other resources within Power Platform. Versions prior to 3.0.0 have an issue in the Power Platform Terraform Provider where sensitive information, specifically the `client_secret` used in the service principal authentication, may be exposed in logs. This exposure occurs due to an error in the logging code that causes the `client_secret` to not be properly masked when logs are persisted or viewed. Users should upgrade to version 3.0.0 to receive a patched version of the provider that removes all logging of sensitive content. Users who have used this provider with the affected versions should take the following additional steps to mitigate the risk: Immediately rotate the `client_secret` for any service principal that has been configured using this Terraform provider. This will invalidate any potentially exposed secrets. Those who have set the `TF_LOG_PATH` environment variable or configured Terraform to persist logs to a file or an external system, consider disabling this until they have updated to a fixed version of the provider. Those who have existing logs that may contain the `client_secret` should remove or sanitize these logs to prevent unauthorized access. This includes logs on disk, in monitoring systems, or in logging services.	7.5	More Details
CVE-2024-41708	An issue was discovered in AdaCore ada_web_services 20.0 allows an attacker to escalate privileges and steal sessions via the Random_String() function in the src/core/aws-utils.adb module.	7.5	More Details
CVE-2024-9393	An attacker could, via a specially crafted multipart response, execute arbitrary JavaScript under the `resource://pdf.js` origin. This could allow them to access cross-origin PDF content. This access is limited to "same site" documents by the Site Isolation feature on desktop clients, but full cross-origin access is possible on Android versions. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Firefox ESR < 115.16, Thunderbird < 128.3, and Thunderbird < 131.	7.5	More Details
CVE-2024-45408	eLabFTW is an open source electronic lab notebook for research labs. An incorrect permission check has been found that could allow an authenticated user to access several kinds of otherwise restricted information. If anonymous access is allowed (something disabled by default), this extends to anyone. Users are advised to upgrade to at least version 5.1.0. System administrators can disable anonymous access in the System configuration panel.	7.5	More Details
CVE-2024-46609	An access control issue in the CheckVip function in UserController.java of IceCMS v3.4.7 and before allows unauthenticated attackers to access and returns all user information, including passwords	7.5	More Details
CVE-2024-46935	Rocket.Chat 6.12.0, 6.11.2, 6.10.5, 6.9.6, 6.8.6, 6.7.8, and earlier is vulnerable to denial of service (DoS). Attackers who craft messages with specific characters may crash the workspace due to an issue in the message parser.	7.5	More Details
CVE-2024-46936	Rocket.Chat 6.12.0, 6.11.2, 6.10.5, 6.9.6, 6.8.6, 6.7.8, and before is vulnerable to a message forgery / impersonation issue. Attackers can abuse the UpdateOTRAck method to send ephemeral messages as if they were any other user they choose.	7.5	More Details
CVE-2024-46610	An access control issue in IceCMS v3.4.7 and before allows attackers to arbitrarily modify users' information, including username and password, via a crafted POST request sent to the endpoint /User/ChangeUser/s in the ChangeUser function in UserController.java	7.5	More Details
CVE-2024-44860	An information disclosure vulnerability in the /Letter/PrintQr/ endpoint of Solvait v24.4.2 allows attackers to access sensitive data via a crafted request.	7.5	More Details
CVE-2024-8941	Path traversal vulnerability in Scriptcase version 9.4.019, in /scriptcase/devel/compat/nm_edit_php_edit.php (in the “subpage” parameter), which allows unauthenticated remote users to bypass SecurityManager's intended restrictions and list and/or read a parent directory via a “/...” or directly into a path used in the POST parameter “field_file” by a web application.	7.5	More Details
CVE-2024-46511	LoadZilla LLC LoadLogic v1.4.3 was discovered to contain insecure permissions vulnerability which allows a remote attacker to execute arbitrary code via the LogicLoadEc2DeployLambda and CredsGenFunction function.	7.5	More Details
CVE-2024-8452	Certain switch models from PLANET Technology only support obsolete algorithms for authentication protocol and encryption protocol in the SNMPv3 service, allowing attackers to obtain plaintext SNMPv3 credentials potentially.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8451	Certain switch models from PLANET Technology have an SSH service that improperly handles insufficiently authenticated connection requests, allowing unauthorized remote attackers to exploit this weakness to occupy connection slots and prevent legitimate users from accessing the SSH service.	7.5	More Details
CVE-2024-38861	Improper Certificate Validation in Checkmk Exchange plugin MikroTik allows attackers in MitM position to intercept traffic. This issue affects MikroTik: from 2.0.0 through 2.5.5, from 0.4a_mk through 2.0a.	7.4	More Details
CVE-2024-46330	VONETS VAP11G-300 v3.3.23.6.9 was discovered to contain a command injection vulnerability via the iptablesWebsFilterRun object.	7.4	More Details
CVE-2024-9403	Memory safety bugs present in Firefox 130. 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 < 131 and Thunderbird < 131.	7.3	More Details
CVE-2024-9296	A vulnerability was found in SourceCodester Advocate Office Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /control/forgot_pass.php. The manipulation of the argument username 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-2024-9326	A vulnerability classified as critical was found in PHPGurukul Online Shopping Portal 2.0. This vulnerability affects unknown code of the file /shopping/admin/index.php of the component Admin Panel. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-8481	The The Special Text Boxes plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 6.2.2. This is due to the plugin adding the filter add_filter('comment_text', 'do_shortcode'); which will run all shortcodes in comments. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-40506	Cross Site Scripting vulnerability in openPetra v.2023.02 allows a remote attacker to obtain sensitive information via the serverMHospitality.asmx function.	7.3	More Details
CVE-2024-40507	Cross Site Scripting vulnerability in openPetra v.2023.02 allows a remote attacker to obtain sensitive information via the serverMPersonnel.asmx function.	7.3	More Details
CVE-2024-40508	Cross Site Scripting vulnerability in openPetra v.2023.02 allows a remote attacker to obtain sensitive information via the serverMConference.asmx function.	7.3	More Details
CVE-2024-9360	A vulnerability was found in code-projects Restaurant Reservation System 1.0. It has been classified as critical. This affects an unknown part of the file /updatebal.php. The manipulation of the argument company 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-2024-45750	An issue in TheGreenBow Windows Standard VPN Client 6.87.108 (and older), Windows Enterprise VPN Client 6.87.109 (and older), Windows Enterprise VPN Client 7.5.007 (and older), Android VPN Client 6.4.5 (and older) VPN Client Linux 3.4 (and older), VPN Client MacOS 2.4.10 (and older) allows a remote attacker to execute arbitrary code via the IKEv2 Authentication phase, it accepts malformed ECDSA signatures and establishes the tunnel.	7.3	More Details
CVE-2024-9359	A vulnerability was found in code-projects Restaurant Reservation System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /addcompany.php. The manipulation of the argument company 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-2024-40512	Cross Site Scripting vulnerability in openPetra v.2023.02 allows a remote attacker to obtain sensitive information via the serverMReporting.asmx function.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40511	Cross Site Scripting vulnerability in openPetra v.2023.02 allows a remote attacker to obtain sensitive information via the serverMServerAdmin.asmx function.	7.3	More Details
CVE-2024-9295	A vulnerability was found in SourceCodester Advocate Office Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /control/login.php. The manipulation of the argument username 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-2024-45817	In x86's APIC (Advanced Programmable Interrupt Controller) architecture, error conditions are reported in a status register. Furthermore, the OS can opt to receive an interrupt when a new error occurs. It is possible to configure the error interrupt with an illegal vector, which generates an error when an error interrupt is raised. This case causes Xen to recurse through vlapic_error(). The recursion itself is bounded; errors accumulate in the the status register and only generate an interrupt when a new status bit becomes set. However, the lock protecting this state in Xen will try to be taken recursively, and deadlock.	7.3	More Details
CVE-2024-40509	Cross Site Scripting vulnerability in openPetra v.2023.02 allows a remote attacker to obtain sensitive information via the serverMFinDev.asmx function.	7.3	More Details
CVE-2024-8996	Unquoted Search Path or Element vulnerability in Grafana Agent (Flow mode) on Windows allows Privilege Escalation from Local User to SYSTEM This issue affects Agent Flow: before 0.43.2	7.3	More Details
CVE-2024-8975	Unquoted Search Path or Element vulnerability in Grafana Alloy on Windows allows Privilege Escalation from Local User to SYSTEM This issue affects Alloy: before 1.3.3, from 1.4.0-rc.0 through 1.4.0-rc.1.	7.3	More Details
CVE-2024-47524	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. User with Admin role can create a Device Groups, the application did not properly sanitize the user input in the Device Groups name, when user see the detail of the Device Group, if java script code is inside the name of the Device Groups, its will be trigger. This vulnerability is fixed in 24.9.0.	7.2	More Details
CVE-2022-4541	The WordPress Visitors plugin for WordPress is vulnerable to Stored Cross-Site Scripting via a spoofed HTTP Header value in versions up to, and including, 1.0 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 nm_vistior page.	7.2	More Details
CVE-2024-7869	The 123.chat - Video Chat plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 1.3.1 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.	7.2	More Details
CVE-2024-9130	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to time-based SQL Injection via the ‘order’ parameter in all versions up to, and including, 3.16.1 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 GiveWP Manager-level access and above, to append additional SQL queries into already existing queries within the Legacy View mode, that can be used to extract sensitive information from the database.	7.2	More Details
CVE-2024-46331	ModStartCMS v8.8.0 was discovered to contain an open redirect vulnerability in the redirect parameter at /admin/login. This vulnerability allows attackers to redirect users to an arbitrary website via a crafted URL.	7.2	More Details
CVE-2024-25659	In Infinera TNMS (Transcend Network Management System) 19.10.3, an insecure default configuration of the internal SFTP server on Linux servers allows remote attacker to access files and directories outside the SFTP user home directory.	7.2	More Details
CVE-2024-6931	The The Events Calendar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via RSVP name field in all versions up to, and including, 6.6.3 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.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8379	The Cost Calculator Builder WordPress plugin before 3.2.29 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by users with a role as low as Admin.	7.2	More Details
CVE-2024-7617	The Contact Form to Any API plugin for WordPress is vulnerable to Stored Cross-Site Scripting via Contact Form 7 form fields in all versions up to, and including, 1.2.2 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.	7.2	More Details
CVE-2023-26691	Directory Traversal vulnerability in CS-Cart MultiVendor 4.16.1 allows remote attackers to run arbitrary code via crafted zip file when installing a new add-on.	7.2	More Details
CVE-2024-43191	IBM ManageIQ could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted yaml file request.	7.2	More Details
CVE-2024-8914	The Thanh Toán Quét Mã QR Code Tự Động – MoMo, ViettelPay, VNPay và 40 ngân hàng Việt Nam plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 2.0.1 due to incorrect use of the wp_kses_allowed_html function, which allows the 'onclick' attribute for certain HTML elements without sufficient restriction or context validation. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2024-8349	The Uncanny Groups for LearnDash plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 6.1.0.1. This is due to the plugin not properly restricting what users a group leader can edit. This makes it possible for authenticated attackers, with group leader-level access and above, to change admin account email addresses which can subsequently lead to admin account access.	7.2	More Details
CVE-2024-8704	The Advanced File Manager plugin for WordPress is vulnerable to Local JavaScript File Inclusion in all versions up to, and including, 5.2.8 via the 'fma_locale' 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.	7.2	More Details
CVE-2024-8459	Certain switch models from PLANET Technology store SNMPv3 users' passwords in plaintext within the configuration files, allowing remote attackers with administrator privileges to read the file and obtain the credentials.	7.2	More Details
CVE-2024-46865	In the Linux kernel, the following vulnerability has been resolved: fou: fix initialization of grc The grc must be initialize first. There can be a condition where if fou is NULL, goto out will be executed and grc would be used uninitialized.	7.1	More Details
CVE-2024-43959	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themepoints Testimonials allows Reflected XSS.This issue affects Testimonials: from n/a through 3.0.8.	7.1	More Details
CVE-2024-46854	In the Linux kernel, the following vulnerability has been resolved: net: dpaa: Pad packets to ETH_ZLEN When sending packets under 60 bytes, up to three bytes of the buffer following the data may be leaked. Avoid this by extending all packets to ETH_ZLEN, ensuring nothing is leaked in the padding. This bug can be reproduced by running $ ping -s 11 destination	7.1	More Details
CVE-2024-8981	The Broken Link Checker plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg in /app/admin-notices/features/class-view.php without appropriate escaping on the URL in all versions up to, and including, 2.4.0. 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.	7.1	More Details
CVE-2024-39577	Dell SmartFabric OS10 Software, versions 10.5.6.x, 10.5.5.x, 10.5.4.x, 10.5.3.x, contains an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability leading to code execution.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41673	Decidim is a participatory democracy framework. The version control feature used in resources is subject to potential XSS attack through a malformed URL. This vulnerability is fixed in 0.27.8.	7.1	More Details
CVE-2024-46858	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: Fix uaf in __timer_delete_sync There are two paths to access mptcp_pm_del_add_timer, result in a race condition: CPU1 CPU2 ==== ==== net_rx_action napi_poll netlink_sendmsg __napi_poll netlink_unicast process_backlog netlink_unicast_kernel __netif_receive_skb genl_rcv __netif_receive_skb_one_core netlink_rcv_skb NF_HOOK genl_rcv_msg ip_local_deliver_finish genl_family_rcv_msg ip_protocol_deliver_rcu genl_family_rcv_msg_doit tcp_v4_rcv mptcp_pm_nl_flush_addrs_doit tcp_v4_do_rcv mptcp_nl_remove_addrs_list tcp_rcv_established mptcp_pm_remove_addrs_and_subflows tcp_data_queue remove_anno_list_by_saddr mptcp_incoming_options mptcp_pm_del_add_timer mptcp_pm_del_add_timer kfree(entry) In remove_anno_list_by_saddr(running on CPU2), after leaving the critical zone protected by "pm.lock", the entry will be released, which leads to the occurrence of uaf in the mptcp_pm_del_add_timer(running on CPU1). Keeping a reference to add_timer inside the lock, and calling sk_stop_timer_sync() with this reference, instead of "entry->add_timer". Move list_del(&entry->list) to mptcp_pm_del_add_timer and inside the pm lock, do not directly access any members of the entry outside the pm lock, which can avoid similar "entry->x" uaf.	7.0	More Details
CVE-2023-7273	Cross site request forgery in Kiteworks OwnCloud allows an unauthenticated attacker to forge requests. If a request has no Authorization header, it is created with an empty string as value by a rewrite rule. The CSRF check is done by comparing the header value to null, meaning that the existing CSRF check is bypassed in this case. An attacker can, for example, create a new administrator account if the request is executed in the browser of an authenticated victim.	6.8	More Details
CVE-2021-37577	Bluetooth LE and BR/EDR Secure Connections pairing and Secure Simple Pairing using the Passkey entry protocol in Bluetooth Core Specifications 2.1 through 5.3 may permit an unauthenticated man-in-the-middle attacker to identify the Passkey used during pairing by reflection of a crafted public key with the same X coordinate as the offered public key and by reflection of the authentication evidence of the initiating device, potentially permitting this attacker to complete authenticated pairing with the responding device using the correct Passkey for the pairing session. This is a related issue to CVE-2020-26558.	6.8	More Details
CVE-2024-23924	Alpine Halo9 UPDM_wemCmdCreatSHA256Hash Command Injection Remote Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Alpine Halo9 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the UPDM_wemCmdCreatSHA256Hash function. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-23105	6.8	More Details
CVE-2024-41999	Smart-tab Android app installed April 2023 or earlier contains an active debug code vulnerability. If this vulnerability is exploited, an attacker with physical access to the device may exploit the debug function to gain access to the OS functions, escalate the privilege, change the device's settings, or spoof devices in other rooms.	6.8	More Details
CVE-2024-47071	OSS Endpoint Manager is an endpoint manager module for FreePBX. OSS Endpoint Manager module activation can allow authenticated web users unauthorized access to read system files with the permissions of the webserver process. This vulnerability is fixed in 14.0.4.	6.8	More Details
CVE-2024-23961	Alpine Halo9 UPDM_wemCmdUpdFSpeDecomp Command Injection Remote Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Alpine Halo9 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the UPDM_wemCmdUpdFSpeDecomp function. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-23306	6.8	More Details
CVE-2024-8725	Multiple plugins and/or themes for WordPress are vulnerable to Limited File Upload in various versions. This is due to a lack of proper checks to ensure lower-privileged roles cannot upload .css and .js files to arbitrary directories. This makes it possible for authenticated attackers, with Subscriber-level access and above, and granted permissions by an administrator, to upload .css and .js files to any directory within the WordPress root directory, which could lead to Stored Cross-Site Scripting. The Advanced File Manager Shortcodes plugin must be installed to exploit this vulnerability.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8449	Certain switch models from PLANET Technology have a Hard-coded Credential in the password recovering functionality, allowing an unauthenticated attacker to connect to the device via the serial console and use this credential to reset any user's password.	6.8	More Details
CVE-2022-49039	Out-of-bounds write vulnerability in backup task management functionality in Synology Drive Client before 3.4.0-15721 allows local users with administrator privileges to execute arbitrary commands via unspecified vectors.	6.7	More Details
CVE-2024-30134	The HCL Traveler for Microsoft Outlook executable (HTMO.exe) is being flagged as potentially Malicious Software or an Unrecognized Application.	6.7	More Details
CVE-2024-6769	A DLL Hijacking caused by drive remapping combined with a poisoning of the activation cache in Microsoft Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, and Windows Server 2022 allows a malicious authenticated attacker to elevate from a medium integrity process to a high integrity process without the intervention of a UAC prompt.	6.7	More Details
CVE-2024-9136	Access permission verification vulnerability in the App Multiplier module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.7	More Details
CVE-2024-28810	An issue was discovered in Infinera hiT 7300 5.60.50. Sensitive information inside diagnostic files (exported by the @CT application) allows an attacker to achieve loss of confidentiality by analyzing these files.	6.6	More Details
CVE-2023-3441	An issue has been discovered in GitLab EE/CE affecting all versions starting from 8.0 before 16.4. The product did not sufficiently warn about security implications of granting merge rights to protected branches.	6.6	More Details
CVE-2024-45993	Giflib Project v5.2.2 is vulnerable to a heap buffer overflow via gif2rgb.	6.5	More Details
CVE-2024-39435	In Logmanager service, there is a possible missing verification incorrect input. This could lead to local escalation of privilege with no additional execution privileges needed.	6.5	More Details
CVE-2024-41445	Library MDF (mdflib) v2.1 is vulnerable to a heap-based buffer overread via a crafted mdf4 file is parsed using the ReadData function	6.5	More Details
CVE-2024-25658	Cleartext storage of passwords in Infinera TNMS (Transcend Network Management System) Server 19.10.3 allows attackers (with access to the database or exported configuration files) to obtain SNMP users' usernames and passwords in cleartext.	6.5	More Details
CVE-2024-47303	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Livemesh Livemesh Addons for Elementor allows Stored XSS.This issue affects Livemesh Addons for Elementor: from n/a through 8.5.	6.5	More Details
CVE-2024-9391	A user who enables full-screen mode on a specially crafted web page could potentially be prevented from exiting full screen mode. This may allow spoofing of other sites as the address bar is no longer visible. *This bug only affects Firefox Focus for Android. Other versions of Firefox are unaffected.* This vulnerability affects Firefox < 131.	6.5	More Details
CVE-2022-49037	Insertion of sensitive information into log file vulnerability in proxy settings component in Synology Drive Client before 3.3.0-15082 allows remote authenticated users to obtain sensitive information via unspecified vectors.	6.5	More Details
CVE-2024-47532	RestrictedPython is a restricted execution environment for Python to run untrusted code. A user can gain access to protected (and potentially sensible) information indirectly via AttributeError.obj and the string module. The problem will be fixed in version 7.3. As a workaround, If the application does not require access to the module string, it can remove it from RestrictedPython.Utilities.utility_builtins or otherwise do not make it available in the restricted execution environment.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47077	authentik is an open-source identity provider. Prior to versions 2024.8.3 and 2024.6.5, access tokens issued to one application can be stolen by that application and used to impersonate the user against any other proxy provider. Also, a user can steal an access token they were legitimately issued for one application and use it to access another application that they aren't allowed to access. Anyone who has more than one proxy provider application with different trust domains or different access control is affected. Versions 2024.8.3 and 2024.6.5 fix the issue.	6.5	More Details
CVE-2024-7011	Sharp NEC Projectors (NP-CB4500UL, NP-CB4500WL, NP-CB4700UL, NP-P525UL, NP-P525UL+, NP-P525ULG, NP-P525ULJL, NP-P525WL, NP-P525WL+, NP-P525WLG, NP-P525WLJL, NP-CG6500UL, NP-CG6500WL, NP-CG6700UL, NP-P605UL, NP-P605UL+, NP-P605ULG, NP-P605ULJL, NP-CA4120X, NP-CA4160W, NP-CA4160X, NP-CA4200U, NP-CA4200W, NP-CA4202W, NP-CA4260X, NP-CA4300X, NP-CA4355X, NP-CD2100U, NP-CD2120X, NP-CD2300X, NP-CR2100X, NP-CR2170W, NP-CR2170X, NP-CR2200U, NP-CR2200W, NP-CR2280X, NP-CR2310X, NP-CR2350X, NP-MC302XG, NP-MC332WG, NP-MC332WJL, NP-MC342XG, NP-MC372X, NP-MC372XG, NP-MC382W, NP-MC382WG, NP-MC422XG, NP-ME342UG, NP-ME372W, NP-ME372WG, NP-ME372WJL, NP-ME382U, NP-ME382UG, NP-ME382UJL, NP-ME402X, NP-ME402XG, NP-ME402XJL, NP-CB4500XL, NP-CG6400UL, NP-CG6400WL, NP-CG6500XL, NP-PE455UL, NP-PE455ULG, NP-PE455WL, NP-PE455WLG, NP-PE505XLG, NP-CB4600U, NP-CF6600U, NP-P474U, NP-P554U, NP-P554U+, NP-P554UG, NP-P554UJL, NP-CG6600UL, NP-P547UL, NP-P547ULG, NP-P547ULJL, NP-P607UL+, NP-P627UL, NP-P627UL+, NP-P627ULG, NP-P627ULJL, NP-PV710UL-B, NP-PV710UL-B1, NP-PV710UL-W, NP-PV710UL-W+, NP-PV710UL-W1, NP-PV730UL-BJL, NP-PV730UL-WJL, NP-PV800UL-B, NP-PV800UL-B+, NP-PV800UL-B1, NP-PV800UL-BJL, NP-PV800UL-W, NP-PV800UL-W+, NP-PV800UL-W1, NP-PV800UL-WJL, NP-CA4200X, NP-CA4265X, NP-CA4300U, NP-CA4300W, NP-CA4305X, NP-CA4400X, NP-CD2125X, NP-CD2200W, NP-CD2300U, NP-CD2310X, NP-CR2105X, NP-CR2200X, NP-CR2205W, NP-CR2300U, NP-CR2300W, NP-CR2315X, NP-CR2400X, NP-MC333XG, NP-MC363XG, NP-MC393WJL, NP-MC423W, NP-MC423WG, NP-MC453X, NP-MC453X, NP-MC453XG, NP-MC453XJL, NP-ME383WG, NP-ME403U, NP-ME403UG, NP-ME403UJL, NP-ME423W, NP-ME423WG, NP-ME423WJL, NP-ME453X, NP-ME453XG, NP-CB4400USL, NP-CB4400WSL, NP-CB4510UL, NP-CB4510WL, NP-CB4510XL, NP-CB4550USL, NP-CB6700UL, NP-CG6510UL, NP-PE456USL, NP-PE456USLG, NP-PE456USLJL, NP-PE456WSLG, NP-PE506UL, NP-PE506ULG, NP-PE506ULJL, NP-PE506WL, NP-PE506WLG, NP-PE506WLJL) allows an attacker to cause a denial-of-service (DoS) condition via SNMP service.	6.5	More Details
CVE-2024-9284	A vulnerability was found in TP-LINK TL-WR841ND up to 20240920. It has been rated as critical. Affected by this issue is some unknown functionality of the file /userRpm/popupSiteSurveyRpm.htm. The manipulation of the argument ssid leads to stack-based buffer overflow. 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.	6.5	More Details
CVE-2024-28807	An issue was discovered in Infinera hiT 7300 5.60.50. Cleartext storage of sensitive information in the memory of the @CT desktop management application allows guest OS administrators to obtain various users' passwords by accessing memory dumps of the desktop application.	6.5	More Details
CVE-2024-47641	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPDeveloperr Confetti Fall Animation allows Stored XSS.This issue affects Confetti Fall Animation: from n/a through 1.3.0.	6.5	More Details
CVE-2024-20414	A vulnerability in the web UI feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system through the web UI. This vulnerability is due to incorrectly accepting configuration changes through the HTTP GET method. An attacker could exploit this vulnerability by persuading a currently authenticated administrator to follow a crafted link. A successful exploit could allow the attacker to change the configuration of the affected device.	6.5	More Details
CVE-2024-45372	MZK-DP300N firmware versions 1.04 and earlier contains a cross-site request forger vulnerability. Viewing a malicious page while logging in to the web management page of the affected product may lead the user to perform unintended operations such as changing the login password, etc.	6.5	More Details
CVE-2024-41722	In the goTenna Pro ATAK Plugin there is a vulnerability that makes it possible to inject any custom message with any GID and Callsign using a software defined radio in existing goTenna mesh networks. This vulnerability can be exploited if the device is being used in an unencrypted environment or if the cryptography has already been compromised. It is advised to use encryption shared with local QR code for higher security operations.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45723	The goTenna Pro ATAK Plugin does not use SecureRandom when generating passwords for sharing cryptographic keys. The random function in use makes it easier for attackers to brute force this password if the broadcasted encryption key is captured over RF. This only applies to the optional broadcast of an encryption key, so it is advised to share the key with local QR code for higher security operations.	6.5	More Details
CVE-2024-47396	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in moveaddons Move Addons for Elementor allows Stored XSS.This issue affects Move Addons for Elementor: from n/a through 1.3.3.	6.5	More Details
CVE-2024-45987	Projectworld Online Voting System Version 1.0 is vulnerable to Cross Site Request Forgery (CSRF) via voter.php. This vulnerability allows an attacker to craft a malicious link that, when clicked by an authenticated user, automatically submits a vote for a specified party without the user's consent or knowledge. The attack leverages the user's active session to perform the unauthorized action, compromising the integrity of the voting process.	6.5	More Details
CVE-2024-9355	A vulnerability was found in Golang FIPS OpenSSL. This flaw allows a malicious user to randomly cause an uninitialized buffer length variable with a zeroed buffer to be returned in FIPS mode. It may also be possible to force a false positive match between non-equal hashes when comparing a trusted computed hmac sum to an untrusted input sum if an attacker can send a zeroed buffer in place of a pre-computed sum. It is also possible to force a derived key to be all zeros instead of an unpredictable value. This may have follow-on implications for the Go TLS stack.	6.5	More Details
CVE-2024-47126	The goTenna Pro App does not use SecureRandom when generating passwords for sharing cryptographic keys. The random function in use makes it easier for attackers to brute force this password if the broadcasted encryption key is captured over RF. This only applies to the optional broadcast of an encryption key, so it is advised to share the key with local QR code for higher security operations.	6.5	More Details
CVE-2024-47127	In the goTenna Pro App there is a vulnerability that makes it possible to inject any custom message with any GID and Callsign using a software defined radio in existing goTenna mesh networks. This vulnerability can be exploited if the device is being used in an unencrypted environment or if the cryptography has already been compromised. It is advised to share encryption keys via QR scanning for higher security operations and update your app to the current release for enhanced encryption protocols.	6.5	More Details
CVE-2024-8632	The KB Support – WordPress Help Desk and Knowledge Base plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on the 'kbs_ajax_load_front_end_replies' and 'kbs_ajax_mark_reply_as_read' functions in all versions up to, and including, 1.6.6. This makes it possible for unauthenticated attackers to read replies of any ticket, and mark any reply as read.	6.5	More Details
CVE-2024-23958	Autel MaxiCharger AC Elite Business C50 BLE Hardcoded Credentials Authentication Bypass Vulnerability. This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of Autel MaxiCharger AC Elite Business C50 charging stations. Authentication is not required to exploit this vulnerability. The specific flaw exists within the BLE AppAuthenRequest command handler. The handler uses hardcoded credentials as a fallback in case of an authentication request failure. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-23196	6.5	More Details
CVE-2024-9224	The Hello World plugin for WordPress is vulnerable to Arbitrary File Reading in all versions up to, and including, 2.1.1 via the hello_world_lyric() function. This makes it possible for authenticated attackers, with subscriber-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information.	6.5	More Details
CVE-2024-6512	Authorization bypass in the PAM access request approval mechanism in Devolutions Server 2024.2.10 and earlier allows authenticated users with permissions to approve their own requests, bypassing intended security restrictions, via the PAM access request approval mechanism.	6.5	More Details
CVE-2024-8861	The ProfileGrid – User Profiles, Groups and Communities plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 5.9.3.2 due to incorrect use of the wp_kses_allowed_html function, which allows the 'onclick' attribute for certain HTML elements without sufficient restriction or context validation. 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-2024-8668	The ShopLentor – WooCommerce Builder for Elementor & Gutenberg +12 Modules – All in One Solution (formerly WooLentor) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the tooltip and countdown functionality in all versions up to, and including, 2.9.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9127	The Super Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'alignment' parameter in all versions up to, and including, 3.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8858	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'piechart_settings' parameter in all versions up to, and including, 8.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9125	The king_IE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0 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-2024-9118	The QS Dark Mode Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.9 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-2024-8288	The Guten Post Layout – An Advanced Post Grid Collection for WordPress Gutenberg plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' attribute within the 'wp:guten-post-layout/post-grid' Gutenberg block in all versions up to, and including, 1.2.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9117	The Mapplic Lite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0 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-2024-9115	The Common Tools for Site plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.2 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-2024-9274	The Elastik Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 0.27.4 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-2024-8324	The XO Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'get_slider' function in all versions up to, and including, 3.8.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9272	The R Animated Icon Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0 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-2024-9304	The LocateAndFilter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.6.14 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-2024-9119	The SVG Complete plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.2 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-2024-8723	The 012 Ps Multi Languages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via translated titles in all versions up to, and including, 1.6 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8515	The Themesflat Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several widgets like 'TF E Slider Widget', 'TF Video Widget', 'TF Team Widget' and more in all versions up to, and including, 2.2.1 due to insufficient input sanitization and output escaping on URL 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-2024-8103	The WP Category Dropdown plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' parameter in all versions up to, and including, 1.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9073	The GutenGeek Free Gutenberg Blocks for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.1.3 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-2024-9069	The Graphicsly – The ultimate graphics plugin for WordPress website builder (Gutenberg, Elementor, Beaver Builder, WPBakery) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.2 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-2024-9269	The Relogo plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 0.4.2 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-2024-9060	The AVIF & SVG Uploader plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in version 1.1.0 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-2024-9024	The Material Design Icons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's mdi-icon shortcode in all versions up to, and including, 0.0.5 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-2024-9068	The OneElements – Best Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.3.7 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-2024-9028	The WP GPX Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'sgpx' shortcode in all versions up to, and including, 1.7.08 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-2024-9027	The WPZOOM Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'box' shortcode in all versions up to, and including, 1.0.5 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 Number	Description	Base Score	Reference
CVE-2024-9023	The WP-WebAuthn plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wwa_login_form shortcode in all versions up to, and including, 1.3.1 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-2024-8547	The Simple Popup Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's [popup] shortcode in all versions up to, and including, 4.5 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-2024-8546	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Video widget in all versions up to, and including, 3.2.7 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-2024-8107	The Slider Revolution plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 6.7.18 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. By default, this can only be exploited by administrators, but the ability to use and configure Slider Revolution can be extended to authors.	6.4	More Details
CVE-2024-8681	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Media Grid widget in all versions up to, and including, 4.10.52 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-2024-8990	The Geo Mashup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's geo_mashup_visible_posts_list shortcode in all versions up to, and including, 1.13.13 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-2024-9049	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Button Group module in all versions up to, and including, 2.8.3.6 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-2024-8917	The AnWP Football Leagues plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 0.16.7 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-2024-8720	The RumbleTalk Live Group Chat – HTML5 plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'rumbletalk-admin-button' shortcode in all versions up to, and including, 6.3.0 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-2024-8989	The Free Responsive Testimonials, Social Proof Reviews, and Customer Reviews – Stars Testimonials plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's stars_testimonials shortcode in all versions up to, and including, 3.3.1 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 Number	Description	Base Score	Reference
CVE-2024-8991	The OSM – OpenStreetMap plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's osm_map and osm_map_v3 shortcodes in all versions up to, and including, 6.1.0 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-2024-47075	LayUI is a native minimalist modular Web UI component library. Versions prior to 2.9.17 have a DOM Clobbering vulnerability that can lead to Cross-site Scripting (XSS) on web pages where attacker-controlled HTML elements (e.g., `img` tags with unsanitized `name` attributes) are present. Version 2.9.17 fixes this issue.	6.4	More Details
CVE-2024-8267	The Radio Player – Live Shoutcast, Icecast and Any Audio Stream Player for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'align' attribute within the 'wp:radio-player' Gutenberg block in all versions up to, and including, 2.0.78 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8965	The Absolute Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Name' field of a custom post criteria in all versions up to, and including, 1.1.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8919	The Confetti Fall Animation plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'confetti-fall-animation' shortcode in all versions up to, and including, 1.3.0 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-2024-20475	A vulnerability in the web-based management interface of Cisco Catalyst SD-WAN Manager, formerly Cisco SD-WAN vManage, could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface.	6.4	More Details
CVE-2024-9173	The GF Custom Style plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.0 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-2024-9177	The Themedy Toolbox plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's themedy_col, themedy_social_link, themedy_alertbox, and themedy_pullleft shortcodes in all versions up to, and including, 1.0.14, and up to, and including 1.0.15 for the plugin's themedy_button shortcode 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-2024-9328	A vulnerability was found in SourceCodester Advocate Office Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /control/edit_client.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-2024-9327	A vulnerability was found in code-projects Blood Bank System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /forgot.php. The manipulation of the argument useremail 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-2024-8942	Vulnerability in Scriptcase version 9.4.019 that consists of a Cross-Site Scripting (XSS), due to the lack of input validation, affecting the “id_form_msg_title” parameter, among others. This vulnerability could allow a remote user to send a specially crafted URL to a victim and retrieve their credentials.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6590	The Spreadsheet Integration – Automate Google Sheets With WordPress, WooCommerce & Most Popular Form Plugins. Also, Display Google sheet as a Table. plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several functions in all versions up to, and including, 3.7.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to edit post status, edit Google sheet integrations, and create Google sheet integrations.	6.3	More Details
CVE-2024-9275	A vulnerability was found in jeanmarc77 123solar up to 1.8.4.5. It has been rated as critical. This issue affects some unknown processing of the file /admin/admin_invt2.php. The manipulation of the argument PROTOCOLx leads to file inclusion. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9293	A vulnerability classified as critical was found in skyselang yylAdmin up to 3.0. Affected by this vulnerability is the function list of the file /app/admin/controller/file/File.php of the component Backend. The manipulation of the argument is_disable 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-2024-39364	Advantech ADAM-5630 has built-in commands that can be executed without authenticating the user. These commands allow for restarting the operating system, rebooting the hardware, and stopping the execution. The commands can be sent to a simple HTTP request and are executed by the device automatically, without discrimination of origin or level of privileges of the user sending the commands.	6.3	More Details
CVE-2024-46257	A Command injection vulnerability in requestLetsEncryptSslWithDnsChallenge in NginxProxyManager 2.11.3 allows an attacker to achieve remote code execution via Add Let's Encrypt Certificate. NOTE: this is not part of any NGINX software shipped by F5.	6.3	More Details
CVE-2024-46485	dingfanzu CMS 1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admin/doAdminAction.php?act=addCate	6.3	More Details
CVE-2024-9297	A vulnerability was found in SourceCodester Online Railway Reservation System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/. The manipulation of the argument page with the input trains/schedules/system_info leads to improper authorization. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9294	A vulnerability, which was classified as critical, has been found in dingfanzu CMS up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. Affected by this issue is some unknown functionality of the file saveNewPwd.php. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	6.3	More Details
CVE-2024-9319	A vulnerability, which was classified as critical, was found in SourceCodester Online Timesheet App 1.0. This affects an unknown part of the file /endpoint/delete-timesheet.php. The manipulation of the argument timesheet 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-2024-46540	A remote code execution (RCE) vulnerability in the component /admin/store.php of Emlog Pro before v2.3.15 allows attackers to use remote file downloads and self-extract fucntions to upload webshells to the target server, thereby obtaining system privileges.	6.3	More Details
CVE-2024-9315	A vulnerability was found in SourceCodester Employee and Visitor Gate Pass Logging System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /admin/maintenance/manage_department.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-2024-9316	A vulnerability classified as critical has been found in code-projects Blood Bank Management System 1.0. Affected is an unknown function of the file /admin/blood/update/B+.php. The manipulation of the argument Bloodname 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-2024-9317	A vulnerability classified as critical was found in SourceCodester Online Eyewear Shop 1.0. Affected by this vulnerability is the function delete_category of the file /classes/Master.php?f=delete_category. 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.	6.3	More Details
CVE-2024-9318	A vulnerability, which was classified as critical, has been found in SourceCodester Advocate Office Management System 1.0. Affected by this issue is some unknown functionality of the file /control/activate.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-2024-46548	TP-Link Tapo P125M and Kasa KP125M v1.0.3 was discovered to improperly validate certificates, allowing attackers to eavesdrop on communications and access sensitive information via a man-in-the-middle attack.	6.3	More Details
CVE-2024-9322	A vulnerability was found in code-projects Supply Chain Management 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/edit_manufacturer.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-2024-9324	A vulnerability was found in Intelbras InControl up to 2.21.57. It has been rated as critical. Affected by this issue is some unknown functionality of the file /v1/operador/ of the component Relatório de Operadores Page. The manipulation of the argument fields leads to code injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2.21.58 is able to address this issue. It is recommended to upgrade the affected component. The vendor was informed early on 2024-07-19 about this issue. The release of a fixed version 2.21.58 was announced for the end of August 2024 but then was postponed until 2024-09-20.	6.3	More Details
CVE-2024-45983	A Cross-Site Request Forgery (CSRF) vulnerability exists in kishan0725's Hospital Management System version 6.3.5. The vulnerability allows an attacker to craft a malicious HTML form that submits a request to delete a doctor record. By enticing an authenticated admin user to visit the specially crafted web page, the attacker can leverage the victim's browser to make unauthorized requests to the vulnerable endpoint, effectively allowing the attacker to perform actions on behalf of the admin without their consent.	6.3	More Details
CVE-2024-45200	In Nintendo Mario Kart 8 Deluxe before 3.0.3, the LAN/LDN local multiplayer implementation allows a remote attacker to exploit a stack-based buffer overflow upon deserialization of session information via a malformed browse-reply packet, aka KartLANPwn. The victim is not required to join a game session with an attacker. The victim must open the "Wireless Play" (or "LAN Play") menu from the game's title screen, and an attacker nearby (LDN) or on the same LAN network as the victim can send a crafted reply packet to the victim's console. This enables a remote attacker to obtain complete denial-of-service on the game's process, or potentially, remote code execution on the victim's console. The issue is caused by incorrect use of the Nintendo Pia library,	6.3	More Details
CVE-2024-39433	In drm service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	6.2	More Details
CVE-2024-23454	Apache Hadoop’s RunJar.run() does not set permissions for temporary directory by default. If sensitive data will be present in this file, all the other local users may be able to view the content. This is because, on unix-like systems, the system temporary directory is shared between all local users. As such, files written in this directory, without setting the correct posix permissions explicitly, may be viewable by all other local users.	6.2	More Details
CVE-2024-47292	Path traversal vulnerability in the Bluetooth module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.2	More Details
CVE-2024-39434	In drm service, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	6.2	More Details
CVE-2024-46934	Rocket.Chat 6.12.0, 6.11.2, 6.10.5, 6.9.6, 6.8.6, 6.7.8, and earlier is vulnerable to DOM-based Cross-site Scripting (XSS). Attackers may be able to abuse the UpdateOTRAck method to forge a message that contains an XSS payload.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47184	Ampache is a web based audio/video streaming application and file manager. Prior to version 6.6.0, the Democratic Playlist Name is vulnerable to a stored cross-site scripting. Version 6.6.0 fixes this issue.	6.1	More Details
CVE-2024-25411	A cross-site scripting (XSS) vulnerability in Flatpress v1.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the username parameter in setup.php.	6.1	More Details
CVE-2024-8727	The DK PDF 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, 1.9.6. 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-2024-9267	The Easy WordPress Subscribe – Optin Hound 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, 1.4.3. 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-2024-25412	A cross-site scripting (XSS) vulnerability in Flatpress v1.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the email field.	6.1	More Details
CVE-2024-8405	An arbitrary file creation vulnerability exists in PaperCut NG/MF that only affects Windows servers with Web Print enabled. This specific flaw exists within the web-print.exe process, which can incorrectly create files that don't exist when a maliciously formed payload is provided. This can be used to flood disk space and result in a Denial of Service (DoS) attack. Note: This CVE has been split from CVE-2024-4712.	6.1	More Details
CVE-2024-9228	The Loggedin – Limit Active Logins 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, 1.3.1. 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. This is only exploitable when the leave a review notice is present.	6.1	More Details
CVE-2024-8803	The Bulk NoIndex & NoFollow Toolkit plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.15. 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-2024-47067	AList is a file list program that supports multiple storages. AList contains a reflected cross-site scripting vulnerability in helper.go. The endpoint /i/:link_name takes in a user-provided value and reflects it back in the response. The endpoint returns an application/xml response, opening it up to HTML tags via XHTML and thus leading to a XSS vulnerability. This vulnerability is fixed in 3.29.0.	6.1	More Details
CVE-2024-8872	The Store Hours for WooCommerce 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, 4.3.20. 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-2024-8728	The Easy Load More 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, 1.0.3. 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-2024-8718	The Gravity Forms Toolbar plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 1.7.0 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-46470	Cross Site Scripting vulnerability in CodeAstro Membership Management System 1.0 allows attackers to run malicious JavaScript via the membership_type field in the edit-type.php component.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47063	Computer Vision Annotation Tool (CVAT) is an interactive video and image annotation tool for computer vision. If a malicious CVAT user with permissions to either create a task, or edit an existing task can trick another logged-in user into visiting a maliciously-constructed URL, they can initiate any API calls on that user's behalf. This gives the attacker temporary access to all data that the victim user has access to. Upgrade to CVAT 2.19.0 or a later version to fix this issue.	6.1	More Details
CVE-2024-9220	The LH Copy Media File 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, 1.08. 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-2024-47064	Computer Vision Annotation Tool (CVAT) is an interactive video and image annotation tool for computer vision. If an attacker can trick a logged-in CVAT user into visiting a maliciously-constructed URL, they can initiate any API calls on that user's behalf. This gives the attacker temporary access to all data that the victim user has access to. Upgrade to CVAT 2.19.0 or a later version to fix this issue.	6.1	More Details
CVE-2024-8715	The Simple LDAP Login 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, 1.6.0. 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-2024-9241	The PDF Image Generator 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, 1.5.6. 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-2024-46453	A cross-site scripting (XSS) vulnerability in the component /test/ of iq3xcite v2.31 to v3.05 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2024-8549	The Simple Calendar – Google Calendar Plugin 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, 3.4.2. 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-2024-45836	Cross-site scripting vulnerability exists in the web management page of PLANEX COMMUNICATIONS network cameras. If a logged-in user accesses a specific file, an arbitrary script may be executed on the web browser of the user.	6.1	More Details
CVE-2024-45613	CKEditor 5 is a JavaScript rich-text editor. Starting in version 40.0.0 and prior to version 43.1.1, a Cross-Site Scripting (XSS) vulnerability is present in the CKEditor 5 clipboard package. This vulnerability could be triggered by a specific user action, leading to unauthorized JavaScript code execution, if the attacker managed to insert a malicious content into the editor, which might happen with a very specific editor configuration. This vulnerability only affects installations where the Block Toolbar plugin is enabled and either the General HTML Support (with a configuration that permits unsafe markup) or the HTML Embed plugin is also enabled. A fix for the problem is available in version 43.1.1. As a workaround, one may disable the block toolbar plugin.	6.1	More Details
CVE-2024-46655	A reflected cross-site scripting (XSS) vulnerability in Ellevo 6.2.0.38160 allows attackers to execute arbitrary code in the context of a user's browser via a crafted payload or URL.	6.1	More Details
CVE-2024-20496	A vulnerability in the UDP packet validation code of Cisco SD-WAN vEdge Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected system. This vulnerability is due to incorrect handling of a specific type of malformed UDP packet. An attacker in a machine-in-the-middle position could exploit this vulnerability by sending crafted UDP packets to an affected device. A successful exploit could allow the attacker to cause the device to reboot, resulting in a DoS condition on the affected system.	6.1	More Details
CVE-2024-8786	The Auto Featured Image from Title 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, 2.3. 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-2024-8793	The Store Exporter for WooCommerce – Export Products, Export Orders, Export Subscriptions, and More 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, 2.7.2.1. 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-2024-8799	The Custom Banners 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, 3.3. 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-2024-9209	The WP Search Analytics 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, 1.4.10. 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-2024-47186	Filament is a collection of full-stack components for Laravel development. Versions of Filament from v3.0.0 through v3.2.114 are affected by a cross-site scripting (XSS) vulnerability. If values passed to a `ColorColumn` or `ColumnEntry` are not valid and contain a specific set of characters, applications are vulnerable to XSS attack against a user who opens a page on which a color column or entry is rendered. Filament v3.2.115 fixes this issue.	6.1	More Details
CVE-2024-6517	The Contact Form 7 Math Captcha WordPress plugin through 2.0.1 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users.	6.1	More Details
CVE-2024-8712	The GTM Server Side 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, 2.1.19. 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-2024-46079	Scriptcase v9.10.023 and before is vulnerable to Cross Site Scripting (XSS) in proj_new.php via the Descricao parameter.	6.1	More Details
CVE-2024-41930	Cross-site scripting vulnerability exists in MF Teacher Performance Management System version 6. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the user who accessed the website using the product.	6.1	More Details
CVE-2024-8741	The Beam me up Scotty – Back to Top Button 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, 1.0.21. 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-2024-8788	The EU/UK VAT Manager for WooCommerce 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, 2.12.11. 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-2024-8713	The Kodex Posts likes 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, 2.5.0. 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-2024-9397	A missing delay in directory upload UI could have made it possible for an attacker to trick a user into granting permission via clickjacking. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	6.1	More Details
CVE-2024-9329	In Eclipse Glassfish versions before 7.0.17, The Host HTTP parameter could cause the web application to redirect to the specified URL, when the requested endpoint is '/management/domain'. By modifying the URL value to a malicious site, an attacker may successfully launch a phishing scam and steal user credentials.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38324	IBM Storage Defender 2.0.0 through 2.0.7 on-prem defender-sensor-cmd CLI does not validate server name during registration and unregistration operations which could expose sensitive information to an attacker with access to the system.	5.9	More Details
CVE-2024-47174	Nix is a package manager for Linux and other Unix systems. Starting in version 1.11 and prior to versions 2.18.8 and 2.24.8, `<nix/fetchurl.nix>` did not verify TLS certificates on HTTPS connections. This could lead to connection details such as full URLs or credentials leaking in case of a man-in-the-middle (MITM) attack. `<nix/fetchurl.nix>` is also known as the builtin derivation builder `builtin:fetchurl`. It's not to be confused with the evaluation-time function `builtins.fetchurl`, which was not affected by this issue. A user may be affected by the risk of leaking credentials if they have a `netrc` file for authentication, or rely on derivations with `impureEnvVars` set to use credentials from the environment. In addition, the commonplace trust-on-first-use (TOFU) technique of updating dependencies by specifying an invalid hash and obtaining it from a remote store was also vulnerable to a MITM injecting arbitrary store objects. This also applied to the impure derivations experimental feature. Note that this may also happen when using Nixpkgs fetchers to obtain new hashes when not using the fake hash method, although that mechanism is not implemented in Nix itself but rather in Nixpkgs using a fixed-output derivation. The behavior was introduced in version 1.11 to make it consistent with the Nixpkgs `pkgs.fetchurl` and to make `<nix/fetchurl.nix>` work in the derivation builder sandbox, which back then did not have access to the CA bundles by default. Nowadays, CA bundles are bind-mounted on Linux. This issue has been fixed in Nix 2.18.8 and 2.24.8. As a workaround, implement (authenticated) fetching with `pkgs.fetchurl` from Nixpkgs, using `impureEnvVars` and `curlOpts` as needed.	5.9	More Details
CVE-2024-38796	EDK2 contains a vulnerability in the PeCoffLoaderRelocateImage(). An Attacker may cause memory corruption due to an overflow via an adjacent network. A successful exploit of this vulnerability may lead to a loss of Confidentiality, Integrity, and/or Availability.	5.9	More Details
CVE-2024-46635	An issue in the API endpoint /AccountMaster/GetCurrentUserInfo of INROAD before v202402060 allows attackers to access sensitive information via a crafted payload to the UserNameOrPhoneNumber parameter.	5.9	More Details
CVE-2024-9199	Rate limit vulnerability in Clibo Manager v1.1.9.2 that could allow an attacker to send a large number of emails to the victim in a short time, affecting availability and leading to a denial of service (DoS).	5.8	More Details
CVE-2024-20465	A vulnerability in the access control list (ACL) programming of Cisco IOS Software running on Cisco Industrial Ethernet 4000, 4010, and 5000 Series Switches could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to the incorrect handling of IPv4 ACLs on switched virtual interfaces when an administrator enables and disables Resilient Ethernet Protocol (REP). An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to bypass an ACL on the affected device.	5.8	More Details
CVE-2024-20508	A vulnerability in Cisco Unified Threat Defense (UTD) Snort Intrusion Prevention System (IPS) Engine for Cisco IOS XE Software could allow an unauthenticated, remote attacker to bypass configured security policies or cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of HTTP requests when they are processed by Cisco UTD Snort IPS Engine. An attacker could exploit this vulnerability by sending a crafted HTTP request through an affected device. A successful exploit could allow the attacker to trigger a reload of the Snort process. If the action in case of Cisco UTD Snort IPS Engine failure is set to the default, fail-open, successful exploitation of this vulnerability could allow the attacker to bypass configured security policies. If the action in case of Cisco UTD Snort IPS Engine failure is set to fail-close, successful exploitation of this vulnerability could cause traffic that is configured to be inspected by Cisco UTD Snort IPS Engine to be dropped.	5.8	More Details
CVE-2024-34542	Advantech ADAM-5630 shares user credentials plain text between the device and the user source device during the login process.	5.7	More Details
CVE-2024-37187	Advantech ADAM-5550 share user credentials with a low level of encryption, consisting of base 64 encoding.	5.7	More Details
CVE-2024-46327	An issue in the Http_handle object of VONETS VAP11G-300 v3.3.23.6.9 allows attackers to access sensitive files via a directory traversal.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44744	An issue in Malwarebytes Premium Security v5.0.0.883 allows attackers to execute arbitrary code via placing crafted binaries into unspecified directories. NOTE: Malwarebytes argues that this issue requires admin privileges and that the contents cannot be altered by non-admin users.	5.7	More Details
CVE-2024-44610	PCAN-Ethernet Gateway FD before 1.3.0 and PCAN-Ethernet Gateway before 2.11.0 are vulnerable to Command injection via shell metacharacters in a Software Update to processing.php.	5.6	More Details
CVE-2024-47291	Permission vulnerability in the ActivityManagerService (AMS) module Impact: Successful exploitation of this vulnerability may affect availability.	5.6	More Details
CVE-2024-4278	An information disclosure issue has been discovered in GitLab EE affecting all versions starting from 16.5 prior to 17.2.8, from 17.3 prior to 17.3.4, and from 17.4 prior to 17.4.1. A maintainer could obtain a Dependency Proxy password by editing a certain Dependency Proxy setting.	5.5	More Details
CVE-2024-46488	sqlite-vec v0.1.1 was discovered to contain a heap buffer overflow via the npy_token_next function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted file.	5.5	More Details
CVE-2024-7421	An information exposure in Devolutions Remote Desktop Manager 2024.2.20.0 and earlier on Windows allows local attackers with access to system logs to obtain session credentials via passwords included in command-line arguments when launching WinSCP sessions	5.5	More Details
CVE-2024-46805	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix the waring dereferencing hive Check the amdgpu_hive_info *hive that maybe is NULL.	5.5	More Details
CVE-2024-46840	In the Linux kernel, the following vulnerability has been resolved: btrfs: clean up our handling of refs == 0 in snapshot delete In reada we BUG_ON(refs == 0), which could be unkind since we aren't holding a lock on the extent leaf and thus could get a transient incorrect answer. In walk_down_proc we also BUG_ON(refs == 0), which could happen if we have extent tree corruption. Change that to return -EUCLEAN. In do_walk_down() we catch this case and handle it correctly, however we return -EIO, which -EUCLEAN is a more appropriate error code. Finally in walk_up_proc we have the same BUG_ON(refs == 0), so convert that to proper error handling. Also adjust the error message so we can actually do something with the information.	5.5	More Details
CVE-2024-46847	In the Linux kernel, the following vulnerability has been resolved: mm: vmalloc: ensure vmap_block is initialised before adding to queue Commit 8c61291fd850 ("mm: fix incorrect vbq reference in purge_fragmented_block") extended the 'vmap_block' structure to contain a 'cpu' field which is set at allocation time to the id of the initialising CPU. When a new 'vmap_block' is being instantiated by new_vmap_block(), the partially initialised structure is added to the local 'vmap_block_queue' xarray before the 'cpu' field has been initialised. If another CPU is concurrently walking the xarray (e.g. via vm_unmap_aliases()), then it may perform an out-of-bounds access to the remote queue thanks to an uninitialised index. This has been observed as UBSAN errors in Android: I Internal error: UBSAN: array index out of bounds: 00000000f2005512 [#1] PREEMPT SMP I I Call trace: I purge_fragmented_block+0x204/0x21c I _vm_unmap_aliases+0x170/0x378 I vm_unmap_aliases+0x1c/0x28 I change_memory_common+0x1dc/0x26c I set_memory_ro+0x18/0x24 I module_enable_ro+0x98/0x238 I do_init_module+0x1b0/0x310 Move the initialisation of 'vb->cpu' in new_vmap_block() ahead of the addition to the xarray.	5.5	More Details
CVE-2024-46843	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Remove SCSI host only if added If host tries to remove ufshcd driver from a UFS device it would cause a kernel panic if ufshcd_async_scan fails during ufshcd_probe_hba before adding a SCSI host with scsi_add_host and MCQ is enabled since SCSI host has been defered after MCQ configuration introduced by commit 0cab4023ec7b ("scsi: ufs: core: Defer adding host to SCSI if MCQ is supported"). To guarantee that SCSI host is removed only if it has been added, set the scsi_host_added flag to true after adding a SCSI host and check whether it is set or not before removing it.	5.5	More Details
CVE-2024-46841	In the Linux kernel, the following vulnerability has been resolved: btrfs: don't BUG_ON on ENOMEM from btrfs_lookup_extent_info() in walk_down_proc() We handle errors here properly, ENOMEM isn't fatal, return the error.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46838	In the Linux kernel, the following vulnerability has been resolved: userfaultfd: don't BUG_ON() if khugepaged yanks our page table Since khugepaged was changed to allow retracting page tables in file mappings without holding the mmap lock, these BUG_ON()s are wrong - get rid of them. We could also remove the preceding "if (unlikely(...))" block, but then we could reach pte_offset_map_lock() with transhuge pages not just for file mappings but also for anonymous mappings - which would probably be fine but I think is not necessarily expected.	5.5	More Details
CVE-2024-46837	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Restrict high priorities on group_create We were allowing any users to create a high priority group without any permission checks. As a result, this was allowing possible denial of service. We now only allow the DRM master or users with the CAP_SYS_NICE capability to set higher priorities than PANTHOR_GROUP_PRIORITY_MEDIUM. As the sole user of that uAPI lives in Mesa and hardcode a value of MEDIUM [1], this should be safe to do. Additionally, as those checks are performed at the ioctl level, panthor_group_create now only check for priority level validity. [1]https://gitlab.freedesktop.org/mesa/mesa/-/blob/f390835074bdf162a63deb0311d1a6de527f9f89/src/gallium/drivers/panfrost/pan_csf.c#L1038	5.5	More Details
CVE-2024-46835	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix smatch static checker warning adev->gfx.imu.funcs could be NULL	5.5	More Details
CVE-2024-46834	In the Linux kernel, the following vulnerability has been resolved: ethtool: fail closed if we can't get max channel used in indirection tables Commit 0d1b7d6c9274 ("bnxt: fix crashes when reducing ring count with active RSS contexts") proves that allowing indirection table to contain channels with out of bounds IDs may lead to crashes. Currently the max channel check in the core gets skipped if driver can't fetch the indirection table or when we can't allocate memory. Both of those conditions should be extremely rare but if they do happen we should try to be safe and fail the channel change.	5.5	More Details
CVE-2024-46832	In the Linux kernel, the following vulnerability has been resolved: MIPS: cevt-r4k: Don't call get_c0_compare_int if timer irq is installed This avoids warning: [0.118053] BUG: sleeping function called from invalid context at kernel/locking/mutex.c:283 Caused by get_c0_compare_int on secondary CPU. We also skipped saving IRQ number to struct clock_event_device *cd as it's never used by clockevent core, as per comments it's only meant for "non CPU local devices".	5.5	More Details
CVE-2024-9169	The LiteSpeed Cache plugin for WordPress is vulnerable to Stored Cross-Site Scripting via plugin debug settings in all versions up to, and including, 6.4.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2024-46829	In the Linux kernel, the following vulnerability has been resolved: rtmutex: Drop rt_mutex::wait_lock before scheduling rt_mutex_handle_deadlock() is called with rt_mutex::wait_lock held. In the good case it returns with the lock held and in the deadlock case it emits a warning and goes into an endless scheduling loop with the lock held, which triggers the 'scheduling in atomic' warning. Unlock rt_mutex::wait_lock in the dead lock case before issuing the warning and dropping into the schedule for ever loop. [tglx: Moved unlock before the WARN(), removed the pointless comment, massaged changelog, added Fixes tag]	5.5	More Details
CVE-2024-46827	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix firmware crash due to invalid peer nss Currently, if the access point receives an association request containing an Extended HE Capabilities Information Element with an invalid MCS-NSS, it triggers a firmware crash. This issue arises when EHT-PHY capabilities shows support for a bandwidth and MCS-NSS set for that particular bandwidth is filled by zeros and due to this, driver obtains peer_nss as 0 and sending this value to firmware causes crash. Address this issue by implementing a validation step for the peer_nss value before passing it to the firmware. If the value is greater than zero, proceed with forwarding it to the firmware. However, if the value is invalid, reject the association request to prevent potential firmware crashes. Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.0.1-00029-QCAHKSWPL_SILICONZ-1	5.5	More Details
CVE-2024-46826	In the Linux kernel, the following vulnerability has been resolved: ELF: fix kernel.randomize_va_space double read ELF loader uses "randomize_va_space" twice. It is sysctl and can change at any moment, so 2 loads could see 2 different values in theory with unpredictable consequences. Issue exactly one load for consistent value across one exec.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46825	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: use IWL_FW_CHECK for link ID check The lookup function iwl_mvm_rcu_fw_link_id_to_link_conf() is normally called with input from the firmware, so it should use IWL_FW_CHECK() instead of WARN_ON().	5.5	More Details
CVE-2024-46824	In the Linux kernel, the following vulnerability has been resolved: iommufd: Require drivers to supply the cache_invalidate_user ops If drivers don't do this then iommufd will oops invalidation ioctls with something like: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000086000004 EC = 0x21: IABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault user pgtable: 4k pages, 48-bit VAs, pgdp=0000000101059000 [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000086000004 [#1] PREEMPT SMP Modules linked in: CPU: 2 PID: 371 Comm: qemu-system-aar Not tainted 6.8.0-rc7-gde77230ac23a #9 Hardware name: linux,dummy-virt (DT) pstate: 81400809 (Nzcv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=-c) pc : 0x0 lr : iommufd_hwpt_invalidate+0xa4/0x204 sp : ffff800080f3bcc0 x29: ffff800080f3bcf0 x28: ffff0000c369b300 x27: 0000000000000000 x26: 0000000000000000 x25: 0000000000000000 x24: 0000000000000000 x23: 0000000000000000 x22: 00000000c1e334a0 x21: ffff0000c1e334a0 x20: ffff800080f3bd38 x19: ffff800080f3bd58 x18: 0000000000000000 x17: 0000000000000000 x16: 0000000000000000 x15: 0000ffff8240d6d8 x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : 0000000000000000 x8 : 0000001000000002 x7 : 0000fffeac1ec950 x6 : 0000000000000000 x5 : ffff800080f3bd78 x4 : 0000000000000003 x3 : 0000000000000002 x2 : 0000000000000000 x1 : ffff800080f3bcc8 x0 : ffff0000c6034d80 Call trace: 0x0 iommufd_fops_ioctl+0x154/0x274 __arm64_sys_ioctl+0xac/0xf0 invoke_syscall+0x48/0x110 el0_svc_common.constprop.0+0x40/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x34/0xb4 el0t_64_sync_handler+0x120/0x12c el0t_64_sync+0x190/0x194 All existing drivers implement this op for nesting, this is mostly a bisection aid.	5.5	More Details
CVE-2024-46823	In the Linux kernel, the following vulnerability has been resolved: kunit/overflow: Fix UB in overflow_allocation_test The 'device_name' array doesn't exist out of the 'overflow_allocation_test' function scope. However, it is being used as a driver name when calling 'kunit_driver_create' from 'kunit_device_register'. It produces the kernel panic with KASAN enabled. Since this variable is used in one place only, remove it and pass the device name into kunit_device_register directly as an ascii string.	5.5	More Details
CVE-2024-46822	In the Linux kernel, the following vulnerability has been resolved: arm64: acpi: Harden get_cpu_for_acpi_id() against missing CPU entry In a review discussion of the changes to support vCPU hotplug where a check was added on the GICC being enabled if was online, it was noted that there is need to map back to the cpu and use that to index into a cpumask. As such, a valid ID is needed. If an MPIDR check fails in acpi_map_gic_cpu_interface() it is possible for the entry in cpu_madt_gicc[cpu] == NULL. This function would then cause a NULL pointer dereference. Whilst a path to trigger this has not been established, harden this caller against the possibility.	5.5	More Details
CVE-2023-52949	Missing authentication for critical function vulnerability in proxy settings functionality in Synology Active Backup for Business Agent before 2.7.0-3221 allows local users to obtain user credential via unspecified vectors.	5.5	More Details
CVE-2024-46819	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: the warning dereferencing obj for nbio_v7_4 if ras_manager obj null, don't print NBIO err data	5.5	More Details
CVE-2024-46817	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Stop amdgpu_dm initialize when stream nums greater than 6 [Why] Coverity reports OVERRUN warning. Should abort amdgpu_dm initialize. [How] Return failure to amdgpu_dm_init.	5.5	More Details
CVE-2024-46816	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Stop amdgpu_dm initialize when link nums greater than max_links [Why] Coverity report OVERRUN warning. There are only max_links elements within dc->links. link count could up to AMDGPU_DM_MAX_DISPLAY_INDEX 31. [How] Make sure link count less than max_links.	5.5	More Details
CVE-2024-46802	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: added NULL check at start of dc_validate_stream [Why] prevent invalid memory access [How] check if dc and stream are NULL	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46803	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Check debug trap enable before write dbg_ev_file In interrupt context, write dbg_ev_file will be run by work queue. It will cause write dbg_ev_file execution after debug_trap_disable, which will cause NULL pointer access. v2: cancel work "debug_event_workarea" before set dbg_ev_file as NULL.	5.5	More Details
CVE-2024-46810	In the Linux kernel, the following vulnerability has been resolved: drm/bridge: tc358767: Check if fully initialized before signalling HPD event via IRQ Make sure the connector is fully initialized before signalling any HPD events via drm_kms_helper_hotplug_event(), otherwise this may lead to NULL pointer dereference.	5.5	More Details
CVE-2024-46809	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check BIOS images before it is used BIOS images may fail to load and null checks are added before they are used. This fixes 6 NULL_RETURNS issues reported by Coverity.	5.5	More Details
CVE-2024-46808	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add missing NULL pointer check within dpcd_extend_address_range [Why & How] ASSERT if return NULL from kcalloc.	5.5	More Details
CVE-2024-46807	In the Linux kernel, the following vulnerability has been resolved: drm/amd/amdgpu: Check tbo resource pointer Validate tbo resource pointer, skip if NULL	5.5	More Details
CVE-2024-46846	In the Linux kernel, the following vulnerability has been resolved: spi: rockchip: Resolve unbalanced runtime PM / system PM handling Commit e882575efc77 ("spi: rockchip: Suspend and resume the bus during NOIRQ_SYSTEM_SLEEP_PM ops") stopped respecting runtime PM status and simply disabled clocks unconditionally when suspending the system. This causes problems when the device is already runtime suspended when we go to sleep -- in which case we double-disable clocks and produce a WARNing. Switch back to pm_runtime_force_{suspend,resume}(), because that still seems like the right thing to do, and the aforementioned commit makes no explanation why it stopped using it. Also, refactor some of the resume() error handling, because it's not actually a good idea to re-disable clocks on failure.	5.5	More Details
CVE-2024-46842	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Handle mailbox timeouts in lpfc_get_sfp_info The MBX_TIMEOUT return code is not handled in lpfc_get_sfp_info and the routine unconditionally frees submitted mailbox commands regardless of return status. The issue is that for MBX_TIMEOUT cases, when firmware returns SFP information at a later time, that same mailbox memory region references previously freed memory in its cmpl routine. Fix by adding checks for the MBX_TIMEOUT return code. During mailbox resource cleanup, check the mbox flag to make sure that the wait did not timeout. If the MBOX_WAKE flag is not set, then do not free the resources because it will be freed when firmware completes the mailbox at a later time in its cmpl routine. Also, increase the timeout from 30 to 60 seconds to accommodate boot scripts requiring longer timeouts.	5.5	More Details
CVE-2024-46848	In the Linux kernel, the following vulnerability has been resolved: perf/x86/intel: Limit the period on Haswell Running the ltp test cve-2015-3290 concurrently reports the following warnings. perfevents: irq loop stuck! WARNING: CPU: 31 PID: 32438 at arch/x86/events/intel/core.c:3174 intel_pmu_handle_irq+0x285/0x370 Call Trace: <NMI> ? __warn+0xa4/0x220 ? intel_pmu_handle_irq+0x285/0x370 ? __report_bug+0x123/0x130 ? intel_pmu_handle_irq+0x285/0x370 ? __report_bug+0x123/0x130 ? intel_pmu_handle_irq+0x285/0x370 ? report_bug+0x3e/0xa0 ? handle_bug+0x3c/0x70 ? exc_invalid_op+0x18/0x50 ? asm_exc_invalid_op+0x1a/0x20 ? irq_work_claim+0x1e/0x40 ? intel_pmu_handle_irq+0x285/0x370 perf_event_nmi_handler+0x3d/0x60 nmi_handle+0x104/0x330 Thanks to Thomas Gleixner's analysis, the issue is caused by the low initial period (1) of the frequency estimation algorithm, which triggers the defects of the HW, specifically erratum HSW11 and HSW143. (For the details, please refer https://lore.kernel.org/lkml/87plq9l5d2.ffs@tglx/) The HSW11 requires a period larger than 100 for the INST_RETIRED.ALL event, but the initial period in the freq mode is 1. The erratum is the same as the BDM11, which has been supported in the kernel. A minimum period of 128 is enforced as well on HSW. HSW143 is regarding that the fixed counter 1 may overcount 32 with the Hyper-Threading is enabled. However, based on the test, the hardware has more issues than it tells. Besides the fixed counter 1, the message 'interrupt took too long' can be observed on any counter which was armed with a period < 32 and two events expired in the same NMI. A minimum period of 32 is enforced for the rest of the events. The recommended workaround code of the HSW143 is not implemented. Because it only addresses the issue for the fixed counter. It brings extra overhead through extra MSR writing. No related overcounting issue has been reported so far.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46860	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7921: fix NULL pointer access in mt7921_ipv6_addr_change When disabling wifi mt7921_ipv6_addr_change() is called as a notifier. At this point mvif->phy is already NULL so we cannot use it here.	5.5	More Details
CVE-2024-46806	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix the warning division or modulo by zero Checks the partition mode and returns an error for an invalid mode.	5.5	More Details
CVE-2024-46869	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btintel_pcie: Allocate memory for driver private data Fix driver not allocating memory for struct btintel_data which is used to store internal data.	5.5	More Details
CVE-2024-46868	In the Linux kernel, the following vulnerability has been resolved: firmware: qcom: uefisecapp: Fix deadlock in qcuefi_acquire() If the __qcuefi pointer is not set, then in the original code, we would hold onto the lock. That means that if we tried to set it later, then it would cause a deadlock. Drop the lock on the error path. That's what all the callers are expecting.	5.5	More Details
CVE-2024-46867	In the Linux kernel, the following vulnerability has been resolved: drm/xe/client: fix deadlock in show_meminfo() There is a real deadlock as well as sleeping in atomic() bug in here, if the bo put happens to be the last ref, since bo destruction wants to grab the same spinlock and sleeping locks. Fix that by dropping the ref using xe_bo_put_deferred(), and moving the final commit outside of the lock. Dropping the lock around the put is tricky since the bo can go out of scope and delete itself from the list, making it difficult to navigate to the next list entry. (cherry picked from commit 0083b8e6f11d7662283a267d4ce7c966812ffd8a)	5.5	More Details
CVE-2024-46866	In the Linux kernel, the following vulnerability has been resolved: drm/xe/client: add missing bo locking in show_meminfo() bo_meminfo() wants to inspect bo state like tt and the ttm resource, however this state can change at any point leading to stuff like NPD and UAF, if the bo lock is not held. Grab the bo lock when calling bo_meminfo(), ensuring we drop any spinlocks first. In the case of object_idr we now also need to hold a ref. v2 (MattB) - Also add xe_bo_assert_held() (cherry picked from commit 4f63d712fa104c3ebefcb289d1e733e86d8698c7)	5.5	More Details
CVE-2024-46863	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: soc-acpi-intel-lnl-match: add missing empty item There is no links_num in struct snd_soc_acpi_mach {}, and we test !link->num_adr as a condition to end the loop in hda_sdw_machine_select(). So an empty item in struct snd_soc_acpi_link_adr array is required.	5.5	More Details
CVE-2024-46862	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: soc-acpi-intel-mtl-match: add missing empty item There is no links_num in struct snd_soc_acpi_mach {}, and we test !link->num_adr as a condition to end the loop in hda_sdw_machine_select(). So an empty item in struct snd_soc_acpi_link_adr array is required.	5.5	More Details
CVE-2024-46861	In the Linux kernel, the following vulnerability has been resolved: usbnet: ipheth: do not stop RX on failing RX callback RX callbacks can fail for multiple reasons: * Payload too short * Payload formatted incorrecly (e.g. bad NCM framing) * Lack of memory None of these should cause the driver to seize up. Make such failures non-critical and continue processing further incoming URBs.	5.5	More Details
CVE-2024-46864	In the Linux kernel, the following vulnerability has been resolved: x86/hyperv: fix kexec crash due to VP assist page corruption commit 9636be85cc5b ("x86/hyperv: Fix hyperv_pcpu_input_arg handling when CPUs go online/offline") introduces a new cpuhp state for hyperv initialization. cpuhp_setup_state() returns the state number if state is CPUHP_AP_ONLINE_DYN or CPUHP_BP_PREPARE_DYN and 0 for all other states. For the hyperv case, since a new cpuhp state was introduced it would return 0. However, in hv_machine_shutdown(), the cpuhp_remove_state() call is conditioned upon "hyperv_init_cpuhp > 0". This will never be true and so hv_cpu_die() won't be called on all CPUs. This means the VP assist page won't be reset. When the kexec kernel tries to setup the VP assist page again, the hypervisor corrupts the memory region of the old VP assist page causing a panic in case the kexec kernel is using that memory elsewhere. This was originally fixed in commit dfe94d4086e4 ("x86/hyperv: Fix kexec panic/hang issues"). Get rid of hyperv_init_cpuhp entirely since we are no longer using a dynamic cpuhp state and use CPUHP_AP_HYPERV_ONLINE directly with cpuhp_remove_state().	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8633	The Form Maker by 10Web – Mobile-Friendly Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 1.15.27 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2024-46857	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix bridge mode operations when there are no VFs Currently, trying to set the bridge mode attribute when numvfs=0 leads to a crash: bridge link set dev eth2 hwmode vepa [168.967392] BUG: kernel NULL pointer dereference, address: 0000000000000030 [...] [168.969989] RIP: 0010:mlx5_add_flow_rules+0x1f/0x300 [mlx5_core] [...] [168.976037] Call Trace: [168.976188] <TASK> [168.978620] _mlx5_eswitch_set_vepa_locked+0x113/0x230 [mlx5_core] [168.979074] mlx5_eswitch_set_vepa+0x7f/0xa0 [mlx5_core] [168.979471] rtnl_bridge_setlink+0xe9/0x1f0 [168.979714] rtnetlink_rcv_msg+0x159/0x400 [168.980451] netlink_rcv_skb+0x54/0x100 [168.980675] netlink_unicast+0x241/0x360 [168.980918] netlink_sendmsg+0x1f6/0x430 [168.981162] ____sys_sendmsg+0x3bb/0x3f0 [168.982155] ___sys_sendmsg+0x88/0xd0 [168.985036] __sys_sendmsg+0x59/0xa0 [168.985477] do_syscall_64+0x79/0x150 [168.987273] entry_SYSCALL_64_after_hwframe+0x76/0x7e [168.987773] RIP: 0033:0x7f8f7950f917 (esw->fdb_table.legacy.vepa_fdb is null) The bridge mode is only relevant when there are multiple functions per port. Therefore, prevent setting and getting this setting when there are no VFs. Note that after this change, there are no settings to change on the PF interface using `bridge link` when there are no VFs, so the interface no longer appears in the `bridge link` output.	5.5	More Details
CVE-2024-46856	In the Linux kernel, the following vulnerability has been resolved: net: phy: dp83822: Fix NULL pointer dereference on DP83825 devices The probe() function is only used for DP83822 and DP83826 PHY, leaving the private data pointer uninitialized for the DP83825 models which causes a NULL pointer dereference in the recently introduced/changed functions dp8382x_config_init() and dp83822_set_wol(). Add the dp8382x_probe() function, so all PHY models will have a valid private data pointer to fix this issue and also prevent similar issues in the future.	5.5	More Details
CVE-2024-46855	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_socket: fix sk refcount leaks We must put 'sk' reference before returning.	5.5	More Details
CVE-2024-47290	Input validation vulnerability in the USB service module Impact: Successful exploitation of this vulnerability may affect availability.	5.5	More Details
CVE-2024-46082	Scriptcase v.9.10.023 and before is vulnerable to Cross Site Scripting (XSS) in nm_cor.php via the form and field parameters.	5.4	More Details
CVE-2024-42406	Mattermost versions 9.11.x <= 9.11.0, 9.10.x <= 9.10.1, 9.9.x <= 9.9.2 and 9.5.x <= 9.5.8 fail to properly authorize requests when viewing archived channels is disabled, which allows an attacker to retrieve post and file information about archived channels. Examples are flagged or unread posts as well as files.	5.4	More Details
CVE-2024-46081	Scriptcase v9.10.023 and before is vulnerable to Cross Site Scripting (XSS). An authenticated user can craft malicious payloads in the To-Do List. The assigned user will trigger a stored XSS, which is particularly dangerous because tasks are assigned to various users on the platform.	5.4	More Details
CVE-2024-7398	Concrete CMS versions 9 through 9.3.3 and versions below 8.5.19 are vulnerable to stored XSS in the calendar event addition feature because the calendar event name was not sanitized on output. Users or groups with permission to create event calendars can embed scripts, and users or groups with permission to modify event calendars can execute scripts. The Concrete CMS Security Team gave this vulnerability a CVSS v4 score of 1.8 with vector CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:A/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:A/VC:N/VI:N/VA:N/SC:L/SI:N/SA:N . Thank you, Yusuke Uchida for reporting.	5.4	More Details
CVE-2024-47048	Rocket.Chat 6.12.0, 6.11.2, 6.10.5, 6.9.6, 6.8.6, 6.7.8, and earlier allows stored XSS in the description and release notes of the marketplace and private apps.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47172	Computer Vision Annotation Tool (CVAT) is an interactive video and image annotation tool for computer vision. An attacker with a CVAT account may retrieve certain information about any project, task, job or membership resource on the CVAT instance. The information exposed in this way is the same as the information returned on a GET request to the resource. In addition, the attacker can also alter the default source and target storage associated with any project or task. Upgrade to CVAT 2.19.1 or any later version to fix the issue.	5.4	More Details
CVE-2024-8536	The Ultimate Blocks WordPress plugin before 3.2.2 does not validate and escape some of its block attributes before outputting them back in a page/post where the block is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2024-45986	A stored Cross-Site Scripting (XSS) vulnerability was identified in Projectworld Online Voting System 1.0 that occurs when an account is registered with a malicious javascript payload. The payload is stored and subsequently executed in the voter.php and profile.php pages whenever the account information is accessed.	5.4	More Details
CVE-2024-8239	The Starbox WordPress plugin before 3.5.3 does not properly render social media profiles URLs in certain contexts, like the malicious user's profile or pages where the starbox shortcode is used, which may be abused by users with at least the contributor role to conduct Stored XSS attacks.	5.4	More Details
CVE-2023-26688	Cross Site Scripting (XSS) vulnerability in CS-Cart MultiVendor 4.16.1 allows remote attackers to run arbitrary code via the product_data parameter of add/edit product in the administration interface.	5.4	More Details
CVE-2024-47530	Scout is a web-based visualizer for VCF-files. Open redirect vulnerability allows performing phishing attacks on users by redirecting them to malicious page. /login API endpoint is vulnerable to open redirect attack via next parameter due to absence of sanitization logic. Additionally, due to lack of scheme validation, HTTPS Downgrade Attack can be performed on the users. This vulnerability is fixed in 4.89.	5.4	More Details
CVE-2024-47315	Cross-Site Request Forgery (CSRF) vulnerability in GiveWP.This issue affects GiveWP: from n/a through 3.15.1.	5.4	More Details
CVE-2024-9141	Cross-Site Scripting (XSS) vulnerability in the Oct8ne system. This flaw could allow an attacker to embed harmful JavaScript code into the body of a chat message. This manipulation occurs when the chat content is intercepted and altered, leading to the execution of the JavaScript payload.	5.4	More Details
CVE-2024-9341	A flaw was found in Go. When FIPS mode is enabled on a system, container runtimes may incorrectly handle certain file paths due to improper validation in the containers/common Go library. This flaw allows an attacker to exploit symbolic links and trick the system into mounting sensitive host directories inside a container. This issue also allows attackers to access critical host files, bypassing the intended isolation between containers and the host system.	5.4	More Details
CVE-2023-51157	Cross Site Scripting vulnerability in ZKTeco WDMS v.5.1.3 Pro allows a remote attacker to execute arbitrary code and obtain sensitive information via a crafted script to the Emp Name parameter.	5.4	More Details
CVE-2024-46083	Scriptcase v9.10.023 and before is vulnerable to Cross Site Scripting (XSS). An authenticated user can craft malicious payloads using the messages feature, which allows the injection of malicious code into any user's account on the platform. It is important to note that regular users can trigger actions for administrator users.	5.4	More Details
CVE-2024-8608	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Oceanic Software ValeApp allows Stored XSS.This issue affects ValeApp: before v2.0.0.	5.4	More Details
CVE-2024-45920	A Stored Cross-Site Scripting (XSS) vulnerability in Solvait 24.4.2 allows remote attackers to inject malicious scripts into the application. This issue arises due to insufficient input validation and sanitization in "Intrest" feature.	5.4	More Details
CVE-2024-47178	basic-auth-connect is Connect's Basic Auth middleware in its own module. basic-auth-connect < 1.1.0 uses a timing-unsafe equality comparison that can leak timing information. This issue has been fixed in basic-auth-connect 1.1.0.	5.3	More Details
CVE-2024-8454	The swctrl service is used to detect and remotely manage PLANET Technology devices. Certain switch models have a Denial-of-Service vulnerability in the swctrl service, allowing unauthenticated remote attackers to send crafted packets that can crash the service.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52950	Missing encryption of sensitive data vulnerability in login component in Synology Active Backup for Business Agent before 2.7.0-3221 allows adjacent man-in-the-middle attackers to obtain user credential via unspecified vectors.	5.3	More Details
CVE-2024-9358	A vulnerability has been found in ThingsBoard up to 3.7.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the component HTTP RPC API. The manipulation leads to resource consumption. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. Upgrading to version 3.7.1 is able to address this issue. It is recommended to upgrade the affected component. The vendor was informed on 2024-07-24 about this vulnerability and announced the release of 3.7.1 for the second half of September 2024.	5.3	More Details
CVE-2024-7491	The HUSKY – Products Filter Professional for WooCommerce plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.3.6.1 via the woof_messenger_remove_subscr AJAX action due to missing validation on the 'key' user controlled key. This makes it possible for authenticated attackers, with subscriber-level access and above, to unsubscribe users from a product notification sign-ups, if they can successfully obtain or brute force the key value for users who signed up to receive notifications. This vulnerability requires the plugin's Products Messenger extension to be enabled.	5.3	More Details
CVE-2024-21531	All versions of the package git-shallow-clone are vulnerable to Command injection due to missing sanitization or mitigation flags in the process variable of the gitShallowClone function.	5.3	More Details
CVE-2024-7426	The Community by PeepSo – Social Network, Membership, Registration, User Profiles plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 6.4.6.0. This is due to the plugin displaying errors and allowing direct access to the sse.php file. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2024-45863	A null-dereference vulnerability involving parsing requests specifying invalid protocols can cause the application to crash or potentially result in other undesirable effects. This issue affects Facebook Thrift from v2024.09.09.00 until v2024.09.23.00.	5.3	More Details
CVE-2024-47176	CUPS is a standards-based, open-source printing system, and `cups-browsed` contains network printing functionality including, but not limited to, auto-discovering print services and shared printers. `cups-browsed` binds to `INADDR_ANY:631`, causing it to trust any packet from any source, and can cause the `Get-Printer-Attributes` IPP request to an attacker controlled URL. When combined with other vulnerabilities, such as CVE-2024-47076, CVE-2024-47175, and CVE-2024-47177, an attacker can execute arbitrary commands remotely on the target machine without authentication when a malicious printer is printed to.	5.3	More Details
CVE-2024-9025	The Sight – Professional Image Gallery and Portfolio plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'handler_post_title' function in all versions up to, and including, 1.1.2. This makes it possible for unauthenticated attackers to expose private, pending, trashed, and draft post titles. Successful exploitation requires the Elementor plugin to be installed and activated.	5.3	More Details
CVE-2024-43237	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in TaxoPress WordPress Tag Cloud Plugin – Tag Groups.This issue affects WordPress Tag Cloud Plugin – Tag Groups: from n/a through 2.0.3.	5.3	More Details
CVE-2024-47123	The goTenna Pro App uses AES CTR type encryption for short, encrypted messages without any additional integrity checking mechanisms. This leaves messages malleable to an attacker that can access the message. It is recommended to continue to use encryption in the app and update to the current release for more secure operations.	5.3	More Details
CVE-2024-47044	Multiple Home GateWay/Hikari Denwa routers provided by NIPPON TELEGRAPH AND TELEPHONE EAST CORPORATION are vulnerable to insufficient access restrictions for Device Setting pages. If this vulnerability is exploited, an attacker who identified WAN-side IPv6 address may access the product's Device Setting page via WAN-side. Note that, the same products are also provided by NIPPON TELEGRAPH AND TELEPHONE WEST CORPORATION, but the vulnerability only affects products subscribed and used in NIPPON TELEGRAPH AND TELEPHONE EAST CORPORATION areas.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8658	The myCred – Loyalty Points and Rewards plugin for WordPress and WooCommerce – Give Points, Ranks, Badges, Cashback, WooCommerce rewards, and WooCommerce credits for Gamification plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the mycred_update_database() function in all versions up to, and including, 2.7.3. This makes it possible for unauthenticated attackers to upgrade an out of date database.	5.3	More Details
CVE-2024-43108	The goTenna Pro ATAK Plugin uses AES CTR type encryption for short, encrypted messages without any additional integrity checking mechanisms. This leaves messages malleable to an attacker that can access the message. It is advised to continue to use encryption in the plugin and update to the current release for enhanced encryption protocols.	5.3	More Details
CVE-2024-6845	The Chatbot with ChatGPT WordPress plugin before 2.4.6 does not have proper authorization in one of its REST endpoint, allowing unauthenticated users to retrieve the encoded key and then decode it, thereby leaking the OpenAI API key	5.3	More Details
CVE-2024-40761	Inadequate Encryption Strength vulnerability in Apache Answer. This issue affects Apache Answer: through 1.3.5. Using the MD5 value of a user's email to access Gravatar is insecure and can lead to the leakage of user email. The official recommendation is to use SHA256 instead. Users are recommended to upgrade to version 1.4.0, which fixes the issue.	5.3	More Details
CVE-2024-9405	An incorrect limitation of a path to a restricted directory (path traversal) has been detected in Pluck CMS, affecting version 4.7.18. An unauthenticated attacker could extract sensitive information from the server via the absolute path of a file located in the same directory or subdirectory as the module, but not from recursive directories.	5.3	More Details
CVE-2024-38809	Applications that parse ETags from "If-Match" or "If-None-Match" request headers are vulnerable to DoS attack. Users of affected versions should upgrade to the corresponding fixed version. Users of older, unsupported versions could enforce a size limit on "If-Match" and "If-None-Match" headers, e.g. through a Filter.	5.3	More Details
CVE-2024-8678	The Revolut Gateway for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the /wc/v3/revolut REST API endpoint in all versions up to, and including, 4.17.3. This makes it possible for unauthenticated attackers to mark orders as completed.	5.3	More Details
CVE-2024-23586	HCL Nomad is susceptible to an insufficient session expiration vulnerability. Under certain circumstances, an unauthenticated attacker could obtain old session information.	5.3	More Details
CVE-2024-9189	The EU/UK VAT Manager for WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the alg_wc_eu_vat_exempt_vat_from_admin() function in all versions up to, and including, 2.12.12. This makes it possible for unauthenticated attackers to update the VAT status for any order.	5.3	More Details
CVE-2024-43990	Insertion of Sensitive Information into Log File vulnerability in StylemixThemes Masterstudy LMS Starter.This issue affects Masterstudy LMS Starter: from n/a through 1.1.8.	5.3	More Details
CVE-2024-9398	By checking the result of calls to `window.open` with specifically set protocol handlers, an attacker could determine if the application which implements that protocol handler is installed. This vulnerability affects Firefox < 131, Firefox ESR < 128.3, Thunderbird < 128.3, and Thunderbird < 131.	5.3	More Details
CVE-2024-9395	A specially crafted filename containing a large number of spaces could obscure the file's extension when displayed in the download dialog. *This bug only affects Firefox for Android. Other versions of Firefox are unaffected.* This vulnerability affects Firefox < 131.	5.3	More Details
CVE-2024-9321	A vulnerability was found in SourceCodester Online Railway Reservation System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/inquiries/view_details.php. The manipulation of the argument id leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2024-8430	The Spice Starter Sites plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the spice_starter_sites_importer_creater function in all versions up to, and including, 1.2.5. This makes it possible for unauthenticated attackers to import demo content.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45374	The goTenna Pro ATAK plugin uses a weak password for sharing encryption keys via the key broadcast method. If the broadcasted encryption key is captured over RF, and password is cracked via brute force attack, it is possible to decrypt it and use it to decrypt all future and past messages sent via encrypted broadcast with that particular key. This only applies when the key is broadcasted over RF. This is an optional feature, so it is advised to use local QR encryption key sharing for additional security on this and previous versions.	5.3	More Details
CVE-2024-47121	The goTenna Pro App uses a weak password for sharing encryption keys via the key broadcast method. If the broadcasted encryption key is captured over RF, and password is cracked via brute force attack, it is possible to decrypt it and use it to decrypt all future and past messages sent via encrypted broadcast with that particular key. This only applies when the key is broadcasted over RF. This is an optional feature, so it is recommended to use local QR encryption key sharing for additional security on this and previous versions.	5.3	More Details
CVE-2024-45772	Deserialization of Untrusted Data vulnerability in Apache Lucene Replicator. This issue affects Apache Lucene's replicator module: from 4.4.0 before 9.12.0. The deprecated org.apache.lucene.replicator.http package is affected. The org.apache.lucene.replicator.nrt package is not affected. Users are recommended to upgrade to version 9.12.0, which fixes the issue. The deserialization can only be triggered if users actively deploy an network-accessible implementation and a corresponding client using a HTTP library that uses the API (e.g., a custom servlet and HTTPClient). Java serialization filters (such as -Djdk.serialFilter='!*' on the commandline) can mitigate the issue on vulnerable versions without impacting functionality.	5.1	More Details
CVE-2024-45745	TopQuadrant TopBraid EDG before version 8.0.1 allows an authenticated attacker to upload an XML DTD file and execute JavaScript to read local files or access URLs (XXE). Fixed in 8.0.1 (bug fix: TBS-6721).	5.0	More Details
CVE-2023-52948	Missing encryption of sensitive data vulnerability in settings functionality in Synology Active Backup for Business Agent before 2.7.0-3221 allows local users to obtain user credential via unspecified vectors.	5.0	More Details
CVE-2024-0116	NVIDIA Triton Inference Server contains a vulnerability where a user may cause an out-of-bounds read issue by releasing a shared memory region while it is in use. A successful exploit of this vulnerability may lead to denial of service.	4.9	More Details
CVE-2024-8453	Certain switch models from PLANET Technology use an insecure hashing function to hash user passwords without being salted. Remote attackers with administrator privileges can read configuration files to obtain the hash values, and potentially crack them to retrieve the plaintext passwords.	4.9	More Details
CVE-2024-31835	Cross Site Scripting vulnerability in flatpress CMS Flatpress v1.3 allows a remote attacker to execute arbitrary code via a crafted payload to the file name parameter.	4.8	More Details
CVE-2024-3635	The Post Grid WordPress plugin before 7.5.0 does not sanitise and escape some of its Grid settings, which could allow high privilege users such as Editor and above to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2024-45073	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	4.8	More Details
CVE-2024-8283	The Slider by 10Web WordPress plugin before 1.2.59 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2024-46475	A reflected cross-site scripting (XSS) vulnerability on the homepage of Metronic Admin Dashboard Template v2.0 allows attackers to execute arbitrary code in the context of a user's browser via injecting a crafted payload.	4.8	More Details
CVE-2024-7878	The WP ULike WordPress plugin before 4.7.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2024-46333	An authenticated cross-site scripting (XSS) vulnerability in Piwigo v14.5.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Album Name parameter under the Add Album function.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8291	Concrete CMS versions 9.0.0 to 9.3.3 and below 8.5.19 are vulnerable to Stored XSS in Image Editor Background Color. A rogue admin could add malicious code to the Thumbnails/Add-Type. The Concrete CMS Security Team gave this a CVSS v4 score of 2.1 with vector CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N Thanks, Alexey Solovyev for reporting.	4.8	More Details
CVE-2024-47528	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. Stored Cross-Site Scripting (XSS) can be achieved by uploading a new Background for a Custom Map. Users with "admin" role can set background for a custom map, this allow the upload of SVG file that can contain XSS payload which will trigger on load. This led to Stored Cross-Site Scripting (XSS). The vulnerability is fixed in 24.9.0.	4.8	More Details
CVE-2024-8457	Certain switch models from PLANET Technology have a web application that does not properly validate specific parameters, allowing remote authenticated users with administrator privileges to inject arbitrary JavaScript, leading to Stored XSS attack.	4.8	More Details
CVE-2024-47182	Dozzle is a realtime log viewer for docker containers. Before version 8.5.3, the app uses sha-256 as the hash for passwords, which leaves users susceptible to rainbow table attacks. The app switches to bcrypt, a more appropriate hash for passwords, in version 8.5.3.	4.8	More Details
CVE-2024-45985	A Cross Site Scripting (XSS) vulnerability in update_contact.php of Blood Bank and Donation Management System v1.0 allows an attacker to inject malicious scripts via the name parameter of the update_contact.php	4.7	More Details
CVE-2024-45984	A Cross Site Scripting (XSS) vulnerability in add_donor.php of Blood Bank And Donation Management System 1.0 allows an attacker to inject malicious scripts that will be executed when the Donor List is viewed.	4.7	More Details
CVE-2024-20510	A vulnerability in the Central Web Authentication (CWA) feature of Cisco IOS XE Software for Wireless Controllers could allow an unauthenticated, adjacent attacker to bypass the pre-authentication access control list (ACL), which could allow access to network resources before user authentication. This vulnerability is due to a logic error when activating the pre-authentication ACL that is received from the authentication, authorization, and accounting (AAA) server. An attacker could exploit this vulnerability by connecting to a wireless network that is configured for CWA and sending traffic through an affected device that should be denied by the configured ACL before user authentication. A successful exploit could allow the attacker to bypass configured ACL protections on the affected device before the user authentication is completed, allowing the attacker to access trusted networks that the device might be protecting.	4.7	More Details
CVE-2024-46600	dingfanzu CMS 1.0 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/doAdminAction.php?act=delCate&id=31	4.7	More Details
CVE-2024-9278	A vulnerability, which was classified as critical, has been found in HuankeMao SCRM up to 0.0.3. Affected by this issue is the function upload_domain_verification_file of the file WxkConfig.php of the component Administrator Backend. The manipulation of the argument domain_verification_file leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-46851	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid race between dcn10_set_drr() and dc_state_destruct() dc_state_destruct() nulls the resource context of the DC state. The pipe context passed to dcn10_set_drr() is a member of this resource context. If dc_state_destruct() is called parallel to the IRQ processing (which calls dcn10_set_drr() at some point), we can end up using already nulled function callback fields of struct stream_resource. The logic in dcn10_set_drr() already tries to avoid this, by checking tg against NULL. But if the nulling happens exactly after the NULL check and before the next access, then we get a race. Avoid this by copying tg first to a local variable, and then use this variable for all the operations. This should work, as long as nobody frees the resource pool where the timing generators live. (cherry picked from commit a3cc326a43bdc48fbdf53443e1027a03e309b643)	4.7	More Details
CVE-2024-45967	Pagekit 1.0.18 is vulnerable to Cross Site Scripting (XSS) in index.php/admin/site/widget.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3866	The Ninja Forms Contact Form plugin for WordPress is vulnerable to Reflected Self-Based Cross-Site Scripting via the 'Referer' header in all versions up to, and including, 3.8.15 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. Successful exploitation of this vulnerability requires "maintenance mode" for a targeted form to be enabled. However, there is no setting available to the attacker or even an administrator-level user to enable this mode. The mode is only enabled during a required update, which is a very short window of time. Additionally, because of the self-based nature of this vulnerability, attackers would have to rely on additional techniques to execute a supplied payload in the context of targeted user.	4.7	More Details
CVE-2024-47293	Out-of-bounds write vulnerability in the HAL-WIFI module Impact: Successful exploitation of this vulnerability may affect availability.	4.7	More Details
CVE-2024-46850	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid race between dcn35_set_drr() and dc_state_destruct() dc_state_destruct() nulls the resource context of the DC state. The pipe context passed to dcn35_set_drr() is a member of this resource context. If dc_state_destruct() is called parallel to the IRQ processing (which calls dcn35_set_drr() at some point), we can end up using already nulled function callback fields of struct stream_resource. The logic in dcn35_set_drr() already tries to avoid this, by checking tg against NULL. But if the nulling happens exactly after the NULL check and before the next access, then we get a race. Avoid this by copying tg first to a local variable, and then use this variable for all the operations. This should work, as long as nobody frees the resource pool where the timing generators live. (cherry picked from commit 0607a50c004798a96e62c089a4c34c220179dcb5)	4.7	More Details
CVE-2024-9280	A vulnerability has been found in kalvinGit kvf-admin up to f12a94dc1ebb7d1c51ee978a85e4c7ed75c620ff and classified as critical. This vulnerability affects the function fileUpload of the file FileUploadKit.java. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Continious delivery with rolling releases is used by this product. Therefore, no version details of affected nor updated releases are available.	4.7	More Details
CVE-2024-9407	A vulnerability exists in the bind-propagation option of the Dockerfile RUN --mount instruction. The system does not properly validate the input passed to this option, allowing users to pass arbitrary parameters to the mount instruction. This issue can be exploited to mount sensitive directories from the host into a container during the build process and, in some cases, modify the contents of those mounted files. Even if SELinux is used, this vulnerability can bypass its protection by allowing the source directory to be relabeled to give the container access to host files.	4.7	More Details
CVE-2024-47082	Strawberry GraphQL is a library for creating GraphQL APIs. Prior to version 0.243.0, multipart file upload support as defined in the GraphQL multipart request specification was enabled by default in all Strawberry HTTP view integrations. This made all Strawberry HTTP view integrations vulnerable to cross-site request forgery (CSRF) attacks if users did not explicitly enable CSRF preventing security mechanism for their servers. Additionally, the Django HTTP view integration, in particular, had an exemption for Django's built-in CSRF protection (i.e., the `CsrfViewMiddleware` middleware) by default. In affect, all Strawberry integrations were vulnerable to CSRF attacks by default. Version `v0.243.0` is the first `strawberry-graphql` including a patch.	4.6	More Details
CVE-2024-47531	Scout is a web-based visualizer for VCF-files. Due to the lack of sanitization in the filename, it is possible bypass intended file extension and make users download malicious files with any extension. With malicious content injected inside the file data and users unknowingly downloading it and opening may lead to the compromise of users' devices or data. This vulnerability is fixed in 4.89.	4.6	More Details
CVE-2024-23960	Alpine Halo9 Improper Verification of Cryptographic Signature Vulnerability. This vulnerability allows physically present attackers to bypass signature validation mechanism on affected installations of Alpine Halo9 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the firmware metadata signature validation mechanism. The issue results from the lack of proper verification of a cryptographic signature. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-23102	4.6	More Details
CVE-2024-47294	Access permission verification vulnerability in the input method framework module Impact: Successful exploitation of this vulnerability may affect availability.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45042	Ory Kratos is an identity, user management and authentication system for cloud services. Prior to version 1.3.0, given a number of preconditions, the `highest_available` setting will incorrectly assume that the identity's highest available AAL is `aal1` even though it really is `aal2`. This means that the `highest_available` configuration will act as if the user has only one factor set up, for that particular user. This means that they can call the settings and whoami endpoint without a `aal2` session, even though that should be disallowed. An attacker would need to steal or guess a valid login OTP of a user who has only OTP for login enabled and who has an incorrect `available_aal` value stored, to exploit this vulnerability. All other aspects of the session (e.g. the session's aal) are not impacted by this issue. On the Ory Network, only 0.00066% of registered users were affected by this issue, and most of those users appeared to be test users. Their respective AAL values have since been updated and they are no longer vulnerable to this attack. Version 1.3.0 is not affected by this issue. As a workaround, those who require MFA should disable the passwordless code login method. If that is not possible, check the sessions `aal` to identify if the user has `aal1` or `aal2`.	4.4	More Details
CVE-2022-49041	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in backup task management functionality in Synology Drive Client before 3.4.0-15721 allows local users with administrator privileges to crash the client via unspecified vectors.	4.4	More Details
CVE-2022-49040	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in connection management functionality in Synology Drive Client before 3.4.0-15721 allows local users with administrator privileges to crash the client via unspecified vectors.	4.4	More Details
CVE-2024-7259	A flaw was found in oVirt. A user with administrator privileges, including users with the ReadOnlyAdmin permission, may be able to use browser developer tools to view Provider passwords in cleartext.	4.4	More Details
CVE-2024-8189	The WP MultiTasking – WP Utilities plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wpmt_menu_name' parameter in all versions up to, and including, 0.1.17 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2023-46175	IBM Cloud Pak for Multicloud Management 2.3 through 2.3 FP8 stores user credentials in a log file plain clear text which can be read by a privileged user.	4.4	More Details
CVE-2024-47330	Missing Authorization vulnerability in Supsystic Slider by Supsystic, Supsystic Social Share Buttons by Supsystic.This issue affects Slider by Supsystic: from n/a through 1.8.6; Social Share Buttons by Supsystic: from n/a through 2.2.9.	4.3	More Details
CVE-2024-8552	The Download Monitor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the enable_shop() function in all versions up to, and including, 5.0.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to enable shop functionality.	4.3	More Details
CVE-2024-8675	The Soumettre.fr plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the soumettre_disconnect_gateway function in all versions up to, and including, 2.1.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to disconnect the gateway and delete the API key.	4.3	More Details
CVE-2024-47305	Cross-Site Request Forgery (CSRF) vulnerability in Dnesscarkey Use Any Font allows Cross Site Request Forgery.This issue affects Use Any Font: from n/a through 6.3.08.	4.3	More Details
CVE-2024-8437	The WP Easy Gallery – WordPress Gallery Plugin plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on several functions hooked via AJAX like wpeg_settings and wpeg_add_gallery in all versions up to, and including, 4.8.5. This makes it possible for authenticated attackers, with subscriber-level access and above, to modify galleries.	4.3	More Details
CVE-2024-8771	The Email Subscribers by Icegram Express – Email Marketing, Newsletters, Automation for WordPress & WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'preview_email_template_design' function in all versions up to, and including, 5.7.34. This makes it possible for authenticated attackers, with Subscriber-level access and above, to extract sensitive data including the content of private, password protected, pending, and draft posts and pages.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7892	The adstxt Plugin WordPress plugin through 1.0.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	4.3	More Details
CVE-2024-47128	The goTenna Pro App encryption key name is always sent unencrypted when the key is shared over RF through a broadcast message. It is advised to share the encryption key via local QR for higher security operations.	4.3	More Details
CVE-2024-9282	A vulnerability was found in bg5sbk MiniCMS 1.11. It has been classified as problematic. Affected is an unknown function of the file page-edit.php. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions confusing version and file name information. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-9281	A vulnerability was found in bg5sbk MiniCMS up to 1.11 and classified as problematic. This issue affects some unknown processing of the file post-edit.php. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions confusing version and file name information. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-8910	The HT Mega – Absolute Addons For Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.6.5 via the render function in includes/widgets/htmega_accordion.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-2024-31899	IBM Cognos Command Center 10.2.4.1 and 10.2.5 could disclose highly sensitive user information to an authenticated user with physical access to the device.	4.3	More Details
CVE-2024-8516	The Themesflat Addons For Elementor plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 2.2.1 via the render() function. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract limited post information from draft and future scheduled posts.	4.3	More Details
CVE-2024-9155	Mattermost versions 9.10.x <= 9.10.1, 9.9.x <= 9.9.2, 9.5.x <= 9.5.8 fail to limit access to channels files that have not been linked to a post which allows an attacker to view them in channels that they are a member of.	4.3	More Details
CVE-2024-20434	A vulnerability in Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on the control plane of an affected device. This vulnerability is due to improper handling of frames with VLAN tag information. An attacker could exploit this vulnerability by sending crafted frames to an affected device. A successful exploit could allow the attacker to render the control plane of the affected device unresponsive. The device would not be accessible through the console or CLI, and it would not respond to ping requests, SNMP requests, or requests from other control plane protocols. Traffic that is traversing the device through the data plane is not affected. A reload of the device is required to restore control plane services.	4.3	More Details
CVE-2024-9298	A vulnerability was found in SourceCodester Online Railway Reservation System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /?page=tickets of the component Ticket Handler. The manipulation of the argument id leads to improper access controls. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2024-47171	Agnai is an artificial-intelligence-agnostic multi-user, mult-bot roleplaying chat system. A vulnerability in versions prior to 1.0.330 permits attackers to upload image files at attacker-chosen location on the server. This issue can lead to image file uploads to unauthorized or unintended directories, including overwriting of existing images which may be used for defacement. This does not affect `agnai.chat`, installations using S3-compatible storage, or self-hosting that is not publicly exposed. Version 1.0.330 fixes this vulnerability.	4.3	More Details
CVE-2024-9300	A vulnerability classified as problematic was found in SourceCodester Online Railway Reservation System 1.0. This vulnerability affects unknown code of the file contact_us.php of the component Message Us Form. The manipulation of the argument fullname/email/message leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47170	Agnai is an artificial-intelligence-agnostic multi-user, mult-bot roleplaying chat system. A vulnerability in versions prior to 1.0.330 permits attackers to read arbitrary JSON files at attacker-chosen locations on the server. This issue can lead to unauthorized access to sensitive information and exposure of confidential configuration files. This only affects installations with `JSON_STORAGE` enabled which is intended to local/self-hosting only. Version 1.0.330 fixes this issue.	4.3	More Details
CVE-2024-8801	The Happy Addons for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.12.2 via the Content Switcher widget. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive data including private, draft, and pending Elementor templates.	4.3	More Details
CVE-2024-8476	The Easy PayPal Events plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.1. This is due to missing or incorrect nonce validation on the wpeevent_plugin_buttons() function. This makes it possible for unauthenticated attackers to delete arbitrary posts 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-2024-47129	The goTenna Pro App does not inject extra characters into broadcasted frames to obfuscate the length of messages. This makes it possible to tell the length of the payload regardless of the encryption used.	4.3	More Details
CVE-2024-8483	The MAS Static Content plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.0.8 via the static_content() function. This makes it possible for authenticated attackers, with contributor-level access and above, to extract potentially sensitive information from private static content pages.	4.3	More Details
CVE-2024-8434	The Easy Mega Menu Plugin for WordPress – ThemeHunk plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on several functions hooked via AJAX in all versions up to, and including, 1.0.9. This makes it possible for authenticated attackers, with subscriber-level access and above, to perform actions like updating plugin settings.	4.3	More Details
CVE-2024-43814	The goTenna Pro ATAK Plugin's default settings are to share Automatic Position, Location, and Information (PLI) updates every 60 seconds once the plugin is active and goTenna is connected. Users that are unaware of their settings and have not activated encryption before a mission may accidentally broadcast their location unencrypted. It is advised to verify PLI settings are the desired rate and activate encryption prior to mission. Update to the latest Plugin to disable this default setting.	4.3	More Details
CVE-2024-46632	Assimp v5.4.3 is vulnerable to Buffer Overflow via the MD5Importer::LoadMD5MeshFile function.	4.3	More Details
CVE-2024-41715	The goTenna Pro ATAK Plugin does not inject extra characters into broadcasted frames to obfuscate the length of messages. This makes it possible to tell the length of the payload regardless of the encryption used.	4.3	More Details
CVE-2024-41931	The goTenna Pro ATAK Plugin encryption key name is always sent unencrypted when the key is sent over RF through a broadcast message. It is advised to share the encryption key via local QR for higher security operations.	4.3	More Details
CVE-2024-47124	The goTenna Pro App does not encrypt callsigns in messages. It is recommended to not use sensitive information in callsigns when using this and previous versions of the app and update your app to the current app version which uses AES-256 encryption for callsigns in encrypted operation.	4.3	More Details
CVE-2024-7386	The Premium Packages – Sell Digital Products Securely plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.9.1. This is due to missing nonce validation on the addRefund() function. This makes it possible for unauthenticated attackers to perform actions such as initiating refunds via a forged request granted they can trick a site administrator or shop manager into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-43694	In the goTenna Pro ATAK Plugin application, the encryption keys are stored along with a static IV on the device. This allows for complete decryption of keys stored on the device. This allows an attacker to decrypt all encrypted broadcast communications based on broadcast keys stored on the device.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35495	An Information Disclosure vulnerability in the Telemetry component in TP-Link Kasa KP125M V1.0.0 and Tapo P125M 1.0.0 Build 220930 Rel.143947 allows attackers to observe device state via observing network traffic.	4.3	More Details
CVE-2024-45838	The goTenna Pro ATAK Plugin does not encrypt callsigns in messages. It is advised to not use sensitive information in callsigns when using this and previous versions of the plugin. Update to current plugin version which uses AES-256 encryption for callsigns in encrypted operation	4.3	More Details
CVE-2024-47122	In the goTenna Pro App, the encryption keys are stored along with a static IV on the End User Device (EUD). This allows for complete decryption of keys stored on the EUD if physically compromised. This allows an attacker to decrypt all encrypted broadcast communications based on encryption keys stored on the EUD. This requires access to and control of the EUD, so it is recommended to use strong access control measures and layered encryption on the EUD for more secure operation.	4.3	More Details
CVE-2024-47337	Missing Authorization vulnerability in Stuart Wilson Joy Of Text Lite.This issue affects Joy Of Text Lite: from n/a through 2.3.1.	4.3	More Details
CVE-2024-0133	NVIDIA Container Toolkit 1.16.1 or earlier contains a vulnerability in the default mode of operation allowing a specially crafted container image to create empty files on the host file system. This does not impact use cases where CDI is used. A successful exploit of this vulnerability may lead to data tampering.	4.1	More Details
CVE-2024-45989	Monica AI Assistant desktop application v2.3.0 is vulnerable to Exposure of Sensitive Information to an Unauthorized Actor. A prompt injection allows an attacker to modify chatbot answer with an unloaded image that exfiltrates the user's sensitive chat data of the current session to a malicious third-party or attacker-controlled server.	4.0	More Details
CVE-2023-52947	Missing authentication for critical function vulnerability in logout functionality in Synology Active Backup for Business Agent before 2.6.3-3101 allows local users to logout the client via unspecified vectors. The backup functionality will continue to operate and will not be affected by the logout.	4.0	More Details
CVE-2024-45599	Cursor is an artificial intelligence code editor. Prior to version 0.41.0, if a user on macOS has granted Cursor access to the camera or microphone, any program that is run on the machine is able to access the camera or the microphone without explicitly being granted access, through a DyLib Injection using DYLD_INSERT_LIBRARIES environment variable. The usage of `com.apple.security.cs.allow-dyld-environment-variables` and `com.apple.security.cs.disable-library-validation` allows an external dynamic library to be injected into the application using DYLD_INSERT_LIBRARIES environment variable. Moreover, the entitlement `com.apple.security.device.camera` allows the application to use the host camera and `com.apple.security.device.audio-input` allows the application to use the microphone. This means that untrusted code that is executed on the user's machine can access the camera or the microphone, if the user has already given permission for Cursor to do so. In version 0.41.0, the entitlements have been split by process: the main process gets the camera and microphone entitlements, but not the DyLib entitlements, whereas the extension host process gets the DyLib entitlements but not the camera or microphone entitlements. As a workaround, do not explicitly give Cursor the permission to access the camera or microphone if untrusted users can run arbitrary commands on the affected machine.	3.8	More Details
CVE-2023-5359	The W3 Total Cache plugin for WordPress is vulnerable to Sensitive Information Exposure in versions up to, and including, 2.7.5 via Google OAuth API secrets stored in plaintext in the publicly visible plugin source. This can allow unauthenticated attackers to impersonate W3 Total Cache and gain access to user account information in successful conditions. This would not impact the WordPress users site in any way.	3.7	More Details
CVE-2024-30132	HCL Nomad server on Domino did not configure certain HTTP Security headers by default which could allow an attacker to obtain sensitive information via unspecified vectors.	3.7	More Details
CVE-2022-43845	IBM Aspera Console 3.4.0 through 3.4.4 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie.	3.7	More Details
CVE-2024-9411	A vulnerability classified as problematic has been found in OFCMS 1.1.2. This affects the function add of the file /admin/system/dict/add.json?sqlid=system.dict.save. The manipulation of the argument dict_value 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.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9276	A vulnerability classified as problematic has been found in TMsoft MyAuth Gateway 3. Affected is an unknown function of the file /index.php. The manipulation of the argument console/nocache/cmd 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. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-9277	A vulnerability classified as problematic was found in Langflow up to 1.0.18. Affected by this vulnerability is an unknown functionality of the file \src\backend\base\langflow\interface\utils.py of the component HTTP POST Request Handler. The manipulation of the argument remaining_text leads to inefficient regular expression complexity. 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.	3.5	More Details
CVE-2024-47526	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Self Cross-Site Scripting (Self-XSS) vulnerability in the "Alert Templates" feature allows users to inject arbitrary JavaScript into the alert template's name. This script executes immediately upon submission but does not persist after a page refresh.	3.5	More Details
CVE-2024-9291	A vulnerability classified as problematic has been found in kalvinGit kvf-admin up to f12a94dc1ebb7d1c51ee978a85e4c7ed75c620ff. Affected is an unknown function of the file /ueditor/upload?configPath=ueditor/config.json&action=uploadfile of the component XML File Handler. The manipulation of the argument upfile 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. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The GitHub repository of the project did not receive an update for more than two years.	3.5	More Details
CVE-2024-9323	A vulnerability was found in SourceCodester Inventory Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /app/action/add_staff.php. The manipulation 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-2024-9320	A vulnerability has been found in SourceCodester Online Timesheet App 1.0 and classified as problematic. This vulnerability affects unknown code of the file /endpoint/add-timesheet.php of the component Add Timesheet Form. The manipulation of the argument day/task leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-9299	A vulnerability classified as problematic has been found in SourceCodester Online Railway Reservation System 1.0. This affects an unknown part of the file /?page=reserve. The manipulation of the argument First Name/Middle Name/Last 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.	3.5	More Details
CVE-2024-28811	An issue was discovered in Infinera hiT 7300 5.60.50. A web application allows a remote privileged attacker to execute applications contained in a specific OS directory via HTTP invocations.	3.3	More Details
CVE-2023-25189	BTS is affected by information disclosure vulnerability where mobile network operator personnel connected over BTS Web Element Manager, regardless of the access privileges, having a possibility to read BTS service operation details performed by Nokia Care service personnel via SSH.	3.3	More Details
CVE-2024-9283	A vulnerability classified as problematic has been found in RelaxedJS ReLaXed up to 0.2.2. Affected is an unknown function of the component Pug to PDF Converter. The manipulation leads to cross site scripting. An attack has to be approached locally. The exploit has been disclosed to the public and may be used.	3.3	More Details
CVE-2024-47145	Mattermost versions 9.5.x <= 9.5.8 fail to properly authorize access to archived channels when viewing archived channels is disabled, which allows an attacker to view posts and files of archived channels via file links.	3.1	More Details
CVE-2024-47003	Mattermost versions 9.11.x <= 9.11.0 and 9.5.x <= 9.5.8 fail to validate that the message of the permalink post is a string, which allows an attacker to send a non-string value as the message of a permalink post and crash the frontend.	3.1	More Details
CVE-2024-45843	Mattermost versions 9.5.x <= 9.5.8 fail to include the metadata endpoints of Oracle Cloud and Alibaba in the SSRF denylist, which allows an attacker to possibly cause an SSRF if Mattermost was deployed in Oracle Cloud or Alibaba.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4099	An issue has been discovered in GitLab EE affecting all versions starting from 16.0 prior to 17.2.8, from 17.3 prior to 17.3.4, and from 17.4 prior to 17.4.1. An AI feature was found to read unsanitized content in a way that could have allowed an attacker to hide prompt injection.	3.1	More Details
CVE-2024-45744	TopQuadrant TopBraid EDG stores external credentials insecurely. An authenticated attacker with file system access can read edg-setup.properites and obtain the secret to decrypt external passwords stored in edg-vault.properties. An authenticated attacker could gain file system access using a separate vulnerability such as CVE-2024-45745. At least version 7.1.3 is affected. Version 7.3 adds HashiCorp Vault integration that does not store external passwords locally.	3.0	More Details
CVE-2024-8350	The Uncanny Groups for LearnDash plugin for WordPress is vulnerable to user group add due to a missing capability check on the /wp-json/ulgm_management/v1/add_user/ REST API endpoint in all versions up to, and including, 6.1.0.1. This makes it possible for authenticated attackers, with group leader-level access and above, to add users to their group which ultimately allows them to leverage CVE-2024-8349 and gain admin access to the site.	2.7	More Details
CVE-2024-28808	An issue was discovered in Infinera hiT 7300 5.60.50. Hidden functionality in the web interface allows a remote authenticated attacker to access reserved information by accessing undocumented web applications.	2.7	More Details
CVE-2024-8974	Information disclosure in Gitlab EE/CE affecting all versions from 15.6 prior to 17.2.8, 17.3 prior to 17.3.4, and 17.4 prior to 17.4.1 in specific conditions it was possible to disclose to an unauthorised user the path of a private project."	2.6	More Details
CVE-2024-9203	A vulnerability, which was classified as problematic, has been found in Enpass Password Manager up to 6.9.5 on Windows. This issue affects some unknown processing. The manipulation leads to cleartext storage of sensitive information in memory. An attack has to be approached locally. The complexity of an attack is rather high. The exploitation is known to be difficult. Upgrading to version 6.10.1 is able to address this issue. It is recommended to upgrade the affected component.	2.5	More Details
CVE-2024-9279	A vulnerability, which was classified as problematic, was found in funnyzpc Mee-Admin up to 1.6. This affects an unknown part of the file /mee/index of the component User Center. The manipulation of the argument User Nickname 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 vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2024-46503	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2024-42496	Smart-tab Android app installed April 2023 or earlier contains an issue with plaintext storage of a password. If this vulnerability is exploited, an attacker with physical access to the device may retrieve the credential information and spoof the device to access the related external service.	N/A	More Details
CVE-2024-9063	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-2024-47536	Citizen is a MediaWiki skin that makes extensions part of the cohesive experience. A user with the editmyprivateinfo right or who can otherwise change their name can XSS themselves by setting their "real name" to an XSS payload. This vulnerability is fixed in 2.31.0.	N/A	More Details
CVE-2024-45792	Mantis Bug Tracker (MantisBT) is an open source issue tracker. Using a crafted POST request, an unprivileged, registered user is able to retrieve information about other users' personal system profiles. This vulnerability is fixed in 2.26.4.	N/A	More Details
CVE-2024-9145	Wiz Code Visual Studio Code extension in versions 1.0.0 up to 1.5.3 and Wiz (legacy) Visual Studio Code extension in versions 0.13.0 up to 0.17.8 are vulnerable to local command injection if the user opens a maliciously crafted Dockerfile located in a path that has been marked as a "trusted folder" within Visual Studio Code, and initiates a manual scan of the file.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6051	Cross Application Scripting vulnerability in Vercom S.A. Redlink SDK in specific situations allows local code injection and to manipulate the view of a vulnerable application.This issue affects Redlink SDK versions through 1.13.	N/A	More Details
CVE-2024-9194	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Linux and Microsoft Windows Octopus Server on Windows, Linux allows SQL Injection.This issue affects Octopus Server: from 2024.1.0 before 2024.1.13038, from 2024.2.0 before 2024.2.9482, from 2024.3.0 before 2024.3.12766.	N/A	More Details
CVE-2024-6394	A Local File Inclusion vulnerability exists in parisneo/lollms-webui versions below v9.8. The vulnerability is due to unverified path concatenation in the `serve_js` function in `app.py`, which allows attackers to perform path traversal attacks. This can lead to unauthorized access to arbitrary files on the server, potentially exposing sensitive information such as private SSH keys, configuration files, and source code.	N/A	More Details
CVE-2024-9166	The device enables an unauthorized attacker to execute system commands with elevated privileges. This exploit is facilitated through the use of the 'getcommand' query within the application, allowing the attacker to gain root access.	N/A	More Details
CVE-2024-47560	RevoWorks Cloud Client 3.0.91 and earlier contains an incorrect authorization vulnerability. If this vulnerability is exploited, unintended processes may be executed in the sandbox environment. Even if malware is executed in the sandbox environment, it does not compromise the client's local environment. However, information in the sandbox environment may be disclosed to outside or behaviors of the sandbox environment may be violated by tampering registry.	N/A	More Details
CVE-2024-47609	Tonic is a native gRPC client & server implementation with async/await support. When using tonic::transport::Server there is a remote DoS attack that can cause the server to exit cleanly on accepting a TCP/TLS stream. This can be triggered by causing the accept call to error out with errors that were not covered correctly causing the accept loop to exit. Upgrading to tonic 0.12.3 and above contains the fix.	N/A	More Details
CVE-2024-3373	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in RSM Design Website Template allows SQL Injection.This issue affects Website Template: before 1.2.	N/A	More Details
CVE-2024-6436	An input validation vulnerability exists in the Rockwell Automation Sequence Manager™ which could allow a malicious user to send malformed packets to the server and cause a denial-of-service condition. If exploited, the device would become unresponsive, and a manual restart will be required for recovery. Additionally, if exploited, there could be a loss of view for the downstream equipment sequences in the controller. Users would not be able to view the status or command the equipment sequences, however the equipment sequence would continue to execute uninterrupted.	N/A	More Details
CVE-2024-8118	In Grafana, the wrong permission is applied to the alert rule write API endpoint, allowing users with permission to write external alert instances to also write alert rules.	N/A	More Details
CVE-2024-39319	aimeos/ai-controller-frontend is the Aimeos frontend controller package for e-commerce projects. Prior to versions 2024.4.2, 2023.10.9, 2022.10.8, 2021.10.8, and 2020.10.15, an insecure direct object reference allows an attacker to disable subscriptions and reviews of another customer. Versions 2024.4.2, 2023.10.9, 2022.10.8, 2021.10.8, and 2020.10.15 fix this issue.	N/A	More Details
CVE-2024-9160	In versions of the PEADM Forge Module prior to 3.24.0 a security misconfiguration was discovered.	N/A	More Details
CVE-2024-7400	The vulnerability potentially allowed an attacker to misuse ESET’s file operations during the removal of a detected file on the Windows operating system to delete files without having proper permissions to do so.	N/A	More Details
CVE-2024-9273	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9268	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-47534	go-tuf is a Go implementation of The Update Framework (TUF). The go-tuf client inconsistently traces the delegations. For example, if targets delegate to "A", and to "B", and "B" delegates to "C", then the client should trace the delegations in the order "A" then "B" then "C" but it may incorrectly trace the delegations "B"->"C"->"A". This vulnerability is fixed in 2.0.1.	N/A	More Details
CVE-2024-6654	Products for macOS enables a user logged on to the system to perform a denial-of-service attack, which could be misused to disable the protection of the ESET security product and cause general system slow-down.	N/A	More Details
CVE-2024-9202	In Eclipse Dataspace Components versions 0.1.3 to 0.9.0, the Connector component filters which datasets (= data offers) another party can see in a requested catalog, to ensure that only authorized parties are able to view restricted offers. However, there is the possibility to request a single dataset, which should be subject to the same filtering process, but currently is missing the correct filtering. This enables parties to potentially see datasets they should not have access to, thereby exposing sensitive information. Exploiting this vulnerability requires knowing the ID of a restricted dataset, but some IDs may be guessed by trying out many IDs in an automated way. Affected code: DatasetResolverImpl, L76-79 https://github.com/eclipse-edc/Connector/blob/v0.9.0/core/control-plane/control-plane-catalog/src/main/java/org/eclipse/edc/connector/controlplane/catalog/DatasetResolverImpl.java	N/A	More Details
CVE-2024-9171	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-22170	Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in Western Digital My Cloud ddns-start on Linux allows Overflow Buffers.This issue affects My Cloud: before 5.29.102.	N/A	More Details
CVE-2024-4657	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Talent Software BAP Automation allows Stored XSS.This issue affects BAP Automation: before 30840.	N/A	More Details
CVE-2024-6983	mudler/localai version 2.17.1 is vulnerable to remote code execution. The vulnerability arises because the localai backend receives inputs not only from the configuration file but also from other inputs, allowing an attacker to upload a binary file and execute malicious code. This can lead to the attacker gaining full control over the system.	N/A	More Details
CVE-2024-46839	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-8067	In versions of Helix Core prior to 2024.1 Patch 2 (2024.1/2655224) a Windows ANSI API Unicode "best fit" argument injection was identified.	N/A	More Details
CVE-2024-8421	Rejected reason: Red Hat Product Security has come to the conclusion that this CVE is not needed.	N/A	More Details