SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 27 March 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-2024-2227	This vulnerability allows access to arbitrary files in the application server file system due to a path traversal vulnerability in JavaServer Faces (JSF) 2.2.20 documented in CVE-2020-6950. The remediation for this vulnerability contained in this security fix provides additional changes to the remediation announced in May 2021 tracked by ETN IIQSAW-3585 and January 2024 tracked by IIQFW-336. This vulnerability in IdentityIQ is assigned CVE-2024-2227.	10.0	More Details
CVE-2023-23656	Unrestricted Upload of File with Dangerous Type vulnerability in MainWP MainWP File Uploader Extension.This issue affects MainWP File Uploader Extension: from n/a through 4.1.	10.0	More Details
CVE-2024-27956	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ValvePress Automatic allows SQL Injection.This issue affects Automatic: from n/a through 3.92.0.	9.9	More Details
CVE-2024-1800	In Progress® Telerik® Report Server versions prior to 2024 Q1 (10.0.24.130), a remote code execution attack is possible through an insecure deserialization vulnerability.	9.9	More Details
CVE-2023-48777	Unrestricted Upload of File with Dangerous Type vulnerability in Elementor.Com Elementor Website Builder.This issue affects Elementor Website Builder: from 3.3.0 through 3.18.1.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36407	Insertion of Sensitive Information into Log File vulnerability in Hitachi Virtual Storage Platform, Hitachi Virtual Storage Platform VP9500, Hitachi Virtual Storage Platform G1000, G1500, Hitachi Virtual Storage Platform F1500, Hitachi Virtual Storage Platform 5100, 5500, 5100H, 5500H, Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H, Hitachi Unified Storage VM, Hitachi Virtual Storage Platform G100, G200, G400, G600, G800, Hitachi Virtual Storage Platform F400, F600, F800, Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900, Hitachi Virtual Storage Platform F350, F370, F700, F900, Hitachi Virtual Storage Platform E390, E590, E790, E990, E1090, E390H, E590H, E790H, E1090H allows local users to gain sensitive information.This issue affects Hitachi Virtual Storage Platform: before DKCMAIN Ver. 70-06-74-00/00, SVP Ver. 70-06-58/00; Hitachi Virtual Storage Platform VP9500: before DKCMAIN Ver. 70-06-74-00/00, SVP Ver. 70-06-58/00; Hitachi Virtual Storage Platform G1000, G1500: before DKCMAIN Ver. 80-06-92-00/00, SVP Ver. 80-06-87/00; Hitachi Virtual Storage Platform F1500: before DKCMAIN Ver. 80-06-92-00/00, SVP Ver. 80-06-87/00; Hitachi Virtual Storage Platform 5100, 5500,5100H, 5500H: before DKCMAIN Ver. 90-08-81-00/00, SVP Ver. 90-08-81/00, before DKCMAIN Ver. 90-08-62-00/00, SVP Ver. 90-08-62/00, before DKCMAIN Ver. 90-08-43-00/00, SVP Ver. 90-08-43/00; Hitachi Virtual Storage Platform 5200, 5600,5200H, 5600H: before DKCMAIN Ver. 90-08-81-00/00, SVP Ver. 90-08-81/00, before DKCMAIN Ver. 90-08-62-00/00, SVP Ver. 90-08-62/00, before DKCMAIN Ver. 90-08-43-00/00, SVP Ver. 90-08-43/00; Hitachi Unified Storage VM: before DKCMAIN Ver. 73-03-75-X0/00, SVP Ver. 73-03-74/00, before DKCMAIN Ver. 73(75)-03-75-X0/00, SVP Ver. 73(75)-03-74/00; Hitachi Virtual Storage Platform G100, G200, G400, G600, G800: before DKCMAIN Ver. 83-06-19-X0/00, SVP Ver. 83-06-20-X0/00, before DKCMAIN Ver. 83-05-47-X0/00, SVP Ver. 83-05-51-X0/00; Hitachi Virtual Storage Platform F400, F600, F800: before DKCMAIN Ver. 83-06-19-X0/00, SVP Ver. 83-06-20-X0/00, before DKCMAIN Ver. 83-05-47-X0/00, SVP Ver. 83-05-51-X0/00; Hitachi Virtual Storage Platform G130, G150, G350, G370, G700, G900: before DKCMAIN Ver. 88-08-09-XX/00, SVP Ver. 88-08-11-X0/02; Hitachi Virtual Storage Platform F350, F370, F700, F900: before DKCMAIN Ver. 88-08-09-XX/00, SVP Ver. 88-08-11-X0/02; Hitachi Virtual Storage Platform E390, E590, E790, E990, E1090, E390H, E590H, E790H, E1090H: before DKCMAIN Ver. 93-06-81-X0/00, SVP Ver. 93-06-81-X0/00, before DKCMAIN Ver. 93-06-62-X0/00, SVP Ver. 93-06-62-X0/00, before DKCMAIN Ver. 93-06-43-X0/00, SVP Ver. 93-06-43-X0/00.	9.9	More Details
CVE-2024-29943	An attacker was able to perform an out-of-bounds read or write on a JavaScript object by fooling range-based bounds check elimination. This vulnerability affects Firefox < 124.0.1.	9.8	More Details
CVE-2024-2724	SQL injection vulnerability in the CIGESv2 system, through /ajaxServiciosAtencion.php, in the 'idServicio' parameter. The exploitation of this vulnerability could allow a remote user to retrieve all data stored in the database by sending a specially crafted SQL query.	9.8	More Details
CVE-2024-2723	SQL injection vulnerability in the CIGESv2 system, through /ajaxSubServicios.php, in the 'idServicio' parameter. The exploitation of this vulnerability could allow a remote user to retrieve all data stored in the database by sending a specially crafted SQL query.	9.8	More Details
CVE-2024-2722	SQL injection vulnerability in the CIGESv2 system, through /ajaxConfigTotem.php, in the 'id' parameter. The exploitation of this vulnerability could allow a remote user to retrieve all data stored in the database by sending a specially crafted SQL query.	9.8	More Details
CVE-2024-22080	An issue was discovered in Elspec G5 digital fault recorder versions 1.1.4.15 and before. Unauthenticated memory corruption can occur during XML body parsing.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29275	SQL injection vulnerability in SeaCMS version 12.9, allows remote unauthenticated attackers to execute arbitrary code and obtain sensitive information via the id parameter in class.php.	9.8	More Details
CVE-2024-28441	File Upload vulnerability in magicflue v.7.0 and before allows a remote attacker to execute arbitrary code via a crafted request to the messageid parameter of the mail/mailupdate.jsp endpoint.	9.8	More Details
CVE-2024-22081	An issue was discovered in Elspec G5 digital fault recorder versions 1.1.4.15 and before. Unauthenticated memory corruption can occur in the HTTP header parsing mechanism.	9.8	More Details
CVE-2024-29876	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/reports/activitylogreport, 'sortby' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	9.8	More Details
CVE-2024-29875	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/default/reports/exportactiveuserrpt, 'sort_name' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	9.8	More Details
CVE-2024-28861	Symfony 1 is a community-driven fork of the 1.x branch of Symfony, a PHP framework for web projects. Starting in version 1.1.0 and prior to version 1.5.19, Symfony 1 has a gadget chain due to dangerous deserialization in `sfNamespacedParameterHolder` class that would enable an attacker to get remote code execution if a developer deserializes user input in their project. Version 1.5.19 contains a patch for the issue.	9.8	More Details
CVE-2024-28393	SQL injection vulnerability in scalapay v.1.2.41 and before allows a remote attacker to escalate privileges via the ScalapayReturnModuleFrontController::postProcess() method.	9.8	More Details
CVE-2024-28386	An issue in Home-Made.io fastmagsync v.1.7.51 and before allows a remote attacker to execute arbitrary code via the getPhpBin() component.	9.8	More Details
CVE-2024-29873	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/reports/businessunits/format/html, 'bunitname' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	9.8	More Details
CVE-2024-2865	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mergen Software Quality Management System allows SQL Injection.This issue affects Quality Management System: through 25032024.	9.8	More Details
CVE-2024-29650	An issue in @thi.ng/paths v.5.1.62 and before allows a remote attacker to execute arbitrary code via the mutIn and mutInManyUnsafe components.	9.8	More Details
CVE-2024-29666	Insecure Permissions vulnerability in Vehicle Monitoring platform system CMSV6 v.7.31.0.2 through v.7.32.0.3 allows a remote attacker to escalate privileges via the default password component.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28421	SQL Injection vulnerability in Razor 0.8.0 allows a remote attacker to escalate privileges via the ChannelModel::updateapk method of the channelmodle.php	9.8	More Details
CVE-2024-29303	The delete admin users function of SourceCodester PHP Task Management System 1.0 is vulnerable to SQL Injection	9.8	More Details
CVE-2024-28048	OS command injection vulnerability exists in ffBull ver.4.11, which may allow a remote unauthenticated attacker to execute an arbitrary OS command with the privilege of the running web server. Note that the developer was unreachable, therefore, users should consider stop using ffBull ver.4.11.	9.8	More Details
CVE-2024-29684	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component /src/dede/makehtml_homepage.php allowing a remote attacker to execute arbitrary code.	9.8	More Details
CVE-2024-29401	xzs-mysql 3.8 is vulnerable to Insufficient Session Expiration, which allows attackers to use the session of a deleted admin to do anything.	9.8	More Details
CVE-2024-2921	Improper access control in PAM vault permissions in Devolutions Server 2024.1.10.0 and earlier allows an authenticated user with access to the PAM to access unauthorized PAM entries via a specific set of permissions.	9.8	More Details
CVE-2024-25421	An issue in Ignite Realtime Openfire v.4.9.0 and before allows a remote attacker to escalate privileges via the ROOM_CACHE component.	9.8	More Details
CVE-2024-29874	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/default/reports/activeuserrptpdf, 'sort_name' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	9.8	More Details
CVE-2024-29243	Shenzhen Libituo Technology Co., Ltd LBT-T300-mini v1.2.9 was discovered to contain a buffer overflow via the vpn_client_ip parameter at /apply.cgi.	9.8	More Details
CVE-2024-29872	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/empscreening/add, 'agencyids' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	9.8	More Details
CVE-2023-48902	An issue was discovered in tramyardg autoexpress version 1.3.0, allows unauthenticated remote attackers to escalate privileges, update car data, delete vehicles, and upload car images via authentication bypass in uploadCarImages.php.	9.8	More Details
CVE-2024-1711	The Create by Mediavine plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 1.9.4 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.	9.8	More Details
CVE-2024-1811	A potential vulnerability has been identified in OpenText ArcSight Platform. The vulnerability could be remotely exploited.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28392	SQL injection vulnerability in pscartabandonmentpro v.2.0.11 and before allows a remote attacker to escalate privileges via the pscartabandonmentproFrontCAPUnsubscribeJobModuleFrontController::setEmailVisualized() method.	9.8	More Details
CVE-2024-28395	SQL injection vulnerability in Best-Kit bestkit_popup v.1.7.2 and before allows a remote attacker to escalate privileges via the bestkit_popup.php component.	9.8	More Details
CVE-2023-38825	SQL injection vulnerability in Vanderbilt REDCap before v.13.8.0 allows a remote attacker to obtain sensitive information via the password reset mechanism in MyCapMobileApp/update.php.	9.8	More Details
CVE-2024-29871	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/index/getdepartments/sentrifugo/index.php/index/updatecontactnumber, 'id' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	9.8	More Details
CVE-2024-25239	SQL Injection vulnerability in Sourcecodester Employee Management System v1.0 allows attackers to run arbitrary SQL commands via crafted POST request to /emloyee_akpoly/Account/login.php.	9.8	More Details
CVE-2024-27922	TOMP Bare Server implements the TompHTTP bare server. A vulnerability in versions prior to 2.0.2 relates to insecure handling of HTTP requests by the @tomphttp/bare-server-node package. This flaw potentially exposes the users of the package to manipulation of their web traffic. The impact may vary depending on the specific usage of the package but it can potentially affect any system where this package is in use. The problem has been patched in version 2.0.2. As of time of publication, no specific workaround strategies have been disclosed.	9.8	More Details
CVE-2024-2054	The Artica-Proxy administrative web application will deserialize arbitrary PHP objects supplied by unauthenticated users and subsequently enable code execution as the "www-data" user.	9.8	More Details
CVE-2023-48901	A SQL injection vulnerability in tramyardg Autoexpress version 1.3.0, allows remote unauthenticated attackers to execute arbitrary SQL commands via the parameter "id" within the getPhotosByCarId function call in details.php.	9.8	More Details
CVE-2024-1202	Authentication Bypass by Primary Weakness vulnerability in XPodas Octopod allows Authentication Bypass.This issue affects Octopod: before v1. NOTE: The vendor was contacted and it was learned that the product is not supported.	9.8	More Details
CVE-2024-29858	In MISP before 2.4.187, __uploadLogo in app/Controller/OrganisationsController.php does not properly check for a valid logo upload.	9.8	More Details
CVE-2024-1147	Weak access control in OpenText PVCS Version Manager allows potential bypassing of authentication and download of files.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29870	SQL injection vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/index/getdepartments/format/html, 'business_id' parameter./sentrifugo/index.php/index/getdepartments/format/html, 'business_id' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted query to the server and extract all the data from it.	9.8	More Details
CVE-2024-29732	A SQL Injection has been found on SCAN_VISIO eDocument Suite Web Viewer of Abast. This vulnerability allows an unauthenticated user to retrieve, update and delete all the information of database. This vulnerability was found on login page via "user" parameter.	9.8	More Details
CVE-2024-27438	Download of Code Without Integrity Check vulnerability in Apache Doris. The jdbc driver files used for JDBC catalog is not checked and may resulting in remote command execution. Once the attacker is authorized to create a JDBC catalog, he/she can use arbitrary driver jar file with unchecked code snippet. This code snippet will be run when catalog is initializing without any check. This issue affects Apache Doris: from 1.2.0 through 2.0.4. Users are recommended to upgrade to version 2.0.5 or 2.1.x, which fixes the issue.	9.8	More Details
CVE-2024-1148	Weak access control in OpenText PVCS Version Manager allows potential bypassing of authentication and uploading of files.	9.8	More Details
CVE-2024-28545	Tenda AC18 V15.03.05.05 contains a command injection vulnerablility in the deviceName parameter of formsetUsbUnload function.	9.8	More Details
CVE-2024-2161	Use of Hard-coded Credentials in Kiloview NDI allows un-authenticated users to bypass authenticationThis issue affects Kiloview NDI N3, N3-s, N4, N20, N30, N40 and was fixed in Firmware version 2.02.0227 .	9.8	More Details
CVE-2024-29864	Distrobox before 1.7.0.1 allows attackers to execute arbitrary code via command injection into exported executables.	9.8	More Details
CVE-2024-29859	In MISP before 2.4.187, add_misp_export in app/Controller/EventsController.php does not properly check for a valid file upload.	9.8	More Details
CVE-2024-28231	eprosima Fast DDS is a C++ implementation of the Data Distribution Service standard of the Object Management Group. Prior to versions 2.14.0, 2.13.4, 2.12.3, 2.10.4, and 2.6.8, manipulated DATA Submessage can cause a heap overflow error in the Fast-DDS process, causing the process to be terminated remotely. Additionally, the payload_size in the DATA Submessage packet is declared as uint32_t. When a negative number, such as -1, is input into this variable, it results in an Integer Overflow (for example, -1 gets converted to 0xFFFFFFFF). This eventually leads to a heap-buffer-overflow, causing the program to terminate. Versions 2.14.0, 2.13.4, 2.12.3, 2.10.4, and 2.6.8 contain a fix for this issue.	9.6	More Details
CVE-2023-28787	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ExpressTech Quiz And Survey Master.This issue affects Quiz And Survey Master: from n/a through 8.1.4.	9.3	More Details
CVE-2024-29866	Datalust Seq before 2023.4.11151 and 2024 before 2024.1.11146 has Incorrect Access Control because a Project Owner or Organization Owner can escalate to System privileges.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-47873	Unrestricted Upload of File with Dangerous Type vulnerability in WEN Solutions WP Child Theme Generator.This issue affects WP Child Theme Generator: from n/a through 1.0.9.	9.1	More Details
CVE-2023-47846	Unrestricted Upload of File with Dangerous Type vulnerability in Terry Lin WP Githuber MD.This issue affects WP Githuber MD: from n/a through 1.16.2.	9.1	More Details
CVE-2023-47842	Unrestricted Upload of File with Dangerous Type vulnerability in Zachary Segal CataBlog.This issue affects CataBlog: from n/a through 1.7.0.	9.1	More Details
CVE-2023-29386	Unrestricted Upload of File with Dangerous Type vulnerability in Julien Crego Manager for Icomoon.This issue affects Manager for Icomoon: from n/a through 2.0.	9.1	More Details
CVE-2024-2862	This vulnerability allows remote attackers to reset the password of anonymous users without authorization on the affected LG LED Assistant.	9.1	More Details
CVE-2024-25294	An SSRF issue in REBUILD v.3.5 allows a remote attacker to obtain sensitive information and execute arbitrary code via the FileDownloader.java, proxyDownload,URL parameters.	9.1	More Details
CVE-2024-29037	datahub-helm provides the Kubernetes Helm charts for deploying Datahub and its dependencies on a Kubernetes cluster. Starting in version 0.1.143 and prior to version 0.2.182, due to configuration issues in the helm chart, if there was a successful initial deployment during a limited window of time, personal access tokens were possibly created with a default secret key. Since the secret key is a static, publicly available value, someone could inspect the algorithm used to generate personal access tokens and generate their own for an instance. Deploying with Metadata Service Authentication enabled would have been difficult during window of releases. If someone circumvented the helm settings and manually set Metadata Service Authentication to be enabled using environment variables directly, this would skip over the autogeneration logic for the Kubernetes Secrets and DataHub GMS would default to the signing key specified statically in the application.yml. Most deployments probably did not attempt to circumvent the helm settings to enable Metadata Service Authentication during this time, so impact is most likely limited. Any deployments with Metadata Service Authentication enabled should ensure that their secret values are properly randomized. Version 0.2.182 contains a patch for this issue. As a workaround, one may reset the token signing key to be a random value, which will invalidate active personal access tokens.	9.1	More Details
CVE-2024-2443	A command injection vulnerability was identified in GitHub Enterprise Server that allowed an attacker with an editor role in the Management Console to gain admin SSH access to the appliance when configuring GeoJSON settings. Exploitation of this vulnerability required access to the GitHub Enterprise Server instance and access to the Management Console with the editor role. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.13 and was fixed in versions 3.8.17, 3.9.12, 3.10.9, 3.11.7, and 3.12.1. This vulnerability was reported via the GitHub Bug Bounty program.	9.1	More Details
CVE-2024-2873	A vulnerability was found in wolfSSH's server-side state machine before versions 1.4.17. A malicious client could create channels without first performing user authentication, resulting in unauthorized access.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26942	An issue discovered in Axigen Mail Server 10.3.x before 10.3.1.27 and 10.3.2.x before 10.3.3.1 allows unauthenticated attackers to submit a setAdminPassword operation request, subsequently setting a new arbitrary password for the admin account.	9.1	More Details
CVE-2024-30231	Unrestricted Upload of File with Dangerous Type vulnerability in WebToffee Product Import Export for WooCommerce.This issue affects Product Import Export for WooCommerce: from n/a through 2.4.1.	9.1	More Details
CVE-2024-28179	Jupyter Server Proxy allows users to run arbitrary external processes alongside their Jupyter notebook servers and provides authenticated web access. Prior to versions 3.2.3 and 4.1.1, Jupyter Server Proxy did not check user authentication appropriately when proxying websockets, allowing unauthenticated access to anyone who had network access to the Jupyter server endpoint. This vulnerability can allow unauthenticated remote access to any websocket endpoint set up to be accessible via Jupyter Server Proxy. In many cases, this leads to remote unauthenticated arbitrary code execution, due to how affected instances use websockets. The websocket endpoints exposed by `jupyter_server` itself is not affected. Projects that do not rely on websockets are also not affected. Versions 3.2.3 and 4.1.1 contain a fix for this issue.	9.0	More Details
CVE-2024-29185	FreeScout is a self-hosted help desk and shared mailbox. Versions prior to 1.8.128 are vulnerable to OS Command Injection in the /public/tools.php source file. The value of the php_path parameter is being executed as an OS command by the shell_exec function, without validating it. This allows an adversary to execute malicious OS commands on the server. A practical demonstration of the successful command injection attack extracted the /etc/passwd file of the server. This represented the complete compromise of the server hosting the FreeScout application. This attack requires an attacker to know the `App_Key` of the application. This limitation makes the Attack Complexity to be High. If an attacker gets hold of the `App_Key`, the attacker can compromise the Complete server on which the application is deployed. Version 1.8.128 contains a patch for this issue.	9.0	More Details
CVE-2023-38388	Unrestricted Upload of File with Dangerous Type vulnerability in Artbees JupiterX Core.This issue affects JupiterX Core: from n/a through 3.3.5.	9.0	More Details
CVE-2024-29385	DIR-845L router <= v1.01KRb03 has an Unauthenticated remote code execution vulnerability in the cgibin binary via soapcgi_main function.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-27964	Unrestricted Upload of File with Dangerous Type vulnerability in Gesundheit Bewegt GmbH Zippy.This issue affects Zippy: from n/a through 1.6.9.	8.8	More Details
CVE-2024-2704	A vulnerability classified as critical was found in Tenda AC10U 15.03.06.49. Affected by this vulnerability is the function formSetFirewallCfg of the file /goform/SetFirewallCfg. The manipulation of the argument firewallEn leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257455. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50894	In Janitza GridVis through 9.0.66, use of hard-coded credentials in the de.janitza.pasw.feature.impl.activators.PasswordEncryption password encryption function allows remote authenticated administrative users to discover cleartext database credentials contained in error report information.	8.8	More Details
CVE-2024-1205	The Management App for WooCommerce – Order notifications, Order management, Lead management, Uptime Monitoring plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the nouvello_upload_csv_file function in all versions up to, and including, 1.2.0. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2024-2625	Object lifecycle issue in V8 in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-28916	Xbox Gaming Services Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-28824	Least privilege violation and reliance on untrusted inputs in the mk_informix Checkmk agent plugin before Checkmk 2.3.0b4 (beta), 2.2.0p24, 2.1.0p41 and 2.0.0 (EOL) allows local users to escalate privileges.	8.8	More Details
CVE-2024-28559	SQL injection vulnerability in Niushop B2B2C v.5.3.3 and before allows an attacker to escalate privileges via the setPrice() function of the Goodsbatchset.php component.	8.8	More Details
CVE-2024-28118	Grav is an open-source, flat-file content management system. Prior to version 1.7.45, due to the unrestricted access to twig extension class from Grav context, an attacker can redefine config variable. As a result, attacker can bypass a previous SSTI mitigation. Twig processing of static pages can be enabled in the front matter by any administrative user allowed to create or edit pages. As the Twig processor runs unsandboxed, this behavior can be used to gain arbitrary code execution and elevate privileges on the instance. Version 1.7.45 contains a fix for this issue.	8.8	More Details
CVE-2024-2627	Use after free in Canvas in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-27299	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. A SQL injection vulnerability has been discovered in the the "Add News" functionality due to improper escaping of the email address. This allows any authenticated user with the rights to add/edit FAQ news to exploit this vulnerability to exfiltrate data, take over accounts and in some cases, even achieve RCE. The vulnerable field lies in the `authorEmail` field which uses PHP's `FILTER_VALIDATE_EMAIL` filter. This filter is insufficient in protecting against SQL injection attacks and should still be properly escaped. However, in this version of phpMyFAQ (3.2.5), this field is not escaped properly can be used together with other fields to fully exploit the SQL injection vulnerability. This vulnerability is fixed in 3.2.6.	8.8	More Details
CVE-2023-49982	Broken access control in the component /admin/management/users of School Fees Management System v1.0 allows attackers to escalate privileges and perform Administrative actions, including adding and deleting user accounts.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27921	Grav is an open-source, flat-file content management system. A file upload path traversal vulnerability has been identified in the application prior to version 1.7.45, enabling attackers to replace or create files with extensions like .json, .zip, .css, .gif, etc. This critical security flaw poses severe risks, that can allow attackers to inject arbitrary code on the server, undermine integrity of backup files by overwriting existing files or creating new ones, and exfiltrate sensitive data using CSS exfiltration techniques. Upgrading to patched version 1.7.45 can mitigate the issue.	8.8	More Details
CVE-2024-2896	A vulnerability was found in Tenda AC7 15.03.06.44. It has been rated as critical. This issue affects the function formWifiWpsStart of the file /goform/WifiWpsStart. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257939. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2895	A vulnerability was found in Tenda AC7 15.03.06.44. It has been declared as critical. This vulnerability affects the function formWifiWpsOOB of the file /goform/WifiWpsOOB. The manipulation of the argument index leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257938 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2891	A vulnerability, which was classified as critical, was found in Tenda AC7 15.03.06.44. Affected is the function formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257934 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2883	Use after free in ANGLE in Google Chrome prior to 123.0.6312.86 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	8.8	More Details
CVE-2024-2885	Use after free in Dawn in Google Chrome prior to 123.0.6312.86 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-28029	Privileges are not fully verified server-side, which can be abused by a user with limited privileges to bypass authorization and access privileged functionality.	8.8	More Details
CVE-2024-25002	Command Injection in the diagnostics interface of the Bosch Network Synchronizer allows unauthorized users full access to the device.	8.8	More Details
CVE-2024-2902	A vulnerability was found in Tenda AC7 15.03.06.44 and classified as critical. This issue affects the function fromSetWifiGusetBasic of the file /goform/WifiGuestSet. The manipulation of the argument shareSpeed leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257945 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28093	The TELNET service of AdTran NetVanta 3120 18.01.01.00.E devices is enabled by default, and has default credentials for a root-level account.	8.8	More Details
CVE-2024-2815	A vulnerability classified as critical has been found in Tenda AC15 15.03.20_multi. Affected is the function R7WebsSecurityHandler of the file /goform/execCommand of the component Cookie Handler. The manipulation of the argument password leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257670 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-25937	SQL injection vulnerability exists in the script DIAE_tagHandler.ashx.	8.8	More Details
CVE-2024-2806	A vulnerability classified as critical has been found in Tenda AC15 15.03.05.18/15.03.20_multi. This affects the function addWifiMacFilter of the file /goform/addWifiMacFilter. The manipulation of the argument deviceId/deviceMac leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257661 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2893	A vulnerability was found in Tenda AC7 15.03.06.44 and classified as critical. Affected by this issue is the function formSetDeviceName of the file /goform/SetOnlineDevName. The manipulation of the argument devName 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 identifier of this vulnerability is VDB-257936. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2807	A vulnerability classified as critical was found in Tenda AC15 15.03.05.18/15.03.20_multi. This vulnerability affects the function formExpandDlnaFile of the file /goform/expandDlnaFile. The manipulation of the argument filePath leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257662 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2808	A vulnerability, which was classified as critical, has been found in Tenda AC15 15.03.05.18/15.03.20_multi. This issue affects the function formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257663. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2898	A vulnerability classified as critical was found in Tenda AC7 15.03.06.44. Affected by this vulnerability is the function fromSetRouteStatic of the file /goform/SetStaticRouteCfg. The manipulation of the argument list leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257941 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2899	A vulnerability, which was classified as critical, has been found in Tenda AC7 15.03.06.44. Affected by this issue is the function fromSetWirelessRepeat of the file /goform/WifiExtraSet. The manipulation of the argument wpapsk_crypto leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257942 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2809	A vulnerability, which was classified as critical, was found in Tenda AC15 15.03.05.18/15.03.20_multi. Affected is the function formSetFirewallCfg of the file /goform/SetFirewallCfg. The manipulation of the argument firewallEn leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257664. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2764	A vulnerability, which was classified as critical, was found in Tenda AC10U 15.03.06.48. This affects the function formSetPPTPServer of the file /goform/SetPptpServerCfg. The manipulation of the argument endIP leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257601 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2810	A vulnerability has been found in Tenda AC15 15.03.05.18/15.03.20_multi and classified as critical. Affected by this vulnerability is the function formWifiWpsOOB of the file /goform/WifiWpsOOB. The manipulation of the argument index leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257665 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2703	A vulnerability classified as critical has been found in Tenda AC10U 15.03.06.49. Affected is the function formSetDeviceName of the file /goform/SetOnlineDevName. The manipulation of the argument mac leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257454 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2900	A vulnerability, which was classified as critical, was found in Tenda AC7 15.03.06.44. This affects the function saveParentControlInfo of the file /goform/saveParentControlInfo. The manipulation of the argument deviceId/time/urls leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257943. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2901	A vulnerability has been found in Tenda AC7 15.03.06.44 and classified as critical. This vulnerability affects the function setSchedWifi of the file /goform/openSchedWifi. The manipulation of the argument schedEndTime leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257944. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2811	A vulnerability was found in Tenda AC15 15.03.20_multi and classified as critical. Affected by this issue is the function formWifiWpsStart of the file /goform/WifiWpsStart. The manipulation of the argument index leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257666 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2813	A vulnerability was found in Tenda AC15 15.03.20_multi. It has been declared as critical. This vulnerability affects the function form_fast_setting_wifi_set of the file /goform/fast_setting_wifi_set. The manipulation of the argument ssid leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257668. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2763	A vulnerability, which was classified as critical, has been found in Tenda AC10U 15.03.06.48. Affected by this issue is the function formSetCfm of the file goform/setcfm. The manipulation of the argument funcpara1 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 identifier of this vulnerability is VDB-257600. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2814	A vulnerability was found in Tenda AC15 15.03.20_multi. It has been rated as critical. This issue affects the function fromDhcpListClient of the file /goform/DhcpListClient. The manipulation of the argument page leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257669 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-28117	Grav is an open-source, flat-file content management system. Prior to version 1.7.45, Grav validates accessible functions through the Utils::isDangerousFunction function, but does not impose restrictions on twig functions like twig_array_map, allowing attackers to bypass the validation and execute arbitrary commands. Twig processing of static pages can be enabled in the front matter by any administrative user allowed to create or edit pages. As the Twig processor runs unsandboxed, this behavior can be used to gain arbitrary code execution and elevate privileges on the instance. Upgrading to patched version 1.7.45 can mitigate this issue.	8.8	More Details
CVE-2024-2894	A vulnerability was found in Tenda AC7 15.03.06.44. It has been classified as critical. This affects the function formSetQosBand of the file /goform/SetNetControlList. The manipulation of the argument list leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257937 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-1962	The CM Download Manager WordPress plugin before 2.9.1 does not have CSRF checks in some places, which could allow attackers to make logged in admins edit downloads via a CSRF attack	8.8	More Details
CVE-2023-50702	Sikka SSCWindowsService 5 2023-09-14 executes a program as LocalSystem but allows full control by low-privileged users (and low-privileged users have write access to %PROGRAMDATA%\SSCService). Consequently, low-privileged users can execute arbitrary code as LocalSystem.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29366	A command injection vulnerability exists in the cgibin binary in DIR-845L router firmware <= v1.01KRb03.	8.8	More Details
CVE-2024-23975	SQL injection vulnerability exists in GetDIAE_slogListParameters.	8.8	More Details
CVE-2024-0856	The Appointment Booking Calendar WordPress plugin before 1.3.83 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks such as adding a booking to the calendar without paying.	8.8	More Details
CVE-2024-23494	SQL injection vulnerability exists in GetDIAE_unListParameters.	8.8	More Details
CVE-2024-28891	SQL injection vulnerability exists in the script Handler_CFG.ashx.	8.8	More Details
CVE-2024-2850	A vulnerability was found in Tenda AC15 15.03.05.18 and classified as critical. Affected by this issue is the function saveParentControlInfo of the file /goform/saveParentControlInfo. The manipulation of the argument urls leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257774 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-1538	The File Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 7.2.4. This is due to missing or incorrect nonce validation on the wp_file_manager page that includes files through the 'lang' parameter. This makes it possible for unauthenticated attackers to include local JavaScript files that can be leveraged to achieve RCE via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This issue was partially patched in version 7.2.4, and fully patched in 7.2.5.	8.8	More Details
CVE-2024-24725	Gibbon through 26.0.00 allows remote authenticated users to conduct PHP deserialization attacks via columnOrder in a POST request to the modules/System%20Admin/import_run.php&type=externalAssessment&step=4 URI.	8.8	More Details
CVE-2024-2708	A vulnerability was found in Tenda AC10U 15.03.06.49 and classified as critical. This issue affects the function formexeCommand of the file /goform/execCommand. The manipulation of the argument cmdinput leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257459. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-28107	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. A SQL injection vulnerability has been discovered in the `insertentry` & `saveentry` when modifying records due to improper escaping of the email address. This allows any authenticated user with the rights to add/edit FAQ news to exploit this vulnerability to exfiltrate data, take over accounts and in some cases, even achieve RCE. This vulnerability is fixed in 3.2.6.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2709	A vulnerability was found in Tenda AC10U 15.03.06.49. It has been classified as critical. Affected is the function fromSetRouteStatic of the file /goform/SetStaticRouteCfg. The manipulation of the argument list leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257460. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-1799	The GamiPress – The #1 gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to SQL Injection via the 'achievement_types' attribute of the gamipress_earnings shortcode in all versions up to, and including, 6.8.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with 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-2024-23755	ClickUp Desktop before 3.3.77 on macOS and Windows allows code injection because of specific Electron Fuses. There is inadequate protection against code injection through settings such as RunAsNode.	8.8	More Details
CVE-2024-2710	A vulnerability was found in Tenda AC10U 15.03.06.49. It has been declared as critical. Affected by this vulnerability is the function setSchedWifi of the file /goform/openSchedWifi. The manipulation of the argument schedStartTime leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257461 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-27923	Grav is a content management system (CMS). Prior to version 1.7.43, users who may write a page may use the `frontmatter` feature due to insufficient permission validation and inadequate file name validation. This may lead to remote code execution. Version 1.7.43 fixes this issue.	8.8	More Details
CVE-2024-27936	Deno is a JavaScript, TypeScript, and WebAssembly runtime with secure defaults. Starting in version 1.32.1 and prior to version 1.41.0 of the deno library, maliciously crafted permission request can show the spoofed permission prompt by inserting a broken ANSI escape sequence into the request contents. Deno is stripping any ANSI escape sequences from the permission prompt, but permissions given to the program are based on the contents that contain the ANSI escape sequences. Any Deno program can spoof the content of the interactive permission prompt by inserting a broken ANSI code, which allows a malicious Deno program to display the wrong file path or program name to the user. Version 1.41.0 of the deno library contains a patch for the issue.	8.8	More Details
CVE-2024-2025	The "BuddyPress WooCommerce My Account Integration. Create WooCommerce Member Pages" plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.4.20 via deserialization of untrusted input in the get_simple_request function. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject a PHP Object. 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 Number	Description	Base Score	Reference
CVE-2024-2711	A vulnerability was found in Tenda AC10U 15.03.06.48. It has been rated as critical. Affected by this issue is the function addWifiMacFilter of the file /goform/addWifiMacFilter. The manipulation of the argument deviceMac leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257462 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-22078	An issue was discovered in Elspec G5 digital fault recorder versions 1.1.4.15 and before. Privilege escalation can occur via world writable files. The network configuration script has weak filesystem permissions. This results in write access for all authenticated users and the possibility to escalate from user privileges to administrative privileges.	8.8	More Details
CVE-2024-28040	SQL injection vulnerability exists in GetDIAE_astListParameters.	8.8	More Details
CVE-2024-2162	An OS Command Injection vulnerability in Kiloview NDI allows a low-privileged user to execute arbitrary code remotely on the device with high privileges. This issue affects Kiloview NDI N3, N3-s, N4, N20, N30, N40 and was fixed in Firmware version 2.02.0227 .	8.8	More Details
CVE-2024-28119	Grav is an open-source, flat-file content management system. Prior to version 1.7.45, due to the unrestricted access to twig extension class from grav context, an attacker can redefine the escape function and execute arbitrary commands. Twig processing of static pages can be enabled in the front matter by any administrative user allowed to create or edit pages. As the Twig processor runs unsandboxed, this behavior can be used to gain arbitrary code execution and elevate privileges on the instance. Version 1.7.45 contains a patch for this issue.	8.8	More Details
CVE-2024-2915	Improper access control in PAM JIT elevation in Devolutions Server 2024.1.6 and earlier allows an attacker with access to the PAM JIT elevation feature to elevate themselves to unauthorized groups via a specially crafted request.	8.8	More Details
CVE-2024-29515	File Upload vulnerability in lepton v.7.1.0 allows a remote authenticated attackers to execute arbitrary code via uploading a crafted PHP file to the save.php and config.php component.	8.8	More Details
CVE-2024-29071	HGW BL1500HM Ver 002.001.013 and earlier contains a use of week credentials issue. A network-adjacent unauthenticated attacker may change the system settings.	8.8	More Details
CVE-2024-2892	A vulnerability has been found in Tenda AC7 15.03.06.44 and classified as critical. Affected by this vulnerability is the function formSetCfm of the file /goform/setcfm. The manipulation of the argument funcpara1 leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257935. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2805	A vulnerability was found in Tenda AC15 15.03.05.18/15.03.20_multi. It has been rated as critical. Affected by this issue is the function formSetSpeedWan of the file /goform/SetSpeedWan. The manipulation of the argument speed_dir 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 identifier of this vulnerability is VDB-257660. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2903	A vulnerability was found in Tenda AC7 15.03.06.44. It has been classified as critical. Affected is the function GetParentControlInfo of the file /goform/GetParentControlInfo. The manipulation of the argument mac leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257946 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-28041	HGW BL1500HM Ver 002.001.013 and earlier allows a network-adjacent unauthenticated attacker to execute an arbitrary command.	8.8	More Details
CVE-2024-2909	A vulnerability classified as critical was found in Ruijie RG-EG350 up to 20240318. Affected by this vulnerability is the function setAction of the file /itbox_pi/networksafe.php?a=set of the component HTTP POST Request Handler. The manipulation of the argument bandwidth leads to os command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257977 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2705	A vulnerability, which was classified as critical, has been found in Tenda AC10U 1.0/15.03.06.49. Affected by this issue is the function formSetQosBand of the file /goform/SetNetControlList. The manipulation of the argument list leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257456. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-28116	Grav is an open-source, flat-file content management system. Grav CMS prior to version 1.7.45 is vulnerable to a Server-Side Template Injection (SSTI), which allows any authenticated user (editor permissions are sufficient) to execute arbitrary code on the remote server bypassing the existing security sandbox. Version 1.7.45 contains a patch for this issue.	8.8	More Details
CVE-2024-2856	A vulnerability, which was classified as critical, has been found in Tenda AC10 16.03.10.13/16.03.10.20. Affected by this issue is the function fromSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument timeZone 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 identifier of this vulnerability is VDB-257780. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2855	A vulnerability classified as critical was found in Tenda AC15 15.03.05.18/15.03.05.19/15.03.20. Affected by this vulnerability is the function fromSetSysTime of the file /goform/SetSysTimeCfg. The manipulation of the argument time leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257779. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2706	A vulnerability, which was classified as critical, was found in Tenda AC10U 15.03.06.49. This affects the function formWifiWpsStart of the file /goform/WifiWpsStart. The manipulation of the argument index leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257457 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2852	A vulnerability was found in Tenda AC15 15.03.20_multi. It has been declared as critical. This vulnerability affects the function saveParentControlInfo of the file /goform/saveParentControlInfo. The manipulation of the argument urls leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257776. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2023-39307	Unrestricted Upload of File with Dangerous Type vulnerability in ThemeFusion Avada.This issue affects Avada: from n/a through 7.11.1.	8.5	More Details
CVE-2024-1856	In Progress® Telerik® Reporting versions prior to 2024 Q1 (18.0.24.130), a code execution attack is possible by a remote threat actor through an insecure deserialization vulnerability.	8.5	More Details
CVE-2024-1973	By leveraging the vulnerability, lower-privileged users of Content Manager can manipulate Content Manager clients to elevate privileges and perform unauthorized operations.	8.5	More Details
CVE-2024-27934	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Starting in version 1.36.2 and prior to version 1.40.3, use of inherently unsafe `*const c_void` and `ExternalPointer` leads to use-after-free access of the underlying structure, resulting in arbitrary code execution. Use of inherently unsafe `*const c_void` and `ExternalPointer` leads to use-after-free access of the underlying structure, which is exploitable by an attacker controlling the code executed inside a Deno runtime to obtain arbitrary code execution on the host machine regardless of permissions. This bug is known to be exploitable for both `*const c_void` and `ExternalPointer` implementations. Version 1.40.3 fixes this issue.	8.4	More Details
CVE-2024-29944	An attacker was able to inject an event handler into a privileged object that would allow arbitrary JavaScript execution in the parent process. Note: This vulnerability affects Desktop Firefox only, it does not affect mobile versions of Firefox. This vulnerability affects Firefox < 124.0.1 and Firefox ESR < 115.9.1.	8.4	More Details
CVE-2024-28582	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to execute arbitrary code via the rgbe_RGBEToFloat() function when reading images in HDR format.	8.4	More Details
CVE-2024-28581	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to execute arbitrary code via the _assignPixel<>() function when reading images in TARGA format.	8.4	More Details
CVE-2024-28580	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to execute arbitrary code via the ReadData() function when reading images in RAS format.	8.4	More Details
CVE-2024-28578	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to execute arbitrary code via the Load() function when reading images in RAS format.	8.4	More Details
CVE-2024-2448	An OS command injection vulnerability has been identified in LoadMaster. An authenticated UI user with any permission settings may be able to inject commands into a UI component using a shell command resulting in OS command injection.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28566	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to execute arbitrary code via the AssignPixel() function when reading images in TIFF format.	8.4	More Details
CVE-2024-25808	Cross-site Request Forgery (CSRF) vulnerability in Lychee version 3.1.6, allows remote attackers to execute arbitrary code via the create new album function.	8.3	More Details
CVE-2024-29194	OneUptime is a solution for monitoring and managing online services. The vulnerability lies in the improper validation of client-side stored data within the web application. Specifically, the is_master_admin key, stored in the local storage of the browser, can be manipulated by an attacker. By changing this key from false to true, the application grants administrative privileges to the user, without proper server-side validation. This has been patched in 7.0.1815.	8.3	More Details
CVE-2024-27933	Deno is a JavaScript, TypeScript, and WebAssembly runtime. In version 1.39.0, use of raw file descriptors in `op_node_ipc_pipe()` leads to premature close of arbitrary file descriptors, allowing standard input to be re-opened as a different resource resulting in permission prompt bypass. Node child_process IPC relies on the JS side to pass the raw IPC file descriptor to `op_node_ipc_pipe()`, which returns a `IpcJsonStreamResource` ID associated with the file descriptor. On closing the resource, the raw file descriptor is closed together. Use of raw file descriptors in `op_node_ipc_pipe()` leads to premature close of arbitrary file descriptors. This allow standard input (fd 0) to be closed and re-opened for a different resource, which allows a silent permission prompt bypass. This is exploitable by an attacker controlling the code executed inside a Deno runtime to obtain arbitrary code execution on the host machine regardless of permissions. This bug is known to be exploitable. There is a working exploit that achieves arbitrary code execution by bypassing prompts from zero permissions, additionally abusing the fact that Cache API lacks filesystem permission checks. The attack can be conducted silently as stderr can also be closed, suppressing all prompt outputs. Version 1.39.1 fixes the bug.	8.2	More Details
CVE-2024-0638	Least privilege violation in the Checkmk agent plugins mk_oracle, mk_oracle.ps1, and mk_oracle_crs before Checkmk 2.3.0b4 (beta), 2.2.0p24, 2.1.0p41 and 2.0.0 (EOL) allows local users to escalate privileges.	8.2	More Details
CVE-2024-2721	Deserialization of Untrusted Data vulnerability in Social Media Share Buttons By Sygnoos Social Media Share Buttons.This issue affects Social Media Share Buttons: from n/a through 2.1.0.	8.2	More Details
CVE-2024-2702	Missing Authorization vulnerability in Olive Themes Olive One Click Demo Import allows importing settings and data, ultimately leading to XSS.This issue affects Olive One Click Demo Import: from n/a through 1.1.1.	8.2	More Details
CVE-2024-29026	Owncast is an open source, self-hosted, decentralized, single user live video streaming and chat server. In versions 0.1.2 and prior, a lenient CORS policy allows attackers to make a cross origin request, reading privileged information. This can be used to leak the admin password. Commit 9215d9ba0f29d62201d3feea9e77dcd274581624 fixes this issue.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27918	Coder allows oragnizations to provision remote development environments via Terraform. Prior to versions 2.6.1, 2.7.3, and 2.8.4, a vulnerability in Coder's OIDC authentication could allow an attacker to bypass the `CODER_OIDC_EMAIL_DOMAIN` verification and create an account with an email not in the allowlist. Deployments are only affected if the OIDC provider allows users to create accounts on the provider. During OIDC registration, the user's email was improperly validated against the allowed `CODER_OIDC_EMAIL_DOMAIN`s. This could allow a user with a domain that only partially matched an allowed domain to successfully login or register. An attacker could register a domain name that exploited this vulnerability and register on a Coder instance with a public OIDC provider. Coder instances with OIDC enabled and protected by the `CODER_OIDC_EMAIL_DOMAIN` configuration are affected. Coder instances using a private OIDC provider are not affected, as arbitrary users cannot register through a private OIDC provider without first having an account on the provider. Public OIDC providers are impacted. GitHub authentication and external authentication are not impacted. This vulnerability is remedied in versions 2.8.4, 2.7.3, and 2.6.1 All versions prior to these patches are affected by the vulnerability.*It is recommended that customers upgrade their deployments as soon as possible if they are utilizing OIDC authentication with the `CODER_OIDC_EMAIL_DOMAIN` setting.	8.2	More Details
CVE-2024-24832	Missing Authorization vulnerability in Metagauss EventPrime.This issue affects EventPrime: from n/a through 3.3.9.	8.2	More Details
CVE-2024-28735	Unit4 Financials by Coda versions prior to 2023Q4 suffer from an incorrect access control authorization bypass vulnerability which allows an authenticated user to modify the password of any user of the application via a crafted request.	8.1	More Details
CVE-2024-24897	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in openEuler A-Tune-Collector on Linux allows Command Injection. This vulnerability is associated with program files https://gitee.Com/openeuler/A-Tune-Collector/blob/master/atune_collector/plugin/monitor/process/sched.Py. This issue affects A-Tune-Collector: from 1.1.0-3 through 1.3.0.	8.1	More Details
CVE-2024-0866	The Check & Log Email plugin for WordPress is vulnerable to Unauthenticated Hook Injection in all versions up to, and including, 1.0.9 via the check_nonce function. This makes it possible for unauthenticated attackers to execute actions with hooks in WordPress under certain circumstances. The action the attacker wishes to execute needs to have a nonce check, and the nonce needs to be known to the attacker. Furthermore, the absence of a capability check is a requirement.	8.1	More Details
CVE-2024-25567	Path traversal attack is possible and write outside of the intended directory and may access sensitive information. If a file name is specified that already exists on the file system, then the original file will be overwritten.	8.1	More Details
CVE-2024-28171	It is possible to perform a path traversal attack and write outside of the intended directory. If a file name is specified that already exists on the file system, then the original file will be overwritten.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28850	WP Crontrol controls the cron events on WordPress websites. WP Crontrol includes a feature that allows administrative users to create events in the WP-Cron system that store and execute PHP code subject to the restrictive security permissions documented here. While there is no known vulnerability in this feature on its own, there exists potential for this feature to be vulnerable to RCE if it were specifically targeted via vulnerability chaining that exploited a separate SQLi (or similar) vulnerability. This is exploitable on a site if one of the below preconditions are met, the site is vulnerable to a writeable SQLi vulnerability in any plugin, theme, or WordPress core, the site's database is compromised at the hosting level, the site is vulnerable to a method of updating arbitrary options in the wp_options table, or the site is vulnerable to a method of triggering an arbitrary action, filter, or function with control of the parameters. As a hardening measure, WP Crontrol version 1.16.2 ships with a new feature that prevents tampering of the code stored in a PHP cron event.	8.1	More Details
CVE-2024-24892	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'), Improper Privilege Management vulnerability in openEuler migration-tools on Linux allows Command Injection, Restful Privilege Elevation. This vulnerability is associated with program files https://gitee.Com/openeuler/migration-tools/blob/master/index.Py. This issue affects migration-tools: from 1.0.0 through 1.0.1.	8.1	More Details
CVE-2024-27105	Frappe is a full-stack web application framework. Prior to versions 14.66.3 and 15.16.0, file permission can be bypassed using certain endpoints, granting less privileged users permission to delete or clone a file. Versions 14.66.3 and 15.16.0 contain a patch for this issue. No known workarounds are available.	8.1	More Details
CVE-2023-51147	Buffer Overflow vulnerability in TRENDnet Trendnet AC1200 TEW-821DAP with firmware version 3.00b06 allows an attacker to execute arbitrary code via the adm_mod_pwd action.	8.0	More Details
CVE-2024-2463	Weak password recovery mechanism in CDeX application allows to retrieve password reset token.This issue affects CDeX application versions through 5.7.1.	8.0	More Details
CVE-2024-27521	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain an unauthenticated remote command execution (RCE) vulnerability via multiple parameters in the "setOpModeCfg" function. This security issue allows an attacker to take complete control of the device. In detail, exploitation allows unauthenticated, remote attackers to execute arbitrary system commands with administrative privileges (i.e., as user "root").	8.0	More Details
CVE-2023-51148	An issue in TRENDnet Trendnet AC1200 Dual Band PoE Indoor Wireless Access Point TEW-821DAP v.3.00b06 allows an attacker to execute arbitrary code via the 'mycli' command-line interface component.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29184	FreeScout is a self-hosted help desk and shared mailbox. A Stored Cross-Site Scripting (XSS) vulnerability has been identified within the Signature Input Field of the FreeScout Application prior to version 1.8.128. Stored XSS occurs when user input is not properly sanitized and is stored on the server, allowing an attacker to inject malicious scripts that will be executed when other users access the affected page. In this case, the Support Agent User can inject malicious scripts into their signature, which will then be executed when viewed by the Administrator. The application protects users against XSS attacks by enforcing a CSP policy, the CSP Policy is: `script-src 'self' 'nonce-abcd' `. The CSP policy only allows the inclusion of JS files that are present on the application server and doesn't allow any inline script or script other than nonce-abcd. The CSP policy was bypassed by uploading a JS file to the server by a POST request to /conversation/upload endpoint. After this, a working XSS payload was crafted by including the uploaded JS file link as the src of the script. This bypassed the CSP policy and XSS attacks became possible. The impact of this vulnerability is severe as it allows an attacker to compromise the FreeScout Application. By exploiting this vulnerability, the attacker can perform various malicious actions such as forcing the Administrator to execute actions without their knowledge or consent. For instance, the attacker can force the Administrator to add a new administrator controlled by the attacker, thereby giving the attacker full control over the application. Alternatively, the attacker can elevate the privileges of a low-privileged user to Administrator, further compromising the security of the application. Attackers can steal sensitive information such as login credentials, session tokens, personal identifiable information (PII), and financial data. The vulnerability can also lead to defacement of the Application. Version 1.8.128 contains a patch for this issue.	8.0	More Details
CVE-2023-48275	Unrestricted Upload of File with Dangerous Type vulnerability in Trustindex.Io Widgets for Google Reviews.This issue affects Widgets for Google Reviews: from n/a through 11.0.2.	8.0	More Details
CVE-2024-2469	An attacker with an Administrator role in GitHub Enterprise Server could gain SSH root access via remote code execution. This vulnerability affected GitHub Enterprise Server version 3.8.0 and above and was fixed in version 3.8.17, 3.9.12, 3.10.9, 3.11.7 and 3.12.1. This vulnerability was reported via the GitHub Bug Bounty program.	8.0	More Details
CVE-2023-51146	Buffer Overflow vulnerability in TRENDnet AC1200 TEW-821DAP with firmware version 3.00b06 allows an attacker to execute arbitrary code via the adm_add_user action.	8.0	More Details
CVE-2024-29188	WiX toolset lets developers create installers for Windows Installer, the Windows installation engine. The custom action behind WiX's `RemoveFolderEx` functionality could allow a standard user to delete protected directories. `RemoveFolderEx` deletes an entire directory tree during installation or uninstallation. It does so by recursing every subdirectory starting at a specified directory and adding each subdirectory to the list of directories Windows Installer should delete. If the setup author instructed `RemoveFolderEx` to delete a per-user folder from a per-machine installer, an attacker could create a directory junction in that per-user folder pointing to a per-machine, protected directory. Windows Installer, when executing the per-machine installer after approval by an administrator, would delete the target of the directory junction. This vulnerability is fixed in 3.14.1 and 4.0.5.	7.9	More Details
CVE-2023-6175	NetScreen file parser crash in Wireshark 4.0.0 to 4.0.10 and 3.6.0 to 3.6.18 allows denial of service via crafted capture file	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28521	SQL Injection vulnerability in Netcome NS-ASG Application Security Gateway v.6.3.1 allows a local attacker to execute arbitrary code and obtain sensitive information via a crafted script to the loginid parameter of the /singlelogin.php component.	7.8	More Details
CVE-2024-21912	An arbitrary code execution vulnerability in Rockwell Automation Arena Simulation could let a malicious user insert unauthorized code into the software. This is done by writing beyond the designated memory area, which causes an access violation. Once inside, the threat actor can run harmful code on the system. This affects the confidentiality, integrity, and availability of the product. To trigger this, the user would unwittingly need to open a malicious file shared by the threat actor.	7.8	More Details
CVE-2024-24520	An issue in Lepton CMS v.7.0.0 allows a local attacker to execute arbitrary code via the upgrade.php file in the languages place.	7.8	More Details
CVE-2024-28131	EasyRange Ver 1.41 contains an issue with the executable file search path when displaying an extracted file on Explorer, which may lead to loading an executable file resides in the same folder where the extracted file is placed. If this vulnerability is exploited, arbitrary code may be executed with the privilege of the running program. Note that the developer was unreachable, therefore, users should consider stop using EasyRange Ver 1.41.	7.8	More Details
CVE-2024-30202	In Emacs before 29.3, arbitrary Lisp code is evaluated as part of turning on Org mode. This affects Org Mode before 9.6.23.	7.8	More Details
CVE-2024-21913	A heap-based memory buffer overflow vulnerability in Rockwell Automation Arena Simulation software could potentially allow a malicious user to insert unauthorized code into the software by overstepping the memory boundaries, which triggers an access violation. Once inside, the threat actor can run harmful code on the system. This affects the confidentiality, integrity, and availability of the product. To trigger this, the user would unwittingly need to open a malicious file shared by the threat actor.	7.8	More Details
CVE-2021-47137	In the Linux kernel, the following vulnerability has been resolved: net: lantiq: fix memory corruption in RX ring In a situation where memory allocation or dma mapping fails, an invalid address is programmed into the descriptor. This can lead to memory corruption. If the memory allocation fails, DMA should reuse the previous skb and mapping and drop the packet. This patch also increments rx drop counter.	7.8	More Details
CVE-2023-41099	In the Windows installer in Atos Eviden CardOS API before 5.5.5.2811, Local Privilege Escalation can occur.(from a regular user to SYSTEM).	7.8	More Details
CVE-2024-21919	An uninitialized pointer in Rockwell Automation Arena Simulation software could potentially allow a malicious user to insert unauthorized code to the software by leveraging the pointer after it is properly. Once inside, the threat actor can run harmful code on the system. This affects the confidentiality, integrity, and availability of the product. To trigger this, the user would unwittingly need to open a malicious file shared by the threat actor.	7.8	More Details
CVE-2024-28569	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to execute arbitrary code via the Imf_2_2::Xdr::read() function when reading images in EXR format.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21918	A memory buffer vulnerability in Rockwell Automation Arena Simulation software could potentially allow a malicious user to insert unauthorized code to the software by corrupting the memory and triggering an access violation. Once inside, the threat actor can run harmful code on the system. This affects the confidentiality, integrity, and availability of the product. To trigger this, the user would unwittingly need to open a malicious file shared by the threat actor.	7.8	More Details
CVE-2024-28583	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to execute arbitrary code via the readLine() function when reading images in XPM format.	7.8	More Details
CVE-2021-47148	In the Linux kernel, the following vulnerability has been resolved: octeontx2-pf: fix a buffer overflow in otx2_set_rxfh_context() This function is called from ethtool_set_rxfh() and "*rss_context" comes from the user. Add some bounds checking to prevent memory corruption.	7.8	More Details
CVE-2024-2929	A memory corruption vulnerability in Rockwell Automation Arena Simulation software could potentially allow a malicious user to insert unauthorized code to the software by corrupting the memory triggering an access violation. Once inside, the threat actor can run harmful code on the system. This affects the confidentiality, integrity, and availability of the product. To trigger this, the user would unwittingly need to open a malicious file shared by the threat actor.	7.8	More Details
CVE-2024-1848	Heap-based Buffer Overflow, Memory Corruption, Out-Of-Bounds Read, Out-Of-Bounds Write, Stack-based Buffer Overflow, Type Confusion, Uninitialized Variable, Use-After-Free vulnerabilities exist in the file reading procedure in SOLIDWORKS Desktop on Release SOLIDWORKS 2024. These vulnerabilities could allow an attacker to execute arbitrary code while opening a specially crafted CATPART, DWG, DXF, IPT, JT, SAT, SLDDRW, SLDPRT, STL, STP, X_B or X_T file.	7.8	More Details
CVE-2024-2955	T.38 dissector crash in Wireshark 4.2.0 to 4.0.3 and 4.0.0 to 4.0.13 allows denial of service via packet injection or crafted capture file	7.8	More Details
CVE-2024-24890	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in openEuler gala-gopher on Linux allows Command Injection. This vulnerability is associated with program files https://gitee.Com/openeuler/gala-gopher/blob/master/src/probes/extends/ebpf.Probe/src/ioprobe/ioprobe.C. This issue affects gala-gopher: through 1.0.2.	7.8	More Details
CVE-2024-1801	In Progress® Telerik® Reporting versions prior to 2024 Q1 (18.0.24.130), a code execution attack is possible by a local threat actor through an insecure deserialization vulnerability.	7.7	More Details
CVE-2024-2887	Type Confusion in WebAssembly in Google Chrome prior to 123.0.6312.86 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	7.7	More Details
CVE-2024-28434	The CRM platform Twenty is vulnerable to stored cross site scripting via file upload in version 0.3.0. A crafted svg file can trigger the execution of the javascript code.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23991	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPdevelop / Oplugins Booking Calendar allows SQL Injection.This issue affects Booking Calendar: from n/a through 9.4.3.	7.6	More Details
CVE-2024-2053	The Artica Proxy administrative web application will deserialize arbitrary PHP objects supplied by unauthenticated users and subsequently enable code execution as the "www-data" user. This issue was demonstrated on version 4.50 of the The Artica-Proxy administrative web application attempts to prevent local file inclusion. These protections can be bypassed and arbitrary file requests supplied by unauthenticated users will be returned according to the privileges of the "www-data" user.	7.5	More Details
CVE-2023-5685	A flaw was found in XNIO. The XNIO NotifierState that can cause a Stack Overflow Exception when the chain of notifier states becomes problematically large can lead to uncontrolled resource management and a possible denial of service (DoS).	7.5	More Details
CVE-2024-26577	VSeeFace through 1.13.38.c2 allows attackers to cause a denial of service (application hang) via a spoofed UDP packet containing at least 10 digits in JSON data.	7.5	More Details
CVE-2024-29059	.NET Framework Information Disclosure Vulnerability	7.5	More Details
CVE-2024-29190	Mobile Security Framework (MobSF) is a pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis. In version 3.9.5 Beta and prior, MobSF does not perform any input validation when extracting the hostnames in `android:host`, so requests can also be sent to local hostnames. This can lead to server-side request forgery. An attacker can cause the server to make a connection to internal-only services within the organization's infrastructure. Commit 5a8eeee73c5f504a6c3abdf2a139a13804efdb77 has a hotfix for this issue.	7.5	More Details
CVE-2024-1394	A memory leak flaw was found in Golang in the RSA encrypting/decrypting code, which might lead to a resource exhaustion vulnerability using attacker-controlled inputs. The memory leak happens in github.com/golang-fips/openssl/openssl/rsa.go#L113. The objects leaked are pkey and ctx. That function uses named return parameters to free pkey and ctx if there is an error initializing the context or setting the different properties. All return statements related to error cases follow the "return nil, nil, fail(...)" pattern, meaning that pkey and ctx will be nil inside the deferred function that should free them.	7.5	More Details
CVE-2024-2426	A denial-of-service vulnerability exists in the Rockwell Automation PowerFlex® 527 due to improper input validation in the device. If exploited, a disruption in the CIP communication will occur and a manual restart will be required by the user to recover it.	7.5	More Details
CVE-2024-28101	The Apollo Router is a graph router written in Rust to run a federated supergraph that uses Apollo Federation. Versions 0.9.5 until 1.40.2 are subject to a Denial-of-Service (DoS) type vulnerability. When receiving compressed HTTP payloads, affected versions of the Router evaluate the `limits.http_max_request_bytes` configuration option after the entirety of the compressed payload is decompressed. If affected versions of the Router receive highly compressed payloads, this could result in significant memory consumption while the compressed payload is expanded. Router version 1.40.2 has a fix for the vulnerability. Those who are unable to upgrade may be able to implement mitigations at proxies or load balancers positioned in front of their Router fleet (e.g. Nginx, HAProxy, or cloud-native WAF services) by creating limits on HTTP body upload size.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2427	A denial-of-service vulnerability exists in the Rockwell Automation PowerFlex® 527 due to improper traffic throttling in the device. If multiple data packets are sent to the device repeatedly the device will crash and require a manual restart to recover.	7.5	More Details
CVE-2024-22084	An issue was discovered in Elspec G5 digital fault recorder versions 1.1.4.15 and before. Cleartext passwords and hashes are exposed through log files.	7.5	More Details
CVE-2024-0901	Remotely executed SEGV and out of bounds read allows malicious packet sender to crash or cause an out of bounds read via sending a malformed packet with the correct length.	7.5	More Details
CVE-2024-29301	SourceCodester PHP Task Management System 1.0 is vulnerable to SQL Injection via update-admin.php?admin_id=	7.5	More Details
CVE-2024-22082	An issue was discovered in Elspec G5 digital fault recorder versions 1.1.4.15 and before. Unauthenticated directory listing can occur: the web interface cay be abused be an attacker get a better understanding of the operating system.	7.5	More Details
CVE-2024-29302	SourceCodester PHP Task Management System 1.0 is vulnerable to SQL Injection via update-employee.php.	7.5	More Details
CVE-2024-27292	Docassemble is an expert system for guided interviews and document assembly. The vulnerability allows attackers to gain unauthorized access to information on the system through URL manipulation. It affects versions 1.4.53 to 1.4.96. The vulnerability has been patched in version 1.4.97 of the master branch.	7.5	More Details
CVE-2024-25136	There is a function in AutomationDirect C-MORE EA9 HMI that allows an attacker to send a relative path in the URL without proper sanitizing of the content.	7.5	More Details
CVE-2024-28286	In mz-automation libiec61850 v1.4.0, a NULL Pointer Dereference was detected in the mmsServer_handleFileCloseRequest.c function of src/mms/iso_mms/server/mms_file_service.c. The vulnerability manifests as SEGV and causes the application to crash	7.5	More Details
CVE-2024-22079	An issue was discovered in Elspec G5 digital fault recorder versions 1.1.4.15 and before. Directory traversal can occur via the system logs download mechanism.	7.5	More Details
CVE-2024-2425	A denial-of-service vulnerability exists in the Rockwell Automation PowerFlex® 527 due to improper input validation in the device. If exploited, the web server will crash and need a manual restart to recover it.	7.5	More Details
CVE-2024-29862	The Kerlink firewall in ChirpStack chirpstack-mqtt-forwarder before 4.2.1 and chirpstack-gateway-bridge before 4.0.11 wrongly accepts certain TCP packets when a connection is not in the ESTABLISHED state.	7.5	More Details
CVE-2024-30156	Varnish Cache before 7.3.2 and 7.4.x before 7.4.3 (and before 6.0.13 LTS), and Varnish Enterprise 6 before 6.0.12r6, allows credits exhaustion for an HTTP/2 connection control flow window, aka a Broke Window Attack.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24813	Frappe is a full-stack web application framework. Prior to versions 14.64.0 and 15.0.0, SQL injection from a particular whitelisted method can result in access to data which the user doesn't have permission to access. Versions 14.64.0 and 15.0.0 contain a patch for this issue. No known workarounds are available.	7.5	More Details
CVE-2024-23721	A Directory Traversal issue was discovered in process_post on Draytek Vigor3910 4.3.2.5 devices. When sending a certain POST request, it calls the function and exports information.	7.5	More Details
CVE-2024-28387	An issue in axonaut v.3.1.23 and before allows a remote attacker to obtain sensitive information via the log.txt component.	7.5	More Details
CVE-2024-28442	Directory Traversal vulnerability in Yealink VP59 v.91.15.0.118 allows a physically proximate attacker to obtain sensitive information via terms of use function in the company portal component.	7.5	More Details
CVE-2024-29031	Meshery is an open source, cloud native manager that enables the design and management of Kubernetes-based infrastructure and applications. A SQL injection vulnerability in Meshery prior to version 0.7.17 allows a remote attacker to obtain sensitive information via the `order` parameter of `GetMeshSyncResources`. Version 0.7.17 contains a patch for this issue.	7.5	More Details
CVE-2024-23722	In Fluent Bit 2.1.8 through 2.2.1, a NULL pointer dereference can be caused via an invalid HTTP payload with the content type of x-www-form-urlencoded. It crashes and does not restart. This could result in logs not being delivered properly.	7.5	More Details
CVE-2024-29033	OAuthenticator provides plugins for JupyterHub to use common OAuth providers, as well as base classes for writing one's own Authenticators with any OAuth 2.0 provider. `GoogleOAuthenticator.hosted_domain` is used to restrict what Google accounts can be authorized access to a JupyterHub. The restriction is intented to be to Google accounts part of one or more Google organization verified to control specified domain(s). Prior to version 16.3.0, the actual restriction has been to Google accounts with emails ending with the domain. Such accounts could have been created by anyone which at one time was able to read an email associated with the domain. This was described by Dylan Ayrey (@dxa4481) in this [blog post] from 15th December 2023). OAuthenticator 16.3.0 contains a patch for this issue. As a workaround, restrict who can login another way, such as `allowed_users` or `allowed_google_groups`.	7.5	More Details
CVE-2023-44989	Insertion of Sensitive Information into Log File vulnerability in GSheetConnector CF7 Google Sheets Connector.This issue affects CF7 Google Sheets Connector: from n/a through 5.0.5.	7.5	More Details
CVE-2023-50967	latchset jose through version 11 allows attackers to cause a denial of service (CPU consumption) via a large p2c (aka PBES2 Count) value.	7.5	More Details
CVE-2023-41038	Firebird is a relational database. Versions 4.0.0 through 4.0.3 and version 5.0 beta1 are vulnerable to a server crash when a user uses a specific form of SET BIND statement. Any non-privileged user with minimum access to a server may type a statement with a long `CHAR` length, which causes the server to crash due to stack corruption. Versions 4.0.4.2981 and 5.0.0.117 contain fixes for this issue. No known workarounds are available.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28396	An issue in MyPrestaModules ordersexport v.6.0.2 and before allows a remote attacker to execute arbitrary code via the download.php component.	7.5	More Details
CVE-2023-47150	IBM Common Cryptographic Architecture (CCA) 7.0.0 through 7.5.36 could allow a remote user to cause a denial of service due to incorrect data handling for certain types of AES operations. IBM X-Force ID: 270602.	7.5	More Details
CVE-2024-2725	Information exposure vulnerability in the CIGESv2 system. A remote attacker might be able to access /vendor/composer/installed.json and retrieve all installed packages used by the application.	7.5	More Details
CVE-2024-2886	Use after free in WebCodecs in Google Chrome prior to 123.0.6312.86 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	7.5	More Details
CVE-2024-21505	Versions of the package web3-utils before 4.2.1 are vulnerable to Prototype Pollution via the utility functions format and mergeDeep, due to insecure recursive merge. An attacker can manipulate an object's prototype, potentially leading to the alteration of the behavior of all objects inheriting from the affected prototype by passing specially crafted input to these functions.	7.5	More Details
CVE-2024-28551	Tenda AC18 V15.03.05.05 has a stack overflow vulnerability in the ssid parameter of form_fast_setting_wifi_set function.	7.5	More Details
CVE-2023-49979	A directory listing vulnerability in Customer Support System v1 allows attackers to list directories and sensitive files within the application without requiring authorization.	7.5	More Details
CVE-2023-49980	A directory listing vulnerability in Best Student Result Management System v1.0 allows attackers to list directories and sensitive files within the application without requiring authorization.	7.5	More Details
CVE-2023-49981	A directory listing vulnerability in School Fees Management System v1.0 allows attackers to list directories and sensitive files within the application without requiring authorization.	7.5	More Details
CVE-2024-2449	A cross-site request forgery vulnerability has been identified in LoadMaster. It is possible for a malicious actor, who has prior knowledge of the IP or hostname of a specific LoadMaster, to direct an authenticated LoadMaster administrator to a third-party site. In such a scenario, the CSRF payload hosted on the malicious site would execute HTTP transactions on behalf of the LoadMaster administrator.	7.5	More Details
CVE-2023-27459	Deserialization of Untrusted Data vulnerability in WPEverest User Registration.This issue affects User Registration: from n/a through 2.3.2.1.	7.4	More Details
CVE-2024-29499	Anchor CMS v0.12.7 was discovered to contain a Cross-Site Request Forgery (CSRF) via /anchor/admin/users/delete/2.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2459	The UX Flat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'button' shortcode in all versions up to, and including, 4.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.4	More Details
CVE-2024-29189	PyAnsys Geometry is a Python client library for the Ansys Geometry service and other CAD Ansys products. On file src/ansys/geometry/core/connection/product_instance.py, upon calling this method _start_program directly, users could exploit its usage to perform malicious operations on the current machine where the script is ran. This vulnerability is fixed in 0.3.3 and 0.4.12.	7.4	More Details
CVE-2024-29180	Prior to versions 7.1.0, 6.1.2, and 5.3.4, the webpack-dev-middleware development middleware for devpack does not validate the supplied URL address sufficiently before returning the local file. It is possible to access any file on the developer's machine. The middleware can either work with the physical filesystem when reading the files or it can use a virtualized in-memory `memfs` filesystem. If `writeToDisk` configuration option is set to `true`, the physical filesystem is used. The `getFilenameFromUrl` method is used to parse URL and build the local file path. The public path prefix is stripped from the URL, and the `unsecaped` path suffix is appended to the `outputPath`. As the URL is not unescaped and normalized automatically before calling the midlleware, it is possible to use `%2e` and `%2f` sequences to perform path traversal attack. Developers using `webpack-dev-server` or `webpack-dev-middleware` are affected by the issue. When the project is started, an attacker might access any file on the developer's machine and exfiltrate the content. If the development server is listening on a public IP address (or `0.0.0.0`), an attacker on the local network can access the local files without any interaction from the victim (direct connection to the port). If the server allows access from third-party domains, an attacker can send a malicious link to the victim. When visited, the client side script can connect to the local server and exfiltrate the local files. Starting with fixed versions 7.1.0, 6.1.2, and 5.3.4, the URL is unescaped and normalized before any further processing.	7.4	More Details
CVE-2024-2014	A vulnerability classified as critical was found in Panabit Panalog 202103080942. This vulnerability affects unknown code of the file /Maintain/sprog_upstatus.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-255268. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-29131	Out-of-bounds Write vulnerability in Apache Commons Configuration.This issue affects Apache Commons Configuration: from 2.0 before 2.10.1. Users are recommended to upgrade to version 2.10.1, which fixes the issue.	7.3	More Details
CVE-2024-28123	Wasmi is an efficient and lightweight WebAssembly interpreter with a focus on constrained and embedded systems. In the WASMI Interpreter, an Out-of-bounds Buffer Write will arise if the host calls or resumes a Wasm function with more parameters than the default limit (128), as it will surpass the stack value. This doesn’t affect calls from Wasm to Wasm, only from host to Wasm. This vulnerability was patched in version 0.31.1.	7.3	More Details
CVE-2024-2864	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KaineLabs Youzify - Buddypress Moderation.This issue affects Youzify - Buddypress Moderation: from n/a through 1.2.5.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29187	WiX toolset lets developers create installers for Windows Installer, the Windows installation engine. When a bundle runs as SYSTEM user, Burn uses GetTempPathW which points to an insecure directory C:\Windows\Temp to drop and load multiple binaries. Standard users can hijack the binary before it's loaded in the application resulting in elevation of privileges. This vulnerability is fixed in 3.14.1 and 4.0.5.	7.3	More Details
CVE-2024-2927	A vulnerability was found in code-projects Mobile Shop 1.0. It has been classified as critical. Affected is an unknown function of the file Details.php of the component Login Page. 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. The identifier of this vulnerability is VDB-258000.	7.3	More Details
CVE-2023-41972	In some rare cases, there is a password type validation missing in Revert Password check and for some features it could be disabled. Fixed Version: Win ZApp 4.3.0.121 and later.	7.3	More Details
CVE-2024-2212	In Eclipse ThreadX before 6.4.0, xQueueCreate() and xQueueCreateSet() functions from the FreeRTOS compatibility API (utility/rtos_compatibility_layers/FreeRTOS/tx_freertos.c) were missing parameter checks. This could lead to integer wraparound, under-allocations and heap buffer overflows.	7.3	More Details
CVE-2024-28033	OS command injection vulnerability exists in WebProxy 1.7.8 and 1.7.9, which may allow a remote unauthenticated attacker to execute an arbitrary OS command with the privilege of the running web server. Note that the developer was unreachable, therefore, users should consider stop using WebProxy 1.7.8 and 1.7.9.	7.3	More Details
CVE-2024-2916	A vulnerability was found in Campcodes House Rental Management System 1.0. It has been classified as critical. Affected is an unknown function of the file ajax.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. VDB-257982 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2021-33633	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in openEuler aops-ceres on Linux allows Command Injection. This vulnerability is associated with program files ceres/function/util.Py. This issue affects aops-ceres: from 1.3.0 through 1.4.1.	7.3	More Details
CVE-2023-41969	An arbitrary file deletion in ZSATrayManager where it protects the temporary encrypted ZApp issue reporting file from the unprivileged end user access and modification. Fixed version: Win ZApp 4.3.0 and later.	7.3	More Details
CVE-2023-41973	ZSATray passes the previousInstallerName as a config parameter to TrayManager, and TrayManager constructs the path and appends previousInstallerName to get the full path of the exe. Fixed Version: Win ZApp 4.3.0.121 and later.	7.3	More Details
CVE-2024-25420	An issue in Ignite Realtime Openfire v.4.9.0 and before allows a remote attacker to escalate privileges via the admin.authorizedJIDs system property component.	7.2	More Details
CVE-2023-6091	Unrestricted Upload of File with Dangerous Type vulnerability in mndpsingh287 Theme Editor.This issue affects Theme Editor: from n/a through 2.7.1.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50895	In Janitza GridVis through 9.0.66, exposed dangerous methods in the de.janitza.pasw.project.server.ServerDatabaseProject project load functionality allow remote authenticated administrative users to execute arbitrary Groovy code.	7.2	More Details
CVE-2023-41877	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A path traversal vulnerability in versions 2.23.4 and prior requires GeoServer Administrator with access to the admin console to misconfigure the Global Settings for log file location to an arbitrary location. The admin console GeoServer Logs page provides a preview of these contents. As this issue requires GeoServer administrators access, often representing a trusted party, the vulnerability has not received a patch as of time of publication. As a workaround, a system administrator responsible for running GeoServer can use the `GEOSERVER_LOG_FILE` setting to override any configuration option provided by the Global Settings page. The `GEOSERVER_LOG_LOCATION` parameter can be set as system property, environment variables, or servlet context parameters.	7.2	More Details
CVE-2023-51444	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. An arbitrary file upload vulnerability exists in versions prior to 2.23.4 and 2.24.1 that enables an authenticated administrator with permissions to modify coverage stores through the REST Coverage Store API to upload arbitrary file contents to arbitrary file locations which can lead to remote code execution. Coverage stores that are configured using relative paths use a GeoServer Resource implementation that has validation to prevent path traversal but coverage stores that are configured using absolute paths use a different Resource implementation that does not prevent path traversal. This vulnerability can lead to executing arbitrary code. An administrator with limited privileges could also potentially exploit this to overwrite GeoServer security files and obtain full administrator privileges. Versions 2.23.4 and 2.24.1 contain a fix for this issue.	7.2	More Details
CVE-2024-24899	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in openEuler aops-zeus on Linux allows Command Injection. This vulnerability is associated with program files https://gitee.Com/openeuler/aops-zeus/blob/master/zeus/conf/constant.Py. This issue affects aops-zeus: from 1.2.0 through 1.4.0.	7.2	More Details
CVE-2023-49978	Incorrect access control in Customer Support System v1 allows non-administrator users to access administrative pages and execute actions reserved for administrators.	7.2	More Details
CVE-2024-28105	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. The category image upload function in phpmyfaq is vulnerable to manipulation of the `Content-type` and `lang` parameters, allowing attackers to upload malicious files with a .php extension, potentially leading to remote code execution (RCE) on the system. This vulnerability is fixed in 3.2.6.	7.2	More Details
CVE-2024-27935	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Starting in version 1.35.1 and prior to version 1.36.3, a vulnerability in Deno's Node.js compatibility runtime allows for cross-session data contamination during simultaneous asynchronous reads from Node.js streams sourced from sockets or files. The issue arises from the re-use of a global buffer (BUF) in stream_wrap.ts used as a performance optimization to limit allocations during these asynchronous read operations. This can lead to data intended for one session being received by another session, potentially resulting in data corruption and unexpected behavior. This affects all users of Deno that use the node.js compatibility layer for network communication or other streams, including packages that may require node.js libraries indirectly. Version 1.36.3 contains a patch for this issue.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27440	Unrestricted Upload of File with Dangerous Type vulnerability in OnTheGoSystems Types.This issue affects Types: from n/a through 3.4.17.	7.2	More Details
CVE-2024-30205	In Emacs before 29.3, Org mode considers contents of remote files to be trusted. This affects Org Mode before 9.6.23.	7.1	More Details
CVE-2024-29879	Cross-Site Scripting (XSS) vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/index/getdepartments/format/html, 'business_id' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted URL to the victim and steal their session data.	7.1	More Details
CVE-2024-29877	Cross-Site Scripting (XSS) vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/expenses/expensecategories/edit, 'expense_category_name' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted URL to the victim and steal their session data.	7.1	More Details
CVE-2024-27993	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Typps Calendarista Basic Edition.This issue affects Calendarista Basic Edition: from n/a through 3.0.2.	7.1	More Details
CVE-2024-27994	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in YITH YITH WooCommerce Product Add-Ons allows Reflected XSS.This issue affects YITH WooCommerce Product Add-Ons: from n/a through 4.5.0.	7.1	More Details
CVE-2024-27968	Cross-Site Request Forgery (CSRF) vulnerability in Optimole Super Page Cache for Cloudflare allows Stored XSS.This issue affects Super Page Cache for Cloudflare: from n/a through 4.7.5.	7.1	More Details
CVE-2024-2465	Open redirection vulnerability in CDeX application allows to redirect users to arbitrary websites via a specially crafted URL.This issue affects CDeX application versions through 5.7.1.	7.1	More Details
CVE-2024-29878	Cross-Site Scripting (XSS) vulnerability in Sentrifugo 3.2, through /sentrifugo/index.php/sitepreference/add, 'description' parameter. The exploitation of this vulnerability could allow a remote user to send a specially crafted URL to the victim and steal their session data.	7.1	More Details
CVE-2024-27962	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Florian 'fkrauthan' Krauthan allows Reflected XSS.This issue affects wp-mpdf: from n/a through 3.7.1.	7.1	More Details
CVE-2023-45771	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Contact Form With Captcha allows Reflected XSS.This issue affects Contact Form With Captcha: from n/a through 1.6.8.	7.1	More Details
CVE-2023-33322	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Etoile Web Design Front End Users allows Reflected XSS.This issue affects Front End Users: from n/a before 3.2.25.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-49839	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KlbTheme Cosmetsy theme (core plugin), KlbTheme Partdo theme (core plugin), KlbTheme Bacola theme (core plugin), KlbTheme Medibazar theme (core plugin), KlbTheme Furnob theme (core plugin), KlbTheme Clotya theme (core plugin) allows Reflected XSS.This issue affects Cosmetsy theme (core plugin): from n/a through 1.3.0; Partdo theme (core plugin): from n/a through 1.0.9; Bacola theme (core plugin): from n/a through 1.3.3; Medibazar theme (core plugin): from n/a through 1.2.3; Furnob theme (core plugin): from n/a through 1.1.7; Clotya theme (core plugin): from n/a through 1.1.5.	7.1	More Details
CVE-2023-28687	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in perfectwpthemes Glaze Blog Lite, themebeez Fascinate, themebeez Cream Blog, themebeez Cream Magazine allows Reflected XSS.This issue affects Glaze Blog Lite: from n/a through <= 1.1.4; Fascinate: from n/a through 1.0.8; Cream Blog: from n/a through 2.1.3; Cream Magazine: from n/a through 2.1.4.	7.1	More Details
CVE-2024-27916	Minder is a software supply chain security platform. Prior to version 0.0.33, a Minder user can use the endpoints `GetRepositoryByName`, `DeleteRepositoryByName`, and `GetArtifactByName` to access any repository in the database, irrespective of who owns the repo and any permissions present. The database query checks by repo owner, repo name and provider name (which is always `github`). These query values are not distinct for the particular user - as long as the user has valid credentials and a provider, they can set the repo owner/name to any value they want and the server will return information on this repo. Version 0.0.33 contains a patch for this issue.	7.1	More Details
CVE-2024-1933	Insecure UNIX Symbolic Link (Symlink) Following in TeamViewer Remote Client prior Version 15.52 for macOS allows an attacker with unprivileged access, to potentially elevate privileges or conduct a denial-of-service-attack by overwriting the symlink.	7.1	More Details
CVE-2024-2228	This vulnerability allows an authenticated user to perform a Lifecycle Manager flow or other QuickLink for a target user outside of the defined QuickLink Population.	7.1	More Details
CVE-2024-1983	The Simple Ajax Chat WordPress plugin before 20240223 does not prevent visitors from using malicious Names when using the chat, which will be reflected unsanitized to other users.	7.1	More Details
CVE-2024-23482	The ZScaler service is susceptible to a local privilege escalation vulnerability found in the ZScalerService process. Fixed Version: Mac ZApp 4.2.0.241 and later.	7.0	More Details
CVE-2024-2214	In Eclipse ThreadX before version 6.4.0, the _Mtxinit() function in the Xtensa port was missing an array size check causing a memory overwrite. The affected file was ports/xtensa/xcc/src/tx_clib_lock.c	7.0	More Details
CVE-2023-35899	IBM Cloud Pak for Automation 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, 22.0.1, and 22.0.2 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 259354.	7.0	More Details
CVE-2021-33632	Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in openEuler iSulad on Linux allows Leveraging Time-of-Check and Time-of-Use (TOCTOU) Race Conditions. This vulnerability is associated with program files https://gitee.Com/openeuler/iSulad/blob/master/src/cmd/isulad/main.C. This issue affects iSulad: 2.0.18-13, from 2.1.4-1 through 2.1.4-2.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2452	In Eclipse ThreadX NetX Duo before 6.4.0, if an attacker can control parameters of __portable_aligned_alloc() could cause an integer wrap-around and an allocation smaller than expected. This could cause subsequent heap buffer overflows.	7.0	More Details
CVE-2024-28102	JWCrypto implements JWK, JWS, and JWE specifications using python-cryptography. Prior to version 1.5.6, an attacker can cause a denial of service attack by passing in a malicious JWE Token with a high compression ratio. When the server processes this token, it will consume a lot of memory and processing time. Version 1.5.6 fixes this vulnerability by limiting the maximum token length.	6.8	More Details
CVE-2023-49983	A cross-site scripting (XSS) vulnerability in the component /management/class of School Fees Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the name parameter.	6.8	More Details
CVE-2024-29034	CarrierWave is a solution for file uploads for Rails, Sinatra and other Ruby web frameworks. The vulnerability CVE-2023-49090 wasn't fully addressed. This vulnerability is caused by the fact that when uploading to object storage, including Amazon S3, it is possible to set a Content-Type value that is interpreted by browsers to be different from what's allowed by `content_type_allowlist`, by providing multiple values separated by commas. This bypassed value can be used to cause XSS. Upgrade to 3.0.7 or 2.2.6.	6.8	More Details
CVE-2024-28562	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to execute arbitrary code via the Imf_2_2::copyIntoFrameBuffer() component when reading images in EXR format.	6.8	More Details
CVE-2024-25958	Dell Grab for Windows, versions up to and including 5.0.4, contain Weak Application Folder Permissions vulnerability. A local authenticated attacker could potentially exploit this vulnerability, leading to privilege escalation, unauthorized access to application data, unauthorized modification of application data and service disruption.	6.7	More Details
CVE-2024-25359	An issue in zuoxingdong lagom v.0.1.2 allows a local attacker to execute arbitrary code via the pickle_load function of the serialize.py file.	6.6	More Details
CVE-2024-22724	An issue was discovered in osCommerce v4, allows local attackers to bypass file upload restrictions and execute arbitrary code via administrator profile photo upload feature.	6.6	More Details
CVE-2024-30234	Missing Authorization vulnerability in Wholesale Team WholesaleX.This issue affects WholesaleX: from n/a through 1.3.1.	6.5	More Details
CVE-2024-29197	Pimcore is an Open Source Data & Experience Management Platform. Any call with the query argument `?pimcore_preview=true` allows to view unpublished sites. In previous versions of Pimcore, session information would propagate to previews, so only a logged in user could open a preview. This no longer applies. Previews are broad open to any user and with just the hint of a restricted link one could gain access to possible confident / unreleased information. This vulnerability is fixed in 11.2.2 and 11.1.6.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27286	Zulip is an open-source team collaboration. When a user moves a Zulip message, they have the option to move all messages in the topic, move only subsequent messages as well, or move just a single message. If the user chose to just move one message, and was moving it from a public stream to a private stream, Zulip would successfully move the message, -- but active users who did not have access to the private stream, but whose client had already received the message, would continue to see the message in the public stream until they reloaded their client. Additionally, Zulip did not remove view permissions on the message from recently-active users, allowing the message to show up in the "All messages" view or in search results, but not in "Inbox" or "Recent conversations" views. While the bug has been present since moving messages between streams was first introduced in version 3.0, this option became much more common starting in Zulip 8.0, when the default option in the picker for moving the very last message in a conversation was changed. This issue is fixed in Zulip Server 8.3. No known workarounds are available.	6.5	More Details
CVE-2024-2888	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BoldGrid Post and Page Builder by BoldGrid – Visual Drag and Drop Editor allows Stored XSS.This issue affects Post and Page Builder by BoldGrid – Visual Drag and Drop Editor: from n/a through 1.26.2.	6.5	More Details
CVE-2023-27608	Missing Authorization vulnerability in WP Swings Points and Rewards for WooCommerce.This issue affects Points and Rewards for WooCommerce: from n/a through 1.5.0.	6.5	More Details
CVE-2024-27927	RSSHub is an open source RSS feed generator. Prior to version 1.0.0-master.a429472, RSSHub allows remote attackers to use the server as a proxy to send HTTP GET requests to arbitrary targets and retrieve information in the internal network or conduct Denial-of-Service (DoS) attacks. The attacker can send malicious requests to a RSSHub server, to make the server send HTTP GET requests to arbitrary destinations and see partial responses. This may lead to leak the server IP address, which could be hidden behind a CDN; retrieving information in the internal network, e.g. which addresses/ports are accessible, the titles and meta descriptions of HTML pages; and denial of service amplification. The attacker could request the server to download some large files, or chain several SSRF requests in a single attacker request.	6.5	More Details
CVE-2022-38057	Missing Authorization vulnerability in ThemeHunk Advance WordPress Search Plugin.This issue affects Advance WordPress Search Plugin: from n/a through 1.2.1.	6.5	More Details
CVE-2024-2630	Inappropriate implementation in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2024-2626	Out of bounds read in Swiftshader in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1313	It is possible for a user in a different organization from the owner of a snapshot to bypass authorization and delete a snapshot by issuing a DELETE request to /api/snapshots/<key> using its view key. This functionality is intended to only be available to individuals with the permission to write/edit to the snapshot in question, but due to a bug in the authorization logic, deletion requests issued by an unprivileged user in a different organization than the snapshot owner are treated as authorized. Grafana Labs would like to thank Ravid Mazon and Jay Chen of Palo Alto Research for discovering and disclosing this vulnerability. This issue affects Grafana: from 9.5.0 before 9.5.18, from 10.0.0 before 10.0.13, from 10.1.0 before 10.1.9, from 10.2.0 before 10.2.6, from 10.3.0 before 10.3.5.	6.5	More Details
CVE-2024-2392	The Blocksy Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Newsletter widget in all versions up to, and including, 2.0.31 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.5	More Details
CVE-2024-2906	Missing Authorization vulnerability in SoftLab Radio Player.This issue affects Radio Player: from n/a through 2.0.73.	6.5	More Details
CVE-2023-52229	Missing Authorization vulnerability in Save as PDF plugin by Pdfcrowd Word Replacer Pro.This issue affects Word Replacer Pro: from n/a through 1.0.	6.5	More Details
CVE-2023-46841	Recent x86 CPUs offer functionality named Control-flow Enforcement Technology (CET). A sub-feature of this are Shadow Stacks (CET-SS). CET-SS is a hardware feature designed to protect against Return Oriented Programming attacks. When enabled, traditional stacks holding both data and return addresses are accompanied by so called "shadow stacks", holding little more than return addresses. Shadow stacks aren't writable by normal instructions, and upon function returns their contents are used to check for possible manipulation of a return address coming from the traditional stack. In particular certain memory accesses need intercepting by Xen. In various cases the necessary emulation involves kind of replaying of the instruction. Such replaying typically involves filling and then invoking of a stub. Such a replayed instruction may raise an exceptions, which is expected and dealt with accordingly. Unfortunately the interaction of both of the above wasn't right: Recovery involves removal of a call frame from the (traditional) stack. The counterpart of this operation for the shadow stack was missing.	6.5	More Details
CVE-2024-29272	Arbitrary File Upload vulnerability in VvvebJs before version 1.7.5, allows unauthenticated remote attackers to execute arbitrary code and obtain sensitive information via the sanitizeFileName parameter in save.php.	6.5	More Details
CVE-2024-22436	A security vulnerability in HPE IceWall Agent products could be exploited remotely to cause a denial of service.	6.5	More Details
CVE-2024-21865	HGW BL1500HM Ver 002.001.013 and earlier contains a use of week credentials issue. A network-adjacent unauthenticated attacker may connect to the product via SSH and use a shell.	6.5	More Details
CVE-2024-22083	An issue was discovered in Elspec G5 digital fault recorder versions 1.1.4.15 and before. A hardcoded backdoor session ID exists that can be used for further access to the device, including reconfiguration tasks.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25138	In AutomationDirect C-MORE EA9 HMI, credentials used by the platform are stored as plain text on the device.	6.5	More Details
CVE-2024-30233	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Wholesale Team WholesaleX.This issue affects WholesaleX: from n/a through 1.3.1.	6.5	More Details
CVE-2024-28863	node-tar is a Tar for Node.js. node-tar prior to version 6.2.1 has no limit on the number of sub-folders created in the folder creation process. An attacker who generates a large number of sub-folders can consume memory on the system running node-tar and even crash the Node.js client within few seconds of running it using a path with too many sub-folders inside. Version 6.2.1 fixes this issue by preventing extraction in excessively deep sub-folders.	6.5	More Details
CVE-2024-27094	OpenZeppelin Contracts is a library for secure smart contract development. The `Base64.encode` function encodes a `bytes` input by iterating over it in chunks of 3 bytes. When this input is not a multiple of 3, the last iteration may read parts of the memory that are beyond the input buffer. The vulnerability is fixed in 5.0.2 and 4.9.6.	6.5	More Details
CVE-2024-24110	SQL Injection vulnerability in crmeb_java before v1.3.4 allows attackers to run arbitrary SQL commands via crafted GET request to the component /api/front/spread/people.	6.5	More Details
CVE-2023-47430	Stack-buffer-overflow vulnerability in ReadyMedia (MiniDLNA) v1.3.3 allows attackers to cause a denial of service via via the SendContainer() function at tivo_commands.c.	6.5	More Details
CVE-2024-22352	IBM InfoSphere Information Server 11.7 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 280361.	6.5	More Details
CVE-2023-7251	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jeff Starr User Submitted Posts allows Stored XSS.This issue affects User Submitted Posts: from n/a through 20230901.	6.5	More Details
CVE-2023-49985	A cross-site scripting (XSS) vulnerability in the component /management/class of School Fees Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the cname parameter.	6.5	More Details
CVE-2024-28244	KaTeX is a JavaScript library for TeX math rendering on the web. KaTeX users who render untrusted mathematical expressions could encounter malicious input using `\def` or `\newcommand` that causes a near-infinite loop, despite setting `maxExpand` to avoid such loops. KaTeX supports an option named maxExpand which aims to prevent infinitely recursive macros from consuming all available memory and/or triggering a stack overflow error. Unfortunately, support for "Unicode (sub|super)script characters" allows an attacker to bypass this limit. Each sub/superscript group instantiated a separate Parser with its own limit on macro executions, without inheriting the current count of macro executions from its parent. This has been corrected in KaTeX v0.16.10.	6.5	More Details
CVE-2024-27963	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Crisp allows Stored XSS.This issue affects Crisp: from n/a through 0.44.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24799	Missing Authorization vulnerability in WooCommerce WooCommerce Box Office.This issue affects WooCommerce Box Office: from n/a through 1.2.2.	6.5	More Details
CVE-2024-25811	An access control issue in Dreamer CMS v4.0.1 allows attackers to download backup files and leak sensitive information.	6.5	More Details
CVE-2023-32237	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in CodexThemes TheGem (Elementor), CodexThemes TheGem (WPBakery) allows Stored XSS.This issue affects TheGem (Elementor): from n/a before 5.8.1.1; TheGem (WPBakery): from n/a before 5.8.1.1.	6.5	More Details
CVE-2024-2580	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FunnelKit Automation By Autonami allows Stored XSS.This issue affects Automation By Autonami: from n/a through 2.8.2.	6.5	More Details
CVE-2024-28243	KaTeX is a JavaScript library for TeX math rendering on the web. KaTeX users who render untrusted mathematical expressions could encounter malicious input using `\edef` that causes a near-infinite loop, despite setting `maxExpand` to avoid such loops. This can be used as an availability attack, where e.g. a client rendering another user's KaTeX input will be unable to use the site due to memory overflow, tying up the main thread, or stack overflow. Upgrade to KaTeX v0.16.10 to remove this vulnerability.	6.5	More Details
CVE-2023-51416	Cross-Site Request Forgery (CSRF) vulnerability in EnvialoSimple EnvíaloSimple.This issue affects EnvíaloSimple: from n/a through 2.2.	6.5	More Details
CVE-2024-30232	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Exclusive Addons Exclusive Addons Elementor allows Stored XSS.This issue affects Exclusive Addons Elementor: from n/a through 2.6.9.	6.5	More Details
CVE-2024-22156	Missing Authorization vulnerability in SNP Digital SalesKing.This issue affects SalesKing: from n/a through 1.6.15.	6.5	More Details
CVE-2024-1450	The Shariff Wrapper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'shariff' shortcode in all versions up to, and including, 4.6.10 due to insufficient input sanitization and output escaping on user supplied attributes such as 'align'. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1278	The Easy Social Feed – Social Photos Gallery – Post Feed – Like Box plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'efb_likebox' shortcode in all versions up to, and including, 6.5.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1326	The Jeg Elementor Kit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via HTML Tag attributes in all versions up to, and including, 2.6.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1049	The Page Builder Gutenberg Blocks – CoBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Icon Widget's in all versions up to, and including, 3.1.6 due to insufficient input sanitization and output escaping on the link value. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2474	The Standout Color Boxes and Buttons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'color-button' shortcode in all versions up to, and including, 0.7.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2124	The Translate WordPress and go Multilingual – Weglot plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widget/block in all versions up to, and including, 4.2.5 due to insufficient input sanitization and output escaping on user supplied attributes such as 'className'. 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-2024-2304	The Animated Headline plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'animated-headline' shortcode in all versions up to, and including, 4.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2129	The WPBITS Addons For Elementor Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's heading widget in all versions up to, and including, 1.3.4.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2170	The VK All in One Expansion Unit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the child page index widget in all versions up to, and including, 9.96.0.1 due to insufficient input sanitization and output escaping on user supplied attributes such as 'className.' This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2500	The ColorMag theme for WordPress is vulnerable to Stored Cross-Site Scripting via a user's Display Name in all versions up to, and including, 3.1.6 due to insufficient input sanitization and output escaping. This makes it possible for authentciated 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-2024-2255	The Essential Blocks – Page Builder Gutenberg Blocks, Patterns & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 4.5.2 due to insufficient input sanitization and output escaping on user supplied attributes such as listStyle. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2460	The GamiPress – Button plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'gamipress_button' shortcode in all versions up to, and including, 1.0.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2468	The EmbedPress – Embed PDF, Google Docs, Vimeo, Wistia, Embed YouTube Videos, Audios, Maps & Embed Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the EmbedPress widget 'embedpress_pro_twitch_theme ' attribute in all versions up to, and including, 3.9.12 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2202	The Page Builder by SiteOrigin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the legacy Image widget in all versions up to, and including, 2.29.6 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-2024-2131	The Move Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's infobox and button widget in all versions up to, and including, 1.2.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1787	The Contests by Rewards Fuel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'update_rewards_fuel_api_key' parameter in all versions up to, and including, 2.0.64 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-2024-1697	The Custom WooCommerce Checkout Fields Editor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the save_wcfe_options function in all versions up to, and including, 1.3.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber-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-2024-2303	The Easy Textillate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'textillate' shortcode in all versions up to, and including, 2.01 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2453	There is an SQL injection vulnerability in Advantech WebAccess/SCADA software that allows an authenticated attacker to remotely inject SQL code in the database. Successful exploitation of this vulnerability could allow an attacker to read or modify data on the remote database.	6.4	More Details
CVE-2023-6500	The Shariff Wrapper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'shariff' shortcode in all versions up to, and including, 4.6.9 due to insufficient input sanitization and output escaping on user supplied attributes such as 'secondarycolor' and 'maincolor'. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-0966	The Shariff Wrapper plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'shariff' shortcode in all versions up to, and including, 4.6.9 due to insufficient input sanitization and output escaping on user supplied attributes like 'info_text'. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page and clicks the information icon.	6.4	More Details
CVE-2024-2849	A vulnerability classified as critical was found in SourceCodester Simple File Manager 1.0. This vulnerability affects unknown code. The manipulation of the argument photo leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257770 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-2673	A vulnerability classified as critical has been found in Campcodes Online Job Finder System 1.0. This affects an unknown part of the file /admin/login.php. The manipulation of the argument user_email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257373 was assigned to this vulnerability.	6.3	More Details
CVE-2024-2672	A vulnerability was found in Campcodes Online Job Finder System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/user/controller.php. The manipulation of the argument UESRID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257372.	6.3	More Details
CVE-2020-36825	** UNSUPPORTED WHEN ASSIGNED ** ** DISPUTED ** A vulnerability has been found in cyberaz0r WebRAT up to 20191222 and classified as critical. This vulnerability affects the function download_file of the file Server/api.php. The manipulation of the argument name leads to unrestricted upload. The attack can be initiated remotely. The real existence of this vulnerability is still doubted at the moment. The patch is identified as 0c394a795b9c10c07085361e6fcea286ee793701. It is recommended to apply a patch to fix this issue. VDB-257782 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: The issue, discovered in a 20-stars GitHub project (now private) by its author, had CVE requested by a third party 4 years post-resolution, referencing the fix commit (now a broken link). Due to minimal attention and usage, it should not be eligible for CVE according to the project maintainer.	6.3	More Details
CVE-2024-2016	A vulnerability, which was classified as critical, was found in ZhiCms 4.0. Affected is the function index of the file app/manage/controller/setcontroller.php. The manipulation of the argument sitename leads to code injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-255270 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2668	A vulnerability has been found in Campcodes Online Job Finder System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/vacancy/controller.php. The manipulation of the argument id/CATEGORY leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257368.	6.3	More Details
CVE-2024-2854	A vulnerability classified as critical has been found in Tenda AC18 15.03.05.05. Affected is the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257778 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2824	A vulnerability was found in Matthias-Wandel jhead 3.08 and classified as critical. This issue affects the function PrintFormatNumber of the file exif.c. The manipulation leads to heap-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257711.	6.3	More Details
CVE-2024-2853	A vulnerability was found in Tenda AC10U 15.03.06.48/15.03.06.49. It has been rated as critical. This issue affects the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257777 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2015	A vulnerability, which was classified as critical, has been found in ZhiCms 4.0. This issue affects the function getindexdata of the file app/index/controller/mcontroller.php. The manipulation of the argument key leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-255269 was assigned to this vulnerability.	6.3	More Details
CVE-2024-2851	A vulnerability was found in Tenda AC15 15.03.05.18/15.03.20_multi. It has been classified as critical. This affects the function formSetSambaConf of the file /goform/setsambacfg. The manipulation of the argument usbName leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257775. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2669	A vulnerability was found in Campcodes Online Job Finder System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/employee/controller.php of the component GET Parameter Handler. The manipulation of the argument EMPLOYEEID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257369 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2828	A vulnerability, which was classified as critical, was found in lakernote EasyAdmin up to 20240315. Affected is the function thumbnail of the file src/main/java/com/laker/admin/module/sys/controller/IndexController.java. The manipulation of the argument url leads to server-side request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The patch is identified as 23165d8cb569048c531150f194fea39f8800b8d5. It is recommended to apply a patch to fix this issue. VDB-257718 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-2827	A vulnerability, which was classified as critical, has been found in lakernote EasyAdmin up to 20240315. This issue affects some unknown processing of the file /ureport/designer/saveReportFile. The manipulation leads to server-side request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257717 was assigned to this vulnerability.	6.3	More Details
CVE-2024-2910	A vulnerability, which was classified as critical, has been found in Ruijie RG-EG350 up to 20240318. Affected by this issue is the function vpnAction of the file /itbox_pi/vpn_quickset_service.php?a=set_vpn of the component HTTP POST Request Handler. The manipulation of the argument ip/port/user/pass/dns/startIp leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257978 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2826	A vulnerability classified as problematic was found in lakernote EasyAdmin up to 20240315. This vulnerability affects unknown code of the file /ureport/designer/saveReportFile. The manipulation leads to xml external entity reference. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257716.	6.3	More Details
CVE-2024-2825	A vulnerability classified as critical has been found in lakernote EasyAdmin up to 20240315. This affects an unknown part of the file /ureport/designer/saveReportFile. The manipulation of the argument file leads to path traversal: '../filedir'. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257715.	6.3	More Details
CVE-2024-2671	A vulnerability was found in Campcodes Online Job Finder System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/user/index.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257371.	6.3	More Details
CVE-2024-2670	A vulnerability was found in Campcodes Online Job Finder System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/vacancy/index.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. VDB-257370 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-2674	A vulnerability classified as critical was found in Campcodes Online Job Finder System 1.0. This vulnerability affects unknown code of the file /admin/employee/index.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257374 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2649	A vulnerability has been found in Netentsec NS-ASG Application Security Gateway 6.3 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /protocol/iscdevicestatus/deleteonlineuser.php. The manipulation of the argument messagecontent leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257287. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2767	A vulnerability was found in Campcodes Complete Online Beauty Parlor Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/forgot-password.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257603.	6.3	More Details
CVE-2024-2675	A vulnerability, which was classified as critical, has been found in Campcodes Online Job Finder System 1.0. This issue affects some unknown processing of the file /admin/company/index.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. The associated identifier of this vulnerability is VDB-257375.	6.3	More Details
CVE-2024-2678	A vulnerability was found in Campcodes Online Job Finder System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/applicants/controller.php. The manipulation of the argument JOBREGID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257378 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-2714	A vulnerability has been found in Campcodes Complete Online DJ Booking System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/booking-bwdates-reports-details.php. The manipulation of the argument fromdate leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257467.	6.3	More Details
CVE-2024-2707	A vulnerability has been found in Tenda AC10U 15.03.06.49 and classified as critical. This vulnerability affects the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257458 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2464	This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.This issue affects CDeX application versions through 5.7.1.	6.3	More Details
CVE-2024-2770	A vulnerability was found in Campcodes Complete Online Beauty Parlor Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/contact-us.php. The manipulation of the argument email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257606 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-44626	Missing Authorization vulnerability in Squirrly SEO Plugin by Squirrly SEO.This issue affects SEO Plugin by Squirrly SEO: from n/a through 12.1.20.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2774	A vulnerability classified as critical was found in Campcodes Online Marriage Registration System 1.0. This vulnerability affects unknown code of the file /user/search.php. The manipulation of the argument searchdata leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257608.	6.3	More Details
CVE-2024-2776	A vulnerability, which was classified as critical, was found in Campcodes Online Marriage Registration System 1.0. Affected is an unknown function of the file /admin/search.php. The manipulation of the argument searchdata leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257610 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-2777	A vulnerability has been found in Campcodes Online Marriage Registration System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/application-bwdates-reports-details.php. The manipulation of the argument fromdate leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257611.	6.3	More Details
CVE-2024-28245	KaTeX is a JavaScript library for TeX math rendering on the web. KaTeX users who render untrusted mathematical expressions could encounter malicious input using `\includegraphics` that runs arbitrary JavaScript, or generate invalid HTML. Upgrade to KaTeX v0.16.10 to remove this vulnerability.	6.3	More Details
CVE-2024-1908	An Improper Privilege Management vulnerability was identified in GitHub Enterprise Server that allowed an attacker to use the Enterprise Actions GitHub Connect download token to fetch private repository data. An attacker would require an account on the server instance with non-default settings for GitHub Connect. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.12 and was fixed in versions 3.8.16, 3.9.11, 3.10.8, and 3.11.6. This vulnerability was reported via the GitHub Bug Bounty program.	6.3	More Details
CVE-2024-2768	A vulnerability was found in Campcodes Complete Online Beauty Parlor Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/edit-services.php. The manipulation of the argument editid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257604.	6.3	More Details
CVE-2024-2690	A vulnerability was found in SourceCodester Online Discussion Forum Site 1.0. It has been classified as critical. Affected is an unknown function of the file /uupdate.php. The manipulation of the argument ima leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257388.	6.3	More Details
CVE-2024-2687	A vulnerability was found in Campcodes Online Job Finder System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/applicants/index.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. The associated identifier of this vulnerability is VDB-257387.	6.3	More Details
CVE-2024-2897	A vulnerability classified as critical has been found in Tenda AC7 15.03.06.44. Affected is the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257940. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2812	A vulnerability was found in Tenda AC15 15.03.05.18/15.03.20_multi. It has been classified as critical. This affects the function formWriteFacMac of the file /goform/WriteFacMac. The manipulation of the argument mac leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257667. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2712	A vulnerability, which was classified as critical, has been found in Campcodes Complete Online DJ Booking System 1.0. This issue affects some unknown processing of the file /admin/user-search.php. The manipulation of the argument searchdata leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257465 was assigned to this vulnerability.	6.3	More Details
CVE-2024-25168	SQL injection vulnerability in snow snow v.2.0.0 allows a remote attacker to execute arbitrary code via the dataScope parameter of the system/role/list interface.	6.3	More Details
CVE-2024-2676	A vulnerability, which was classified as critical, was found in Campcodes Online Job Finder System 1.0. Affected is an unknown function of the file /admin/company/controller.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257376.	6.3	More Details
CVE-2024-2677	A vulnerability has been found in Campcodes Online Job Finder System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/category/controller.php. The manipulation of the argument CATEGORYID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257377 was assigned to this vulnerability.	6.3	More Details
CVE-2024-2769	A vulnerability was found in Campcodes Complete Online Beauty Parlor Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/admin-profile.php. The manipulation of the argument adminname leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257605 was assigned to this vulnerability.	6.3	More Details
CVE-2024-2713	A vulnerability, which was classified as critical, was found in Campcodes Complete Online DJ Booking System 1.0. Affected is an unknown function of the file /admin/booking-search.php. The manipulation of the argument searchdata leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257466 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-2766	A vulnerability has been found in Campcodes Complete Online Beauty Parlor Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/index.php. 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. VDB-257602 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-28579	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the FreeImage_Unload() function when reading images in HDR format.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28568	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the read_iptc_profile() function when reading images in TIFF format.	6.2	More Details
CVE-2024-27277	The private key for the IBM Storage Protect Plus Server 10.1.0 through 10.1.16 certificate can be disclosed, undermining the security of the certificate. IBM X-Force ID: 285205.	6.2	More Details
CVE-2024-28575	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the opj_j2k_read_mct() function when reading images in J2K format.	6.2	More Details
CVE-2024-28574	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the opj_j2k_copy_default_tcp_and_create_tcd() function when reading images in J2K format.	6.2	More Details
CVE-2024-28573	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the jpeg_read_exif_profile() function when reading images in JPEG format.	6.2	More Details
CVE-2024-28572	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the FreeImage_SetTagValue() function when reading images in JPEG format.	6.2	More Details
CVE-2024-28567	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the FreeImage_CreateICCProfile() function when reading images in TIFF format.	6.2	More Details
CVE-2024-28564	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the Imf_2_2::CharPtrIO::readChars() function when reading images in EXR format.	6.2	More Details
CVE-2024-22085	An issue was discovered in Elspec G5 digital fault recorder versions 1.1.4.15 and before. The shadow file is world readable.	6.2	More Details
CVE-2024-2494	A flaw was found in the RPC library APIs of libvirt. The RPC server deserialization code allocates memory for arrays before the non-negative length check is performed by the C API entry points. Passing a negative length to the g_new0 function results in a crash due to the negative length being treated as a huge positive number. This flaw allows a local, unprivileged user to perform a denial of service attack by causing the libvirt daemon to crash.	6.2	More Details
CVE-2021-47147	In the Linux kernel, the following vulnerability has been resolved: ptp: ocp: Fix a resource leak in an error handling path If an error occurs after a successful 'pci_ioremap_bar()' call, it must be undone by a corresponding 'pci_iounmap()' call, as already done in the remove function.	6.2	More Details
CVE-2024-25175	An issue in Kickdler before v1.107.0 allows attackers to provide an XSS payload via a HTTP response splitting attack.	6.1	More Details
CVE-2024-29644	Cross Site Scripting vulnerability in dcat-admin v.2.1.3 and before allows a remote attacker to execute arbitrary code via a crafted script to the user login box.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28183	ESP-IDF is the development framework for Espressif SoCs supported on Windows, Linux and macOS. A Time-of-Check to Time-of-Use (TOCTOU) vulnerability was discovered in the implementation of the ESP-IDF bootloader which could allow an attacker with physical access to flash of the device to bypass anti-rollback protection. Anti-rollback prevents rollback to application with security version lower than one programmed in eFuse of chip. This attack can allow to boot past (passive) application partition having lower security version of the same device even in the presence of the flash encryption scheme. The attack requires carefully modifying the flash contents after the anti-rollback checks have been performed by the bootloader (before loading the application). The vulnerability is fixed in 4.4.7 and 5.2.1.	6.1	More Details
CVE-2024-26018	Cross-site scripting vulnerability exists in TvRock 0.9t8a. An arbitrary script may be executed on the web browser of the user accessing the website that uses the product. Note that the developer was unreachable, therefore, users should consider stop using TvRock 0.9t8a.	6.1	More Details
CVE-2024-29832	The current_url parameter of the AJAX call to the GalleryBox action of admin-ajax.php is vulnerable to reflected Cross Site Scripting. The value of the current_url parameter is embedded within an existing JavaScript within the response allowing arbitrary JavaScript to be inserted and executed. No authentication is required to exploit this issue. Note that other parameters within a AJAX call, such as image_id, must be valid for this vulnerability to be successfully exploited.	6.1	More Details
CVE-2024-29041	Express.js minimalist web framework for node. Versions of Express.js prior to 4.19.0 and all pre-release alpha and beta versions of 5.0 are affected by an open redirect vulnerability using malformed URLs. When a user of Express performs a redirect using a user-provided URL Express performs an encode [using `encodeurl`](https://github.com/pillarjs/encodeurl) on the contents before passing it to the `location` header. This can cause malformed URLs to be evaluated in unexpected ways by common redirect allow list implementations in Express applications, leading to an Open Redirect via bypass of a properly implemented allow list. The main method impacted is `res.location()` but this is also called from within `res.redirect()`. The vulnerability is fixed in 4.19.2 and 5.0.0-beta.3.	6.1	More Details
CVE-2024-29216	Exposed IOCTL with insufficient access control issue exists in cg6kwin2k.sys prior to 2.1.7.0. By sending a specific IOCTL request, a user without the administrator privilege may perform I/O to arbitrary hardware port or physical address, resulting in erasing or altering the firmware.	6.1	More Details
CVE-2024-28126	Cross-site scripting vulnerability exists in 0ch BBS Script ver.4.00. An arbitrary script may be executed on the web browser of the user accessing the website that uses the product. Note that the developer was unreachable, therefore, users should consider stop using 0ch BBS Script ver.4.00.	6.1	More Details
CVE-2024-29009	Cross-site request forgery (CSRF) vulnerability in easy-popup-show all versions allows a remote unauthenticated attacker to hijack the authentication of the administrator and to perform unintended operations if the administrator views a malicious page while logged in.	6.1	More Details
CVE-2024-2726	Stored Cross-Site Scripting (Stored-XSS) vulnerability affecting the CIGESv2 system, allowing an attacker to execute and store malicious javascript code in the application form without prior registration.	6.1	More Details
CVE-2024-2727	HTML injection vulnerability affecting the CIGESv2 system, which allows an attacker to inject arbitrary code and modify elements of the website and email confirmation message.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22258	Spring Authorization Server versions 1.0.0 - 1.0.5, 1.1.0 - 1.1.5, 1.2.0 - 1.2.2 and older unsupported versions are susceptible to a PKCE Downgrade Attack for Confidential Clients. Specifically, an application is vulnerable when a Confidential Client uses PKCE for the Authorization Code Grant. An application is not vulnerable when a Public Client uses PKCE for the Authorization Code Grant.	6.1	More Details
CVE-2024-29273	There is Stored Cross-Site Scripting (XSS) in dzzoffice 2.02.1 SC UTF8 in uploadfile to index.php, with the XSS payload in an SVG document.	6.1	More Details
CVE-2024-29271	Reflected Cross-Site Scripting (XSS) vulnerability in VvvebJs before version 1.7.7, allows remote attackers to execute arbitrary code and obtain sensitive information via the action parameter in save.php.	6.1	More Details
CVE-2024-25807	Cross Site Scripting (XSS) vulnerability in Lychee 3.1.6, allows remote attackers to execute arbitrary code and obtain sensitive information via the title parameter when creating an album.	6.1	More Details
CVE-2024-28635	Cross Site Scripting (XSS) vulnerability in SurveyJS Survey Creator v.1.9.132 and before, allows attackers to execute arbitrary code and obtain sensitive information via the title parameter in form.	6.1	More Details
CVE-2023-48903	Stored Cross-Site Scripting (XSS) vulnerability in tramyardg autoexpress 1.3.0, allows remote unauthenticated attackers to inject arbitrary web script or HTML within parameter "imgType" via in uploadCarImages.php.	6.1	More Details
CVE-2024-0337	The Travelpayouts: All Travel Brands in One Place WordPress plugin through 1.1.15 is vulnerable to Open Redirect due to insufficient validation on the travelpayouts_redirect variable. This makes it possible for unauthenticated attackers to redirect users to potentially malicious sites if they can successfully trick them into performing an action.	6.1	More Details
CVE-2024-29374	A Cross-Site Scripting (XSS) vulnerability exists in the way MOODLE 3.10.9 handles user input within the "GET /?lang=" URL parameter.	6.1	More Details
CVE-2023-49984	A cross-site scripting (XSS) vulnerability in the component /management/settings of School Fees Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the name parameter.	6.1	More Details
CVE-2024-29470	OneBlog v2.3.4 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the component {{rootpath}}/links.	6.1	More Details
CVE-2024-1379	The Website Article Monetization By MageNet plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'abp_auth_key' parameter in all versions up to, and including, 1.0.11 due to insufficient input sanitization and output escaping and a missing authorization check. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27926	RSSHub is an open source RSS feed generator. Starting in version 1.0.0-master.cbbd829 and prior to version 1.0.0-master.d8ca915, ahen the specially crafted image is supplied to the internal media proxy, it proxies the image without handling XSS vulnerabilities, allowing for the execution of arbitrary JavaScript code. Users who access the deliberately constructed URL are affected. This vulnerability was fixed in version 1.0.0-master.d8ca915. No known workarounds are available.	6.1	More Details
CVE-2024-27626	A Reflected Cross-Site Scripting (XSS) vulnerability has been identified in Dotclear version 2.29. The flaw exists within the Search functionality of the Admin Panel.	6.1	More Details
CVE-2024-27291	Docassemble is an expert system for guided interviews and document assembly. Prior to 1.4.97, it is possible to create a URL that acts as an open redirect. The vulnerability has been patched in version 1.4.97 of the master branch.	6.1	More Details
CVE-2024-2387	The Advanced Form Integration – Connect WooCommerce and Contact Form 7 to Google Sheets and other platforms plugin for WordPress is vulnerable to SQL Injection via the ‘integration_id’ parameter in all versions up to, and including, 1.82.0 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 and subsequently 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-2024-27290	Docassemble is an expert system for guided interviews and document assembly. Prior to 1.4.97, a user could type HTML into a field, including the field for the user's name, and then that HTML could be displayed on the screen as HTML. The vulnerability has been patched in version 1.4.97 of the master branch.	6.1	More Details
CVE-2024-25167	Cross Site Scripting vulnerability in eblog v1.0 allows a remote attacker to execute arbitrary code via a crafted script to the argument description parameter when submitting a comment on a post.	6.1	More Details
CVE-2024-29469	A stored cross-site scripting (XSS) vulnerability in OneBlog v2.3.4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Category List parameter under the Lab module.	6.1	More Details
CVE-2024-0957	The WooCommerce PDF Invoices, Packing Slips, Delivery Notes and Shipping Labels plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Customer Notes field in all versions up to, and including, 4.4.1 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 invoice for printing.	6.1	More Details
CVE-2024-29195	The azure-c-shared-utility is a C library for AMQP/MQTT communication to Azure Cloud Services. This library may be used by the Azure IoT C SDK for communication between IoT Hub and IoT Hub devices. An attacker can cause an integer wraparound or under-allocation or heap buffer overflow due to vulnerabilities in parameter checking mechanism, by exploiting the buffer length parameter in Azure C SDK, which may lead to remote code execution. Requirements for RCE are 1. Compromised Azure account allowing malformed payloads to be sent to the device via IoT Hub service, 2. By passing IoT hub service max message payload limit of 128KB, and 3. Ability to overwrite code space with remote code. Fixed in commit https://github.com/Azure/azure-c-shared-utility/commit/1129147c38ac02ad974c4c701a1e01b2141b9fe2.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47153	In the Linux kernel, the following vulnerability has been resolved: i2c: i801: Don't generate an interrupt on bus reset Now that the i2c-i801 driver supports interrupts, setting the KILL bit in a attempt to recover from a timed out transaction triggers an interrupt. Unfortunately, the interrupt handler (i801_isr) is not prepared for this situation and will try to process the interrupt as if it was signaling the end of a successful transaction. In the case of a block transaction, this can result in an out-of-range memory access. This condition was reproduced several times by syzbot: https://syzkaller.appspot.com/bug?extid=ed71512d469895b5b34e https://syzkaller.appspot.com/bug?extid=8c8dedc0ba9e03f6c79e https://syzkaller.appspot.com/bug?extid=c8ff0b6d6c73d81b610e https://syzkaller.appspot.com/bug?extid=33f6c360821c399d69eb https://syzkaller.appspot.com/bug?extid=be15dc0b1933f04b043a https://syzkaller.appspot.com/bug?extid=b4d3fd1dfd53e90afd79 So disable interrupts while trying to reset the bus. Interrupts will be enabled again for the following transaction.	6.0	More Details
CVE-2024-23634	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. An arbitrary file renaming vulnerability exists in versions prior to 2.23.5 and 2.24.2 that enables an authenticated administrator with permissions to modify stores through the REST Coverage Store or Data Store API to rename arbitrary files and directories with a name that does not end in `.zip`. Store file uploads rename zip files to have a `.zip` extension if it doesn't already have one before unzipping the file. This is fine for file and url upload methods where the files will be in a specific subdirectory of the data directory but, when using the external upload method, this allows arbitrary files and directories to be renamed. Renaming GeoServer files will most likely result in a denial of service, either completely preventing GeoServer from running or effectively deleting specific resources (such as a workspace, layer or style). In some cases, renaming GeoServer files could revert to the default settings for that file which could be relatively harmless like removing contact information or have more serious consequences like allowing users to make OGC requests that the customized settings would have prevented them from making. The impact of renaming non-GeoServer files depends on the specific environment although some sort of denial of service is a likely outcome. Versions 2.23.5 and 2.24.2 contain a fix for this issue.	6.0	More Details
CVE-2023-25965	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in mbbhatti Upload Resume.This issue affects Upload Resume: from n/a through 1.2.0.	5.9	More Details
CVE-2023-35888	IBM Security Verify Governance 10.0.2 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 258375.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29018	Moby is an open source container framework that is a key component of Docker Engine, Docker Desktop, and other distributions of container tooling or runtimes. Moby's networking implementation allows for many networks, each with their own IP address range and gateway, to be defined. This feature is frequently referred to as custom networks, as each network can have a different driver, set of parameters and thus behaviors. When creating a network, the `--internal` flag is used to designate a network as _internal_. The `internal` attribute in a docker-compose.yml file may also be used to mark a network _internal_, and other API clients may specify the `internal` parameter as well. When containers with networking are created, they are assigned unique network interfaces and IP addresses. The host serves as a router for non-internal networks, with a gateway IP that provides SNAT/DNAT to/from container IPs. Containers on an internal network may communicate between each other, but are precluded from communicating with any networks the host has access to (LAN or WAN) as no default route is configured, and firewall rules are set up to drop all outgoing traffic. Communication with the gateway IP address (and thus appropriately configured host services) is possible, and the host may communicate with any container IP directly. In addition to configuring the Linux kernel's various networking features to enable container networking, `dockerd` directly provides some services to container networks. Principal among these is serving as a resolver, enabling service discovery, and resolution of names from an upstream resolver. When a DNS request for a name that does not correspond to a container is received, the request is forwarded to the configured upstream resolver. This request is made from the container's network namespace: the level of access and routing of traffic is the same as if the request was made by the container itself. As a consequence of this design, containers solely attached to an internal network will be unable to resolve names using the upstream resolver, as the container itself is unable to communicate with that nameserver. Only the names of containers also attached to the internal network are able to be resolved. Many systems run a local forwarding DNS resolver. As the host and any containers have separate loopback devices, a consequence of the design described above is that containers are unable to resolve names from the host's configured resolver, as they cannot reach these addresses on the host loopback device. To bridge this gap, and to allow containers to properly resolve names even when a local forwarding resolver is used on a loopback address, `dockerd` detects this scenario and instead forward DNS requests from the host namework namespace. The loopback resolver then forwards the requests to its configured upstream resolvers, as expected. Because `dockerd` forwards DNS requests to the host loopback device, bypassing the container network namespace's normal routing semantics entirely, internal networks can unexpectedly forward DNS requests to an external nameserver. By registering a domain for which they control the authoritative nameservers, an attacker could arrange for a compromised container to exfiltrate data by encoding it in DNS queries that will eventually be answered by their nameservers. Docker Desktop is not affected, as Docker Desktop always runs an internal resolver on a RFC 1918 address. Moby releases 26.0.0, 25.0.4, and 23.0.11 are patched to prevent forwarding any DNS requests from internal networks. As a workaround, run containers intended to be solely attached to internal networks with a custom upstream address, which will force all upstream DNS queries to be resolved from the container's network namespace.	5.9	More Details
CVE-2024-28756	The SolarEdge mySolarEdge application before 2.20.1 for Android has a certificate verification issue that allows a Machine-in-the-middle (MitM) attacker to read and alter all network traffic between the application and the server.	5.9	More Details
CVE-2024-2579	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Data443 Tracking Code Manager.This issue affects Tracking Code Manager: from n/a through 2.0.16.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28563	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the Imf_2_2::DwaCompressor::Classifier::Classifier() function when reading images in EXR format.	5.9	More Details
CVE-2024-2578	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPCoder WP Coder allows Stored XSS.This issue affects WP Coder: from n/a through 3.5.	5.9	More Details
CVE-2024-24028	Server Side Request Forgery (SSRF) vulnerability in Likeshop before 2.5.7 allows attackers to view sensitive information via the avatar parameter in function UserLogic::updateWechatInfo.	5.9	More Details
CVE-2024-24818	EspoCRM is an Open Source Customer Relationship Management software. An attacker can inject arbitrary IP or domain in "Password Change" page and redirect victim to malicious page that could lead to credential stealing or another attack. This vulnerability is fixed in 8.1.2.	5.9	More Details
CVE-2024-27965	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPFunnels Team WPFunnels allows Stored XSS.This issue affects WPFunnels: from n/a through 3.0.6.	5.9	More Details
CVE-2024-2889	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Lab WP-Lister Lite for Amazon allows Stored XSS.This issue affects WP-Lister Lite for Amazon: from n/a through 2.6.11.	5.9	More Details
CVE-2024-27995	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Repute Infosystems ARMember – Membership Plugin, Content Restriction, Member Levels, User Profile & User signup allows Stored XSS.This issue affects ARMember – Membership Plugin, Content Restriction, Member Levels, User Profile & User signup: from n/a through 4.0.23.	5.9	More Details
CVE-2024-29916	The dormakaba Saflok system before the November 2023 software update allows an attacker to unlock arbitrary doors at a property via forged keycards, if the attacker has obtained one active or expired keycard for the specific property, aka the "Unsaflok" issue. This occurs, in part, because the key derivation function relies only on a UID. This affects, for example, Saflok MT, and the Confidant, Quantum, RT, and Saffire series.	5.6	More Details
CVE-2021-47158	In the Linux kernel, the following vulnerability has been resolved: net: dsa: sja1105: add error handling in sja1105_setup() If any of sja1105_static_config_load(), sja1105_clocking_setup() or sja1105_devlink_setup() fails, we can't just return in the middle of sja1105_setup() or memory will leak. Add a cleanup path.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47146	In the Linux kernel, the following vulnerability has been resolved: mld: fix panic in mld_newpack() mld_newpack() doesn't allow to allocate high order page, only order-0 allocation is allowed. If headroom size is too large, a kernel panic could occur in skb_put(). Test commands: ip netns del A ip netns del B ip netns add A ip netns add B ip link add veth0 type veth peer name veth1 ip link set veth0 netns A ip link set veth1 netns B ip netns exec A ip link set lo up ip netns exec A ip link set veth0 up ip netns exec A ip -6 a a 2001:db8:0::1/64 dev veth0 ip netns exec B ip link set lo up ip netns exec B ip link set veth1 up ip netns exec B ip -6 a a 2001:db8:0::2/64 dev veth1 for i in {1..99} do let A=$i-1 ip netns exec A ip link add ip6gre$i type ip6gre \ local 2001:db8:$A::1 remote 2001:db8:$A::2 encaplimit 100 ip netns exec A ip -6 a a 2001:db8:$i::1/64 dev ip6gre$i ip netns exec A ip link set ip6gre$i up ip netns exec B ip link add ip6gre$i type ip6gre \ local 2001:db8:$A::2 remote 2001:db8:$A::1 encaplimit 100 ip netns exec B ip -6 a a 2001:db8:$i::2/64 dev ip6gre$i ip netns exec B ip link set ip6gre$i up done Splat looks like: kernel BUG at net/core/skbuff.c:110! invalid opcode: 0000 [#1] SMP DEBUG_PAGEALLOC KASAN PTI CPU: 0 PID: 7 Comm: kworker/0:1 Not tainted 5.12.0+ #891 Workqueue: ipv6_addrconf addrconf_dad_work RIP: 0010:skb_panic+0x15d/0x15f Code: 92 fe 4c 8b 4c 24 10 53 8b 4d 70 45 89 e0 48 c7 c7 00 ae 79 83 41 57 41 56 41 55 48 8b 54 24 a6 26 f9 ff <0f> 0b 48 8b 6c 24 20 89 34 24 e8 4a 4e 92 fe 8b 34 24 48 c7 c1 20 RSP: 0018:ffff88810091f820 EFLAGS: 00010282 RAX: 0000000000000089 RBX: ffff8881086e9000 RCX: 0000000000000000 RDX: 0000000000000089 RSI: 0000000000000008 RDI: ffffed1020123efb RBP: ffff888005f6eac0 R08: ffffed1022fc0031 R09: ffffed1022fc0031 R10: ffff888117e00187 R11: ffffed1022fc0030 R12: 0000000000000028 R13: ffff888008284eb0 R14: 0000000000000ed8 R15: 0000000000000ec0 FS: 0000000000000000(0000) GS:ffff888117c00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f8b801c5640 CR3: 0000000033c2c006 CR4: 00000000003706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: ? ip6_mc_hdr.isra.26.constprop.46+0x12a/0x600 ? ip6_mc_hdr.isra.26.constprop.46+0x12a/0x600 skb_put.cold.104+0x22/0x22 ip6_mc_hdr.isra.26.constprop.46+0x12a/0x600 ? rcu_read_lock_sched_held+0x91/0xc0 mld_newpack+0x398/0x8f0 ? ip6_mc_hdr.isra.26.constprop.46+0x600/0x600 ? lock_contended+0xc40/0xc40 add_grhead.isra.33+0x280/0x380 add_grec+0x5ca/0xff0 ? mld_sendpack+0xf40/0xf40 ? lock_downgrade+0x690/0x690 mld_send_initial_cr.part.34+0xb9/0x180 ipv6_mc_dad_complete+0x15d/0x1b0 addrconf_dad_completed+0x8d2/0xbb0 ? lock_downgrade+0x690/0x690 ? addrconf_rs_timer+0x660/0x660 ? addrconf_dad_work+0x73c/0x10e0 addrconf_dad_work+0x73c/0x10e0 Allowing high order page allocation could fix this problem.	5.5	More Details
CVE-2021-47149	In the Linux kernel, the following vulnerability has been resolved: net: fujitsu: fix potential null-ptr-deref In fmvj18x_get_hwinfo(), if ioremap fails there will be NULL pointer deref. To fix this, check the return value of ioremap and return -1 to the caller in case of failure.	5.5	More Details
CVE-2021-47150	In the Linux kernel, the following vulnerability has been resolved: net: fec: fix the potential memory leak in fec_enet_init() If the memory allocated for cbd_base is failed, it should free the memory allocated for the queues, otherwise it causes memory leak. And if the memory allocated for the queues is failed, it can return error directly.	5.5	More Details
CVE-2021-47151	In the Linux kernel, the following vulnerability has been resolved: interconnect: qcom: bcm-voter: add a missing of_node_put() Add a missing of_node_put() in of_bcm_voter_get() to avoid the reference leak.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52627	In the Linux kernel, the following vulnerability has been resolved: iio: adc: ad7091r: Allow users to configure device events AD7091R-5 devices are supported by the ad7091r-5 driver together with the ad7091r-base driver. Those drivers declared iio events for notifying user space when ADC readings fall bellow the thresholds of low limit registers or above the values set in high limit registers. However, to configure iio events and their thresholds, a set of callback functions must be implemented and those were not present until now. The consequence of trying to configure ad7091r-5 events without the proper callback functions was a null pointer dereference in the kernel because the pointers to the callback functions were not set. Implement event configuration callbacks allowing users to read/write event thresholds and enable/disable event generation. Since the event spec structs are generic to AD7091R devices, also move those from the ad7091r-5 driver the base driver so they can be reused when support for ad7091r-2/-4/-8 be added.	5.5	More Details
CVE-2022-4963	A vulnerability was found in Folio Spring Module Core up to 1.1.5. It has been rated as critical. Affected by this issue is the function dropSchema of the file tenant/src/main/java/org/folio/spring/tenant/hibernate/HibernateSchemaService.java of the component Schema Name Handler. The manipulation leads to sql injection. Upgrading to version 2.0.0 is able to address this issue. The name of the patch is d374a5f77e6b58e36f0e0e4419be18b95edcd7ff. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-257516.	5.5	More Details
CVE-2021-47144	In the Linux kernel, the following vulnerability has been resolved: drm/amd/amdgpu: fix refcount leak [Why] the gem object rfb->base.obj[0] is get according to num_planes in amdgpufb_create, but is not put according to num_planes [How] put rfb->base.obj[0] in amdgpu_fbdev_destroy according to num_planes	5.5	More Details
CVE-2024-28246	KaTeX is a JavaScript library for TeX math rendering on the web. Code that uses KaTeX's `trust` option, specifically that provides a function to blacklist certain URL protocols, can be fooled by URLs in malicious inputs that use uppercase characters in the protocol. In particular, this can allow for malicious input to generate `javascript:` links in the output, even if the `trust` function tries to forbid this protocol via `trust: (context) => context.protocol !== 'javascript'`. Upgrade to KaTeX v0.16.10 to remove this vulnerability.	5.5	More Details
	In the Linux kernel, the following vulnerability has been resolved: SUNRPC: Fix a suspicious RCU usage warning I received the following warning while running cthon against an ontap server running pNFS: [57.202521] ============================= [57.202522] WARNING: suspicious RCU usage [57.202523] 6.7.0-rc3-g2cc14f52aeb7 #41492 Not tainted [57.202525] ----------------------------- [57.202525] net/sunrpc/xprtmultipath.c:349 RCU-list traversed in non-reader section!! [57.202527] other info that might help us debug this: [57.202528] rcu_scheduler_active = 2, debug_locks = 1 [57.202529] no locks held by test5/3567. [57.202530] stack backtrace: [57.202532] CPU: 0 PID: 3567 Comm: test5 Not tainted 6.7.0-rc3-g2cc14f52aeb7 #41492 5b09971b4965c0aceba19f3eea324a4a806e227e [57.202534] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS unknown 2/2/2022 [57.202536] Call Trace: [57.202537] <TASK> [57.202540] dump_stack_lvl+0x77/0xb0 [57.202551] lockdep_rcu_suspicious+0x154/0x1a0 [57.202556] rpc_xprt_switch_has_addr+0x17c/0x190 [sunrpc ebe02571b9a8ceebf7d98e71675af20c19bdb1f6] [57.202596] rpc_clnt_setup_test_and_add_xprt+0x50/0x180 [sunrpc ebe02571b9a8ceebf7d98e71675af20c19bdb1f6] [57.202621] ? rpc_clnt_add_xprt+0x254/0x300 [sunrpc ebe02571b9a8ceebf7d98e71675af20c19bdb1f6] [57.202646] rpc_clnt_add_xprt+0x27a/0x300 [sunrpc ebe02571b9a8ceebf7d98e71675af20c19bdb1f6] [57.202671] ?		

CVE Number	Description	Base Score	Reference
CVE-2023-52623	__pfx_rpc_clnt_setup_test_and_add_xprt+0x10/0x10 [sunrpc ebe02571b9a8ceebf7d98e71675af20c1[illegible]57.202696] nfs4_pnfs_ds_connect+0x345/0x760 [nfsv4 c716d88496ded0ea6d289bbea684fa996f9b57a9] [57.202728] ? __pfx_nfs4_test_session_trunk+0x10/0x10 [nfsv4 c716d88496ded0ea6d289bbea684fa996f9b57a9] [57.202754] nfs4_fl_prepare_ds+0x75/0xc0 [nfs_layout_nfsv41_files e3a4187f18ae8a27b630f9feae6831b584a9360a] [57.202760] filelayout_write_pagelist+0x4a/0x200 [nfs_layout_nfsv41_files e3a4187f18ae8a27b630f9feae6831b584a9360a] [57.202765] pnfs_generic_pg_writepages+0xbe/0x230 [nfsv4 c716d88496ded0ea6d289bbea684fa996f9b57a9] [57.202788] __nfs_pageio_add_request+0x3fd/0x520 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [57.202813] nfs_pageio_add_request+0x18b/0x390 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [57.202831] nfs_do_writepage+0x116/0x1e0 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [57.202849] nfs_writepages_callback+0x13/0x30 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [57.202866] write_cache_pages+0x265/0x450 [57.202870] ? __pfx_nfs_writepages_callback+0x10/0x10 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [57.202891] nfs_writepages+0x141/0x230 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [57.202913] do_writepages+0xd2/0x230 [57.202917] ? filemap_fdatawrite_wbc+0x5c/0x80 [57.202921] filemap_fdatawrite_wbc+0x67/0x80 [57.202924] filemap_write_and_wait_range+0xd9/0x170 [57.202930] nfs_wb_all+0x49/0x180 [nfs 6c976fa593a7c2976f5a0aeb4965514a828e6902] [57.202947] nfs4_file_flush+0x72/0xb0 [nfsv4 c716d88496ded0ea6d289bbea684fa996f9b57a9] [57.202969] __se_sys_close+0x46/0xd0 [57.202972] do_syscall_64+0x68/0x100 [57.202975] ? do_syscall_64+0x77/0x100 [57.202976] ? do_syscall_64+0x77/0x100 [57.202979] entry_SYSCALL_64_after_hwframe+0x6e/0x76 [57.202982] RIP: 0033:0x7fe2b12e4a94 [57.202985] Code: 00 f7 d8 64 89 01 48 83 c8 ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 80 3d d5 18 0e 00 00 74 13 b8 03 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 44 c3 0f 1f 00 48 83 ec 18 89 7c 24 0c e8 c3 [57.202987] RSP: 002b:00007ffe857ddb38 EFLAGS: 00000202 ORIG_RAX: 0000000000000003 [57.202989] RAX: ffffffffffffffda RBX: 00007ffe857dfd68 RCX: 00007fe2b12e4a94 [57.202991] RDX: 0000000000002000 RSI: 00007ffe857ddc40 RDI: 0000000000000003 [57.202992] RBP: 00007ffe857dfc50 R08: 7fffffffffffffff R09: 0000000065650f49 [57.202993] R10: 00007f ---truncated---	5.5	More Details
CVE-2024-30203	In Emacs before 29.3, Gnus treats inline MIME contents as trusted.	5.5	More Details
CVE-2021-47161	In the Linux kernel, the following vulnerability has been resolved: spi: spi-fsl-dspi: Fix a resource leak in an error handling path 'dspi_request_dma()' should be undone by a 'dspi_release_dma()' call in the error handling path of the probe function, as already done in the remove function	5.5	More Details
CVE-2024-27300	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. The `email` field in phpMyFAQ's user control panel page is vulnerable to stored XSS attacks due to the inadequacy of PHP's `FILTER_VALIDATE_EMAIL` function, which only validates the email format, not its content. This vulnerability enables an attacker to execute arbitrary client-side JavaScript within the context of another user's phpMyFAQ session. This vulnerability is fixed in 3.2.6.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47164	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix null deref accessing lag dev It could be the lag dev is null so stop processing the event. In bond_enslave() the active/backup slave being set before setting the upper dev so first event is without an upper dev. After setting the upper dev with bond_master_upper_dev_link() there is a second event and in that event we have an upper dev.	5.5	More Details
CVE-2021-47171	In the Linux kernel, the following vulnerability has been resolved: net: usb: fix memory leak in smsc75xx_bind Syzbot reported memory leak in smsc75xx_bind(). The problem was is non-freed memory in case of errors after memory allocation. backtrace: [<ffffffff84245b62>] kmalloc include/linux/slab.h:556 [inline] [<ffffffff84245b62>] kzalloc include/linux/slab.h:686 [inline] [<ffffffff84245b62>] smsc75xx_bind+0x7a/0x334 drivers/net/usb/smsc75xx.c:1460 [<ffffffff82b5b2e6>] usbnet_probe+0x3b6/0xc30 drivers/net/usb/usbnet.c:1728	5.5	More Details
CVE-2021-47172	In the Linux kernel, the following vulnerability has been resolved: iio: adc: ad7124: Fix potential overflow due to non sequential channel numbers Channel numbering must start at 0 and then not have any holes, or it is possible to overflow the available storage. Note this bug was introduced as part of a fix to ensure we didn't rely on the ordering of child nodes. So we need to support arbitrary ordering but they all need to be there somewhere. Note I hit this when using qemu to test the rest of this series. Arguably this isn't the best fix, but it is probably the most minimal option for backporting etc. Alexandru's sign-off is here because he carried this patch in a larger set that Jonathan then applied.	5.5	More Details
CVE-2021-47179	In the Linux kernel, the following vulnerability has been resolved: NFSv4: Fix a NULL pointer dereference in pnfs_mark_matching_lsegs_return() Commit de144ff4234f changes _pnfs_return_layout() to call pnfs_mark_matching_lsegs_return() passing NULL as the struct pnfs_layout_range argument. Unfortunately, pnfs_mark_matching_lsegs_return() doesn't check if we have a value here before dereferencing it, causing an oops. I'm able to hit this crash consistently when running connectathon basic tests on NFS v4.1/v4.2 against Ontap.	5.5	More Details
CVE-2024-25956	Dell Grab for Windows, versions 5.0.4 and below, contains an improper file permissions vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to the information disclosure of certain system information.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47145	In the Linux kernel, the following vulnerability has been resolved: btrfs: do not BUG_ON in link_to_fixup_dir While doing error injection testing I got the following panic kernel BUG at fs/btrfs/tree-log.c:1862! invalid opcode: 0000 [#1] SMP NOPTI CPU: 1 PID: 7836 Comm: mount Not tainted 5.13.0-rc1+ #305 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.13.0-2.fc32 04/01/2014 RIP: 0010:link_to_fixup_dir+0xd5/0xe0 RSP: 0018:ffffb5800180fa30 EFLAGS: 00010216 RAX: fffffffffffffffb RBX: 00000000ffffffb RCX: ffff8f595287faf0 RDX: ffffb5800180fa37 RSI: ffff8f5954978800 RDI: 0000000000000000 RBP: ffff8f5953af9450 R08: 0000000000000019 R09: 0000000000000001 R10: 000151f408682970 R11: 0000000120021001 R12: ffff8f5954978800 R13: ffff8f595287faf0 R14: ffff8f5953c77dd0 R15: 0000000000000065 FS: 00007fc5284c8c40(0000) GS:ffff8f59bbd00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fc5287f47c0 CR3: 000000011275e002 CR4: 0000000000370ee0 Call Trace: replay_one_buffer+0x409/0x470 ? btree_read_extent_buffer_pages+0xd0/0x110 walk_up_log_tree+0x157/0x1e0 walk_log_tree+0xa6/0x1d0 btrfs_recover_log_trees+0x1da/0x360 ? replay_one_extent+0x7b0/0x7b0 open_ctree+0x1486/0x1720 btrfs_mount_root.cold+0x12/0xea ? __kmalloc_track_caller+0x12f/0x240 legacy_get_tree+0x24/0x40 vfs_get_tree+0x22/0xb0 vfs_kern_mount.part.0+0x71/0xb0 btrfs_mount+0x10d/0x380 ? vfs_parse_fs_string+0x4d/0x90 legacy_get_tree+0x24/0x40 vfs_get_tree+0x22/0xb0 path_mount+0x433/0xa10 __x64_sys_mount+0xe3/0x120 do_syscall_64+0x3d/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae We can get -EIO or any number of legitimate errors from btrfs_search_slot(), panicing here is not the appropriate response. The error path for this code handles errors properly, simply return the error.	5.5	More Details
CVE-2021-47173	In the Linux kernel, the following vulnerability has been resolved: misc/uss720: fix memory leak in uss720_probe uss720_probe forgets to decrease the refcount of usbdev in uss720_probe. Fix this by decreasing the refcount of usbdev by usb_put_dev. BUG: memory leak unreferenced object 0xffff888101113800 (size 2048): comm "kworker/0:1", pid 7, jiffies 4294956777 (age 28.870s) hex dump (first 32 bytes): ff ff ff ff 31 00 00 00 00 00 00 00 00 00 00 00 ....1..... 00 00 00 00 00 00 00 00 00 00 00 00 03 00 00 00 ..... backtrace: [<ffffffff82b8e822>] kmalloc include/linux/slab.h:554 [inline] [<ffffffff82b8e822>] kzalloc include/linux/slab.h:684 [inline] [<ffffffff82b8e822>] usb_alloc_dev+0x32/0x450 drivers/usb/core/usb.c:582 [<ffffffff82b98441>] hub_port_connect drivers/usb/core/hub.c:5129 [inline] [<ffffffff82b98441>] hub_port_connect_change drivers/usb/core/hub.c:5363 [inline] [<ffffffff82b98441>] port_event drivers/usb/core/hub.c:5509 [inline] [<ffffffff82b98441>] hub_event+0x1171/0x20c0 drivers/usb/core/hub.c:5591 [<ffffffff81259229>] process_one_work+0x2c9/0x600 kernel/workqueue.c:2275 [<ffffffff81259b19>] worker_thread+0x59/0x5d0 kernel/workqueue.c:2421 [<ffffffff81261228>] kthread+0x178/0x1b0 kernel/kthread.c:292 [<ffffffff8100227f>] ret_from_fork+0x1f/0x30 arch/x86/entry/entry_64.S:294	5.5	More Details
CVE-2024-26648	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix variable deferencing before NULL check in edp_setup_replay() In edp_setup_replay(), 'struct dc *dc' & 'struct dmub_replay *replay' was dereferenced before the pointer 'link' & 'replay' NULL check. Fixes the below: drivers/gpu/drm/amd/amdgpu/../display/dc/link/protocols/link_edp_panel_control.c:947 edp_setup_replay() warn: variable dereferenced before check 'link' (see line 933)	5.5	More Details
CVE-2024-28571	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the fill_input_buffer() function when reading images in JPEG format.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47141	In the Linux kernel, the following vulnerability has been resolved: gve: Add NULL pointer checks when freeing irqs. When freeing notification blocks, we index priv->msix_vectors. If we failed to allocate priv->msix_vectors (see abort_with_msix_vectors) this could lead to a NULL pointer dereference if the driver is unloaded.	5.5	More Details
CVE-2024-28577	Null Pointer Dereference vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the jpeg_read_exif_profile_raw() function when reading images in JPEG format.	5.5	More Details
CVE-2024-28565	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the psdParser::ReadImageData() function when reading images in PSD format.	5.5	More Details
CVE-2024-28576	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the opj_j2k_tcp_destroy() function when reading images in J2K format.	5.5	More Details
CVE-2021-47142	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix a use-after-free looks like we forget to set ttm->sg to NULL. Hit panic below [1235.844104] general protection fault, probably for non-canonical address 0x6b6b6b6b6b6b7b4b: 0000 [#1] SMP DEBUG_PAGEALLOC NOPTI [1235.989074] Call Trace: [1235.991751] sg_free_table+0x17/0x20 [1235.995667] amdgpu_ttm_backend_unbind.cold+0x4d/0xf7 [amdgpu] [1236.002288] amdgpu_ttm_backend_destroy+0x29/0x130 [amdgpu] [1236.008464] ttm_tt_destroy+0x1e/0x30 [ttm] [1236.013066] ttm_bo_cleanup_memtype_use+0x51/0xa0 [ttm] [1236.018783] ttm_bo_release+0x262/0xa50 [ttm] [1236.023547] ttm_bo_put+0x82/0xd0 [ttm] [1236.027766] amdgpu_bo_unref+0x26/0x50 [amdgpu] [1236.032809] amdgpu_amdkfd_gpuvm_alloc_memory_of_gpu+0x7aa/0xd90 [amdgpu] [1236.040400] kfd_ioctl_alloc_memory_of_gpu+0xe2/0x330 [amdgpu] [1236.046912] kfd_ioctl+0x463/0x690 [amdgpu]	5.5	More Details
CVE-2024-28570	Buffer Overflow vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the processMakerNote() function when reading images in JPEG format.	5.5	More Details
CVE-2022-45351	Missing Authorization vulnerability in Muffingroup Betheme.This issue affects Betheme: from n/a through 26.6.1.	5.4	More Details
CVE-2022-45352	Missing Authorization vulnerability in Muffingroup Betheme.This issue affects Betheme: from n/a through 26.6.1.	5.4	More Details
CVE-2022-45356	Missing Authorization vulnerability in Muffingroup Betheme.This issue affects Betheme: from n/a through 26.6.1.	5.4	More Details
CVE-2022-45851	Missing Authorization vulnerability in ShareThis ShareThis Dashboard for Google Analytics.This issue affects ShareThis Dashboard for Google Analytics: from n/a through 3.1.4.	5.4	More Details
CVE-2023-22699	Missing Authorization vulnerability in MainWP MainWP Wordfence Extension.This issue affects MainWP Wordfence Extension: from n/a through 4.0.7.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37886	Missing Authorization vulnerability in InspiryThemes RealHomes.This issue affects RealHomes: from n/a through 4.0.2.	5.4	More Details
CVE-2024-28435	The CRM platform Twenty version 0.3.0 is vulnerable to SSRF via file upload.	5.4	More Details
CVE-2024-2538	The Permalink Manager Lite plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ajax_save_permalink' function in all versions up to, and including, 2.4.3.1. This makes it possible for authenticated attackers, with author access and above, to modify the permalinks of arbitrary posts.	5.4	More Details
CVE-2024-29471	OneBlog v2.3.4 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Notice Manage module.	5.4	More Details
CVE-2024-29809	The image_url parameter of the AJAX call to the editimage_bwg action of admin-ajax.php is vulnerable to reflected Cross Site Scripting. The value of the image_url parameter is embedded within an existing JavaScript within the response allowing arbitrary JavaScript to be inserted and executed. The attacker must target a an authenticated user with permissions to access this component to exploit this issue.	5.4	More Details
CVE-2024-29472	OneBlog v2.3.4 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Privilege Management module.	5.4	More Details
CVE-2024-29474	OneBlog v2.3.4 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the User Management module.	5.4	More Details
CVE-2024-29133	Out-of-bounds Write vulnerability in Apache Commons Configuration.This issue affects Apache Commons Configuration: from 2.0 before 2.10.1. Users are recommended to upgrade to version 2.10.1, which fixes the issue.	5.4	More Details
CVE-2024-2732	The Themify Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'themify_post_slider shortcode in all versions up to, and including, 2.0.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2023-7246	The System Dashboard WordPress plugin before 2.8.10 does not sanitize and escape some parameters, which could allow administrators in multisite WordPress configurations to perform Cross-Site Scripting attacks	5.4	More Details
CVE-2024-1142	Path Traversal in Sonatype IQ Server from version 143 allows remote authenticated attackers to overwrite or delete files via a specially crafted request. Version 171 fixes this issue.	5.4	More Details
CVE-2024-1785	The Contests by Rewards Fuel plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.62. This is due to missing or incorrect nonce validation on the ajax_handler() function. This makes it possible for unauthenticated attackers to update the plugin's settings and inject malicious JavaScript via a forged request granted they can trick a site's user with the edit_posts capability into performing an action such as clicking on a link.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2917	A vulnerability was found in Campcodes House Rental Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file index.php. The manipulation of the argument page leads to file inclusion. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257983.	5.4	More Details
CVE-2024-2688	The EmbedPress – Embed PDF, Google Docs, Vimeo, Wistia, Embed YouTube Videos, Audios, Maps & Embed Any Documents in Gutenberg & Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the EmbedPress document widget in all versions up to, and including, 3.9.12 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.	5.4	More Details
CVE-2024-1213	The Easy Social Feed – Social Photos Gallery – Post Feed – Like Box plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.5.4. This is due to missing or incorrect nonce validation on the esf_insta_save_access_token and efbl_save_facebook_access_token functions. This makes it possible for unauthenticated attackers to connect their facebook and instagram pages to the site via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.4	More Details
CVE-2024-29808	The image_id parameter of the AJAX call to the editimage_bwg action of admin-ajax.php is vulnerable to reflected Cross Site Scripting. The value of the image_id parameter is embedded within an existing JavaScript within the response allowing arbitrary JavaScript to be inserted and executed. The attacker must target a an authenticated user with permissions to access this component to exploit this issue.	5.4	More Details
CVE-2024-28593	The Chat activity in Moodle 4.3.3 allows students to insert a potentially unwanted HTML A element or IMG element, or HTML content that leads to a performance degradation. NOTE: the vendor's Using_Chat page says "If you know some HTML code, you can use it in your text to do things like insert images, play sounds or create different coloured and sized text." This page also says "Chat is due to be removed from standard Moodle."	5.4	More Details
CVE-2024-29810	The thumb_url parameter of the AJAX call to the editimage_bwg action of admin-ajax.php is vulnerable to reflected Cross Site Scripting. The value of the thumb_url parameter is embedded within an existing JavaScript within the response allowing arbitrary JavaScript to be inserted and executed. The attacker must target a an authenticated user with permissions to access this component to exploit this issue.	5.4	More Details
CVE-2024-29833	The image upload component allows SVG files and the regular expression used to remove script tags can be bypassed by using a Cross Site Scripting payload which does not match the regular expression; one example of this is the inclusion of whitespace within the script tag. An attacker must target an authenticated user with permissions to access this feature, however once uploaded the payload is also accessible to unauthenticated users.	5.4	More Details
CVE-2024-28560	SQL injection vulnerability in Niushop B2B2C v.5.3.3 and before allows an attacker to escalate privileges via the deleteArea() function of the Address.php component.	5.4	More Details
CVE-2024-28034	Cross-site scripting vulnerability exists in Mini Thread Version 3.33βi. An arbitrary script may be executed on the web browser of the user accessing the website that uses the product. Note that the developer was unreachable, therefore, users should consider stop using Mini Thread Version 3.33βi.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1502	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the tutor_delete_announcement() function in all versions up to, and including, 2.6.1. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete arbitrary posts.	5.4	More Details
CVE-2024-29025	Netty is an asynchronous event-driven network application framework for rapid development of maintainable high performance protocol servers & clients. The `HttpPostRequestDecoder` can be tricked to accumulate data. While the decoder can store items on the disk if configured so, there are no limits to the number of fields the form can have, an attacher can send a chunked post consisting of many small fields that will be accumulated in the `bodyListHttpData` list. The decoder cumulates bytes in the `undecodedChunk` buffer until it can decode a field, this field can cumulate data without limits. This vulnerability is fixed in 4.1.108.Final.	5.3	More Details
CVE-2018-25100	The Mojolicious module before 7.66 for Perl may leak cookies in certain situations related to multiple similar cookies for the same domain. This affects Mojo::UserAgent::CookieJar.	5.3	More Details
CVE-2024-29042	Translate is a package that allows users to convert text to different languages on Node.js and the browser. Prior to version 3.0.0, an attacker controlling the second variable of the `translate` function is able to perform a cache poisoning attack. They can change the outcome of translation requests made by subsequent users. The `opt.id` parameter allows the overwriting of the cache key. If an attacker sets the `id` variable to the cache key that would be generated by another user, they can choose the response that user gets served. Version 3.0.0 fixes this issue.	5.3	More Details
CVE-2024-1473	The Coming Soon & Maintenance Mode by Colorlib plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.0.99 via the REST API. This makes it possible for unauthenticated attackers to obtain post and page contents via REST API thus bypassing maintenance mode protection provided by the plugin.	5.3	More Details
CVE-2024-1477	The Easy Maintenance Mode plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.2 via the REST API. This makes it possible for authenticated attackers to obtain post and page content via REST API thus bypassign the protection provided by the plugin.	5.3	More Details
CVE-2022-44595	Improper Authentication vulnerability in Melapress WP 2FA allows Authentication Bypass.This issue affects WP 2FA: from n/a through 2.2.0.	5.3	More Details
CVE-2024-29244	Shenzhen Libituo Technology Co., Ltd LBT-T300-mini v1.2.9 was discovered to contain a buffer overflow via the pin_code_3g parameter at /apply.cgi.	5.3	More Details
CVE-2024-22077	An issue was discovered in Elspec G5 digital fault recorder versions 1.1.4.15 and before. The SQLite database file has weak permissions.	5.3	More Details
CVE-2024-2007	A vulnerability was found in OpenBMB XAgent 1.0.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Privileged Mode. The manipulation leads to sandbox issue. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used. The identifier VDB-255265 was assigned to this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7232	The Backup and Restore WordPress WordPress plugin through 1.45 does not protect some log files containing sensitive information such as site configuration etc, allowing unauthenticated users to access such data	5.3	More Details
CVE-2024-28834	A flaw was found in GnuTLS. The Minerva attack is a cryptographic vulnerability that exploits deterministic behavior in systems like GnuTLS, leading to side-channel leaks. In specific scenarios, such as when using the GNUTLS_PRIVKEY_FLAG_REPRODUCIBLE flag, it can result in a noticeable step in nonce size from 513 to 512 bits, exposing a potential timing side-channel.	5.3	More Details
CVE-2024-30187	Anope before 2.0.15 does not prevent resetting the password of a suspended account.	5.3	More Details
CVE-2024-2863	This vulnerability allows remote attackers to traverse paths via file upload on the affected LG LED Assistant.	5.3	More Details
CVE-2024-26307	Possible race condition vulnerability in Apache Doris. Some of code using `chmod()` method. This method run the risk of someone renaming the file out from under user and chmodding the wrong file. This could theoretically happen, but the impact would be minimal. This issue affects Apache Doris: before 1.2.8, before 2.0.4. Users are recommended to upgrade to version 2.0.4, which fixes the issue.	5.3	More Details
CVE-2024-21914	A vulnerability exists in the affected product that allows a malicious user to restart the Rockwell Automation PanelView™ Plus 7 terminal remotely without security protections. If the vulnerability is exploited, it could lead to the loss of view or control of the PanelView™ product.	5.3	More Details
CVE-2024-29186	Bref is an open-source project that helps users go serverless on Amazon Web Services with PHP. When Bref prior to version 2.1.17 is used with the Event-Driven Function runtime and the handler is a `RequestHandlerInterface`, then the Lambda event is converted to a PSR7 object. During the conversion process, if the request is a MultiPart, each part is parsed. In the parsing process, the `Content-Type` header of each part is read using the `Riverline/multipart-parser` library. The library, in the `StreamedPart::parseHeaderContent` function, performs slow multi-byte string operations on the header value. Precisely, the `mb_convert_encoding` function is used with the first (`$string`) and third (`$from_encoding`) parameters read from the header value. An attacker could send specifically crafted requests which would force the server into performing long operations with a consequent long billed duration. The attack has the following requirements and limitations: The Lambda should use the Event-Driven Function runtime and the `RequestHandlerInterface` handler and should implement at least an endpoint accepting POST requests; the attacker can send requests up to 6MB long (this is enough to cause a billed duration between 400ms and 500ms with the default 1024MB RAM Lambda image of Bref); and if the Lambda uses a PHP runtime <= php-82, the impact is higher as the billed duration in the default 1024MB RAM Lambda image of Bref could be brought to more than 900ms for each request. Notice that the vulnerability applies only to headers read from the request body as the request header has a limitation which allows a total maximum size of ~10KB. Version 2.1.17 contains a fix for this issue.	5.3	More Details
CVE-2023-27630	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in PeepSo Community by PeepSo.This issue affects Community by PeepSo: from n/a through 6.0.9.0.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32751	IBM Security Verify Directory 10.0.0 could disclose sensitive server information that could be used in further attacks against the system. IBM X-Force ID: 228437.	5.3	More Details
CVE-2024-25964	Dell PowerScale OneFS 9.5.0.x through 9.7.0.x contain a covert timing channel vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to denial of service.	5.3	More Details
CVE-2024-29735	Improper Preservation of Permissions vulnerability in Apache Airflow.This issue affects Apache Airflow from 2.8.2 through 2.8.3. Airflow's local file task handler in Airflow incorrectly set permissions for all parent folders of log folder, in default configuration adding write access to Unix group of the folders. In the case Airflow is run with the root user (not recommended) it added group write permission to all folders up to the root of the filesystem. If your log files are stored in the home directory, these permission changes might impact your ability to run SSH operations after your home directory becomes group-writeable. This issue does not affect users who use or extend Airflow using Official Airflow Docker reference images (https://hub.docker.com/r/apache/airflow/) - those images require to have group write permission set anyway. You are affected only if you install Airflow using local installation / virtualenv or other Docker images, but the issue has no impact if docker containers are used as intended, i.e. where Airflow components do not share containers with other applications and users. Also you should not be affected if your umask is 002 (group write enabled) - this is the default on many linux systems. Recommendation for users using Airflow outside of the containers: * if you are using root to run Airflow, change your Airflow user to use non-root * upgrade Apache Airflow to 2.8.4 or above * If you prefer not to upgrade, you can change the https://airflow.apache.org/docs/apache-airflow/stable/configurations-ref.html#file-task-handler-new-folder-permissions to 0o755 (original value 0o775). * if you already ran Airflow tasks before and your default umask is 022 (group write disabled) you should stop Airflow components, check permissions of AIRFLOW_HOME/logs in all your components and all parent directories of this directory and remove group write access for all the parent directories	5.3	More Details
CVE-2023-46839	PCI devices can make use of a functionality called phantom functions, that when enabled allows the device to generate requests using the IDs of functions that are otherwise unpopulated. This allows a device to extend the number of outstanding requests. Such phantom functions need an IOMMU context setup, but failure to setup the context is not fatal when the device is assigned. Not failing device assignment when such failure happens can lead to the primary device being assigned to a guest, while some of the phantom functions are assigned to a different domain.	5.3	More Details
CVE-2024-1181	The Coming Soon, Under Construction & Maintenance Mode By Dazzler plugin for WordPress is vulnerable to maintenance mode bypass in all versions up to, and including, 2.1.2. This is due to the plugin relying on the REQUEST_URI to determine if the page being accesses is an admin area. This makes it possible for unauthenticated attackers to bypass maintenance mode and access the site which may be considered confidential when in maintenance mode.	5.3	More Details
CVE-2023-45177	IBM MQ 9.0 LTS, 9.1 LTS, 9.2 LTS, 9.3 LTS and 9.3 CD is vulnerable to a denial-of-service attack due to an error within the MQ clustering logic. IBM X-Force ID: 268066.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29032	Qiskit IBM Runtime is an environment that streamlines quantum computations and provides optimal implementations of the Qiskit quantum computing SDK. Starting in version 0.1.0 and prior to version 0.21.2, deserializing json data using `qiskit_ibm_runtime.RuntimeDecoder` can lead to arbitrary code execution given a correctly formatted input string. Version 0.21.2 contains a fix for this issue.	5.3	More Details
CVE-2021-47140	In the Linux kernel, the following vulnerability has been resolved: iommu/amd: Clear DMA ops when switching domain Since commit 08a27c1c3ecf ("iommu: Add support to change default domain of an iommu group") a user can switch a device between IOMMU and direct DMA through sysfs. This doesn't work for AMD IOMMU at the moment because dev->dma_ops is not cleared when switching from a DMA to an identity IOMMU domain. The DMA layer thus attempts to use the dma-iommu ops on an identity domain, causing an oops: # echo 0000:00:05.0 > /sys/sys/bus/pci/drivers/e1000e/unbind # echo identity > /sys/bus/pci/devices/0000:00:05.0/iommu_group/type # echo 0000:00:05.0 > /sys/sys/bus/pci/drivers/e1000e/bind ... BUG: kernel NULL pointer dereference, address: 0000000000000028 ... Call Trace: iommu_dma_alloc e1000e_setup_tx_resources e1000e_open Since iommu_change_dev_def_domain() calls probe_finalize() again, clear the dma_ops there like Vt-d does.	5.3	More Details
CVE-2024-1119	The Order Tip for WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the export_tips_to_csv() function in all versions up to, and including, 1.3.1. This makes it possible for unauthenticated attackers to export the plugin's order fees.	5.3	More Details
CVE-2024-28835	A flaw has been discovered in GnuTLS where an application crash can be induced when attempting to verify a specially crafted .pem bundle using the "certtool --verify-chain" command.	5.0	More Details
CVE-2024-22356	IBM App Connect Enterprise 11.0.0.1 through 11.0.0.23, 12.0.1.0 through 12.0.9.0 and IBM Integration Bus for z/OS 10.1 through 10.1.0.2store potentially sensitive information in log or trace files that could be read by a privileged user. IBM X-Force ID: 280893.	4.9	More Details
CVE-2024-29883	CreateWiki is Miraheze's MediaWiki extension for requesting & creating wikis. Suppression of wiki requests does not work as intended, and always restricts visibility to those with the `(createwiki)` user right regardless of the settings one sets on a given wiki request. This may expose information to users who are not supposed to be able to access it.	4.9	More Details
CVE-2024-26303	Authenticated Denial of Service Vulnerability in ArubaOS-Switch SSH Daemon	4.9	More Details
CVE-2023-42954	A privilege escalation issue existed in FileMaker Server, potentially exposing sensitive information to front-end websites when signed in to the Admin Console with an administrator role. This issue has been fixed in FileMaker Server 20.3.1 by reducing the information sent in requests.	4.9	More Details
CVE-2024-25957	Dell Grab for Windows, versions 5.0.4 and below, contains a cleartext storage of sensitive information vulnerability in its appsync module. An authenticated local attacker could potentially exploit this vulnerability, leading to information disclosure that could be used to access the appsync application with elevated privileges.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23819	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.4 and 2.24.1 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in the GeoServer catalog that will execute in the context of another user's browser when viewed in the MapML HTML Page. The MapML extension must be installed and access to the MapML HTML Page is available to all users although data security may limit users' ability to trigger the XSS. Versions 2.23.4 and 2.24.1 contain a patch for this issue.	4.8	More Details
CVE-2024-23643	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.2 and 2.24.1 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in the GeoServer catalog that will execute in the context of another administrator’s browser when viewed in the GWC Seed Form. Access to the GWC Seed Form is limited to full administrators by default and granting non-administrators access to this endpoint is not recommended. Versions 2.23.2 and 2.24.1 contain a fix for this issue.	4.8	More Details
CVE-2024-23818	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.3 and 2.24.1 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in the GeoServer catalog that will execute in the context of another user's browser when viewed in the WMS GetMap OpenLayers Output Format. Access to the WMS OpenLayers Format is available to all users by default although data and service security may limit users' ability to trigger the XSS. Versions 2.23.3 and 2.24.1 contain a patch for this issue.	4.8	More Details
CVE-2024-23821	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.4 and 2.24.1 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in the GeoServer catalog that will execute in the context of another user's browser when viewed in the GWC Demos Page. Access to the GWC Demos Page is available to all users although data security may limit users' ability to trigger the XSS. Versions 2.23.4 and 2.24.1 contain a patch for this issue.	4.8	More Details
CVE-2024-1232	The CM Download Manager WordPress plugin before 2.9.0 does not have CSRF checks in some places, which could allow attackers to make logged in admins delete downloads via a CSRF attack	4.8	More Details
CVE-2024-23642	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.4 and 2.24.1 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in the GeoServer catalog that will execute in the context of another user's browser when viewed in the WMS GetMap SVG Output Format when the Simple SVG renderer is enabled. Access to the WMS SVG Format is available to all users by default although data and service security may limit users' ability to trigger the XSS. Versions 2.23.4 and 2.24.1 contain a fix for this issue.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51445	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.3 and 2.24.0 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in uploaded style/legend resources that will execute in the context of another administrator's browser when viewed in the REST Resources API. Access to the REST Resources API is limited to full administrators by default and granting non-administrators access to this endpoint should be carefully considered as it may allow access to files containing sensitive information. Versions 2.23.3 and 2.24.0 contain a patch for this issue.	4.8	More Details
CVE-2022-32754	IBM Security Verify Directory 10.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 228445.	4.8	More Details
CVE-2024-23640	GeoServer is an open source software server written in Java that allows users to share and edit geospatial data. A stored cross-site scripting (XSS) vulnerability exists in versions prior to 2.23.3 and 2.24.0 that enables an authenticated administrator with workspace-level privileges to store a JavaScript payload in uploaded style/legend resources or in a specially crafted datastore file that will execute in the context of another user's browser when viewed in the Style Publisher. Access to the Style Publisher is available to all users although data security may limit users' ability to trigger the XSS. Versions 2.23.3 and 2.24.0 contain a fix for this issue.	4.8	More Details
CVE-2024-24050	Cross Site Scripting (XSS) vulnerability in Sourcecodester Workout Journal App 1.0 allows attackers to run arbitrary code via parameters firstname and lastname in /add-user.php.	4.7	More Details
CVE-2024-28108	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. Due to insufficient validation on the `contentLink` parameter, it is possible for unauthenticated users to inject HTML code to the page which might affect other users. _Also, requires that adding new FAQs is allowed for guests and that the admin doesn't check the content of a newly added FAQ._ This vulnerability is fixed in 3.2.6.	4.7	More Details
CVE-2024-26247	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	4.7	More Details
CVE-2024-2754	A vulnerability classified as critical has been found in SourceCodester Complete E-Commerce Site 1.0. Affected is an unknown function of the file /admin/users_photo.php. The manipulation of the argument photo leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257544.	4.7	More Details
CVE-2024-28045	Improper neutralization of input within the affected product could lead to cross-site scripting.	4.6	More Details
CVE-2024-27932	Deno is a JavaScript, TypeScript, and WebAssembly runtime. Starting in version 1.8.0 and prior to version 1.40.4, Deno improperly checks that an import specifier's hostname is equal to or a child of a token's hostname, which can cause tokens to be sent to servers they shouldn't be sent to. An auth token intended for `example[.]com` may be sent to `notexample[.]com`. Anyone who uses DENO_AUTH_TOKENS and imports potentially untrusted code is affected. Version 1.40.0 contains a patch for this issue	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32753	IBM Security Verify Directory 10.0.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 228444.	4.5	More Details
CVE-2024-21920	A memory buffer vulnerability in Rockwell Automation Arena Simulation could potentially let a threat actor read beyond the intended memory boundaries. This could reveal sensitive information and even cause the application to crash, resulting in a denial-of-service condition. To trigger this, the user would unwittingly need to open a malicious file shared by the threat actor.	4.4	More Details
CVE-2024-2748	A Cross Site Request Forgery vulnerability was identified in GitHub Enterprise Server that allowed an attacker to execute unauthorized actions on behalf of an unsuspecting user. A mitigating factor is that user interaction is required. This vulnerability affected GitHub Enterprise Server 3.12.0 and was fixed in versions 3.12.1. This vulnerability was reported via the GitHub Bug Bounty program.	4.3	More Details
CVE-2024-2628	Inappropriate implementation in Downloads in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted URL. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-1214	The Easy Social Feed – Social Photos Gallery – Post Feed – Like Box plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 6.5.4. This is due to missing or incorrect nonce validation on the save_groups_list function. This makes it possible for unauthenticated attackers to disconnect a site's facebook or instagram page/group connection 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-2024-2291	In Progress MOVEit Transfer versions released before 2022.0.11 (14.0.11), 2022.1.12 (14.1.12), 2023.0.9 (15.0.9), 2023.1.4 (15.1.4), a logging bypass vulnerability has been discovered. An authenticated user could manipulate a request to bypass the logging mechanism within the web application which results in user activity not being logged properly.	4.3	More Details
CVE-2024-2631	Inappropriate implementation in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2024-2904	Cross-Site Request Forgery (CSRF) vulnerability in Extend Themes Calliope.This issue affects Calliope: from n/a through 1.0.33.	4.3	More Details
CVE-2024-2951	Cross-Site Request Forgery (CSRF) vulnerability in Metagauss RegistrationMagic.This issue affects RegistrationMagic: from n/a through 5.3.0.0.	4.3	More Details
CVE-2024-23520	Missing Authorization vulnerability in AccessAlly PopupAlly.This issue affects PopupAlly: from n/a through 2.1.0.	4.3	More Details
CVE-2024-2629	Incorrect security UI in iOS in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24711	Missing Authorization vulnerability in weDevs WooCommerce Conversion Tracking.This issue affects WooCommerce Conversion Tracking: from n/a through 2.0.11.	4.3	More Details
CVE-2024-1995	The Smart Custom Fields plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the relational_posts_search() function in all versions up to, and including, 4.2.2. This makes it possible for authenticated attackers, with subscrber-level access and above, to retrieve post content that is password protected and/or private.	4.3	More Details
CVE-2024-25137	In AutomationDirect C-MORE EA9 HMI there is a program that copies a buffer of a size controlled by the user into a limited sized buffer on the stack which may lead to a stack overflow. The result of this stack-based buffer overflow can lead to denial-of-service conditions.	4.3	More Details
CVE-2023-52214	Missing Authorization vulnerability in voidCoders Void Contact Form 7 Widget For Elementor Page Builder.This issue affects Void Contact Form 7 Widget For Elementor Page Builder: from n/a through 2.3.	4.3	More Details
CVE-2024-29036	Saleor Storefront is software for building e-commerce experiences. Prior to commit 579241e75a5eb332ccf26e0bcdd54befa33f4783, when any user authenticates in the storefront, anonymous users are able to access their data. The session is leaked through cache and can be accessed by anyone. Users should upgrade to a version that incorporates commit 579241e75a5eb332ccf26e0bcdd54befa33f4783 or later to receive a patch. A possible workaround is to temporarily disable authentication by changing the usage of `createSaleorAuthClient()`.	4.3	More Details
CVE-2024-2384	The WooCommerce POS plugin for WordPress is vulnerable to information disclosure in all versions up to, and including, 1.4.11. This is due to the plugin not properly verifying the authentication and authorization of the current user This makes it possible for authenticated attackers, with customer-level access and above, to view potentially sensitive information about other users by leveraging their order id	4.3	More Details
CVE-2024-1325	The Live Sales Notification for Woocommerce – Woomotiv plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.4.3. This is due to missing or incorrect nonce validation on the 'ajax_cancel_review' function. This makes it possible for unauthenticated attackers to reset the site's review count 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-2024-29881	TinyMCE is an open source rich text editor. A cross-site scripting (XSS) vulnerability was discovered in TinyMCE's content loading and content inserting code. A SVG image could be loaded though an `object` or `embed` element and that image could potentially contain a XSS payload. This vulnerability is fixed in 6.8.1 and 7.0.0.	4.3	More Details
CVE-2024-24718	Missing Authorization vulnerability in PropertyHive.This issue affects PropertyHive: from n/a through 2.0.6.	4.3	More Details
CVE-2024-24719	Missing Authorization vulnerability in Uriahs Victor Location Picker at Checkout for WooCommerce.This issue affects Location Picker at Checkout for WooCommerce: from n/a through 1.8.9.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29203	TinyMCE is an open source rich text editor. A cross-site scripting (XSS) vulnerability was discovered in TinyMCE's content insertion code. This allowed `iframe` elements containing malicious code to execute when inserted into the editor. These `iframe` elements are restricted in their permissions by same-origin browser protections, but could still trigger operations such as downloading of malicious assets. This vulnerability is fixed in 6.8.1.	4.3	More Details
CVE-2024-30235	Missing Authorization vulnerability in Themeisle Multiple Page Generator Plugin – MPG.This issue affects Multiple Page Generator Plugin – MPG: from n/a through 3.4.0.	4.3	More Details
CVE-2024-2911	A vulnerability, which was classified as problematic, was found in Tianjin PubliCMS 4.0.202302.e. This affects an unknown part. The manipulation leads to cross-site request forgery. 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.	4.3	More Details
CVE-2024-1844	The RevivePress – Keep your Old Content Evergreen plugin for WordPress is vulnerable to unauthorized access and modification of data due to a missing capability check on the import_data and copy_data functions in all versions up to, and including, 1.5.6. This makes it possible for authenticated attackers, with subscriber-level access or higher, to overwrite plugin settings and view them.	4.3	More Details
CVE-2024-2197	The Chirp Access app contains a hard-coded password, BEACON_PASSWORD. An attacker within Bluetooth range could change configuration settings within the Bluetooth beacon, effectively disabling the application's ability to notify users when they are near a Beacon-enabled access point. This variable cannot be used to change the configuration settings of the door readers or locksets and does not affect the ability for authorized users of the mobile application to lock or unlock access points.	4.3	More Details
CVE-2024-1503	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.6.1. This is due to missing or incorrect nonce validation on the erase_tutor_data() function. This makes it possible for unauthenticated attackers to deactivate the plugin and erase all data via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This requires the "Erase upon uninstallation" option to be enabled.	4.3	More Details
CVE-2023-30480	Missing Authorization vulnerability in Sparkle WP Educenter.This issue affects Educenter: from n/a through 1.5.5.	4.3	More Details
CVE-2024-2080	The LiquidPoll – Polls, Surveys, NPS and Feedback Reviews plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.3.76 via the poller_list shortcode. This makes it possible for authenticated attackers, with contributor-level access and above, to extract information from polls that may be private.	4.3	More Details
CVE-2022-45349	Missing Authorization vulnerability in Muffingroup Betheme.This issue affects Betheme: from n/a through 26.6.1.	4.3	More Details
CVE-2023-25039	Missing Authorization vulnerability in CodePeople Google Maps CP.This issue affects Google Maps CP: from n/a through 1.0.43.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45824	OroPlatform is a PHP Business Application Platform (BAP). A logged in user can access page state data of pinned pages of other users by pageId hash. This vulnerability is fixed in 5.1.4.	4.3	More Details
CVE-2023-48296	OroPlatform is a PHP Business Application Platform (BAP). Navigation history, most viewed and favorite navigation items are returned to storefront user in JSON navigation response if ID of storefront user matches ID of back-office user. This vulnerability is fixed in 5.1.4.	4.3	More Details
CVE-2024-28106	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. By manipulating the news parameter in a POST request, an attacker can inject malicious JavaScript code. Upon browsing to the compromised news page, the XSS payload triggers. This vulnerability is fixed in 3.2.6.	4.3	More Details
CVE-2024-27190	Missing Authorization vulnerability in Jean-David Daviet Download Media.This issue affects Download Media: from n/a through 1.4.2.	4.3	More Details
CVE-2024-2816	A vulnerability classified as problematic was found in Tenda AC15 15.03.05.18. Affected by this vulnerability is the function fromSysToolReboot of the file /goform/SysToolReboot. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257671. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-2817	A vulnerability, which was classified as problematic, has been found in Tenda AC15 15.03.05.18. Affected by this issue is the function fromSysToolRestoreSet of the file /goform/SysToolRestoreSet. The manipulation leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257672. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-24805	Missing Authorization vulnerability in Deepak anand WP Dummy Content Generator.This issue affects WP Dummy Content Generator: from n/a through 3.1.2.	4.3	More Details
CVE-2024-1564	The wp-schema-pro WordPress plugin before 2.7.16 does not validate post access allowing a contributor user to access custom fields on any post regardless of post type or status via a shortcode	4.3	More Details
CVE-2023-37885	Missing Authorization vulnerability in InspiryThemes RealHomes.This issue affects RealHomes: from n/a through 4.0.2.	4.3	More Details
CVE-2023-33923	Missing Authorization vulnerability in HashThemes Viral News, HashThemes Viral, HashThemes HashOne.This issue affects Viral News: from n/a through 1.4.5; Viral: from n/a through 1.8.0; HashOne: from n/a through 1.3.0.	4.3	More Details
CVE-2023-47715	IBM Storage Protect Plus Server 10.1.0 through 10.1.16 could allow an authenticated user with read-only permissions to add or delete entries from an existing HyperVisor configuration. IBM X-Force ID: 271538.	4.3	More Details
CVE-2024-24840	Missing Authorization vulnerability in BdThemes Element Pack Elementor Addons.This issue affects Element Pack Elementor Addons: from n/a through 5.4.11.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24835	Missing Authorization vulnerability in realmag777 BEAR.This issue affects BEAR: from n/a through 1.1.4.	4.3	More Details
CVE-2024-2821	A vulnerability, which was classified as problematic, has been found in DedeCMS 5.7. Affected by this issue is some unknown functionality of the file /src/dede/friendlink_edit.php. The manipulation of the argument id leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257708. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-2822	A vulnerability, which was classified as problematic, was found in DedeCMS 5.7. This affects an unknown part of the file /src/dede/vote_edit.php. The manipulation of the argument aid leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257709 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-49838	Cross-Site Request Forgery (CSRF) vulnerability in KlbTheme Clotya theme, KlbTheme Cosmetsy theme, KlbTheme Furnob theme, KlbTheme Bacola theme, KlbTheme Partdo theme, KlbTheme Medibazar theme, KlbTheme Machic theme.This issue affects Clotya theme: from n/a through 1.1.6; Cosmetsy theme: from n/a through 1.7.7; Furnob theme: from n/a through 1.2.2; Bacola theme: from n/a through 1.3.3; Partdo theme: from n/a through 1.1.1; Medibazar theme: from n/a through 1.8.6; Machic theme: from n/a through 1.2.8.	4.3	More Details
CVE-2024-2823	A vulnerability has been found in DedeCMS 5.7 and classified as problematic. This vulnerability affects unknown code of the file /src/dede/mda_main.php. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257710 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-29057	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4.3	More Details
CVE-2024-2326	The Pretty Links – Affiliate Links, Link Branding, Link Tracking & Marketing Plugin plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.6.3. This is due to missing or incorrect nonce validation when saving plugin settings. This makes it possible for unauthenticated attackers to change the plugin's configuration including stripe integration 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-2024-26196	Microsoft Edge for Android (Chromium-based) Information Disclosure Vulnerability	4.3	More Details
CVE-2024-2820	A vulnerability classified as problematic was found in DedeCMS 5.7. Affected by this vulnerability is an unknown functionality of the file /src/dede/baidunews.php. The manipulation of the argument filename leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257707. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1745	The Testimonial Slider WordPress plugin before 2.3.7 does not properly ensure that a user has the necessary capabilities to edit certain sensitive Testimonial Slider WordPress plugin before 2.3.7 settings, making it possible for users with at least the Author role to edit them.	4.3	More Details
CVE-2024-29880	In JetBrains TeamCity before 2023.11 users with access to the agent machine might obtain permissions of the user running the agent process	4.2	More Details
CVE-2024-2728	Information exposure vulnerability in the CIGESv2 system. This vulnerability could allow a local attacker to intercept traffic due to the lack of proper implementation of the TLS protocol.	4.1	More Details
CVE-2023-46840	Incorrect placement of a preprocessor directive in source code results in logic that doesn't operate as intended when support for HVM guests is compiled out of Xen.	4.1	More Details
CVE-2024-29196	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. There is a Path Traversal vulnerability in Attachments that allows attackers with admin rights to upload malicious files to other locations of the web root. This vulnerability is fixed in 3.2.6.	3.8	More Details
CVE-2024-1742	Invocation of the sqlplus command with sensitive information in the command line in the mk_oracle Checkmk agent plugin before Checkmk 2.3.0b4 (beta), 2.2.0p24, 2.1.0p41 and 2.0.0 (EOL) allows the extraction of this information from the process list.	3.8	More Details
CVE-2024-29199	Nautobot is a Network Source of Truth and Network Automation Platform. A number of Nautobot URL endpoints were found to be improperly accessible to unauthenticated (anonymous) users. These endpoints will not disclose any Nautobot data to an unauthenticated user unless the Nautobot configuration variable EXEMPT_VIEW_PERMISSIONS is changed from its default value (an empty list) to permit access to specific data by unauthenticated users. This vulnerability is fixed in 1.6.16 and 2.1.9.	3.7	More Details
CVE-2023-33855	Under certain conditions, RSA operations performed by IBM Common Cryptographic Architecture (CCA) 7.0.0 through 7.5.36 may exhibit non-constant-time behavior. This could allow a remote attacker to obtain sensitive information using a timing-based attack. IBM X-Force ID: 257676.	3.7	More Details
CVE-2024-28868	Umbraco is an ASP.NET content management system. Umbraco 10 prior to 10.8.4 with access to the native login screen is vulnerable to a possible user enumeration attack. This issue was fixed in version 10.8.5. As a workaround, one may disable the native login screen by exclusively using external logins.	3.7	More Details
CVE-2024-2686	A vulnerability has been found in Campcodes Online Job Finder System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/applicants/controller.php. The manipulation of the argument JOBREGID leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257386 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-2685	A vulnerability, which was classified as problematic, was found in Campcodes Online Job Finder System 1.0. This affects an unknown part of the file /admin/applicants/index.php. The manipulation of the argument view leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257385 was assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2684	A vulnerability, which was classified as problematic, has been found in Campcodes Online Job Finder System 1.0. Affected by this issue is some unknown functionality of the file /admin/category/index.php. The manipulation of the argument view leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257384.	3.5	More Details
CVE-2024-2679	A vulnerability was found in Campcodes Online Job Finder System 1.0. It has been classified as problematic. This affects an unknown part of the file /admin/vacancy/index.php. The manipulation of the argument view leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257379.	3.5	More Details
CVE-2024-2683	A vulnerability classified as problematic was found in Campcodes Online Job Finder System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/company/index.php. The manipulation of the argument view leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257383.	3.5	More Details
CVE-2024-2780	A vulnerability was found in Campcodes Online Marriage Registration System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/admin-profile.php. The manipulation of the argument adminname leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257614 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-2682	A vulnerability classified as problematic has been found in Campcodes Online Job Finder System 1.0. Affected is an unknown function of the file /admin/employee/controller.php. The manipulation of the argument EMPLOYEEID 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. VDB-257382 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-2681	A vulnerability was found in Campcodes Online Job Finder System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/employee/index.php. The manipulation of the argument view leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257381 was assigned to this vulnerability.	3.5	More Details
CVE-2024-2680	A vulnerability was found in Campcodes Online Job Finder System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/user/index.php. The manipulation of the argument view leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257380.	3.5	More Details
CVE-2020-36826	A vulnerability was found in AwesomestCode LiveBot. It has been classified as problematic. Affected is the function parseSend of the file js/parseMessage.js. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. Upgrading to version 0.1 is able to address this issue. The name of the patch is 57505527f838d1e46e8f93d567ba552a30185bfa. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-257784.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2779	A vulnerability was found in Campcodes Online Marriage Registration System 1.0. It has been classified as problematic. This affects an unknown part of the file /admin/application-bwdates-reports-details.php. The manipulation of the argument fromdate leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257613 was assigned to this vulnerability.	3.5	More Details
CVE-2024-2832	A vulnerability classified as problematic was found in Campcodes Online Shopping System 1.0. This vulnerability affects unknown code of the file /offersmail.php. The manipulation of the argument email leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257752.	3.5	More Details
CVE-2024-2773	A vulnerability classified as problematic has been found in Campcodes Online Marriage Registration System 1.0. This affects an unknown part of the file /user/search.php. The manipulation of the argument searchdata leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257607.	3.5	More Details
CVE-2024-2720	A vulnerability classified as problematic was found in Campcodes Complete Online DJ Booking System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/aboutus.php. The manipulation of the argument pagetitle leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257473 was assigned to this vulnerability.	3.5	More Details
CVE-2024-2716	A vulnerability was found in Campcodes Complete Online DJ Booking System 1.0. It has been classified as problematic. This affects an unknown part of the file /admin/contactus.php. The manipulation of the argument email leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257469 was assigned to this vulnerability.	3.5	More Details
CVE-2024-2775	A vulnerability, which was classified as problematic, has been found in Campcodes Online Marriage Registration System 1.0. This issue affects some unknown processing of the file /user/user-profile.php. The manipulation of the argument lname leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257609 was assigned to this vulnerability.	3.5	More Details
CVE-2024-2778	A vulnerability was found in Campcodes Online Marriage Registration System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/search.php. The manipulation of the argument searchdata leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257612.	3.5	More Details
CVE-2024-2717	A vulnerability was found in Campcodes Complete Online DJ Booking System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/booking-search.php. The manipulation of the argument searchdata leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257470 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2024-2719	A vulnerability classified as problematic has been found in Campcodes Complete Online DJ Booking System 1.0. Affected is an unknown function of the file /admin/admin-profile.php. The manipulation of the argument adminname 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 identifier of this vulnerability is VDB-257472.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2718	A vulnerability was found in Campcodes Complete Online DJ Booking System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/booking-bwdates-reports-details.php. The manipulation of the argument fromdate leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257471.	3.5	More Details
CVE-2024-2715	A vulnerability was found in Campcodes Complete Online DJ Booking System 1.0 and classified as problematic. Affected by this issue is some unknown functionality of the file /admin/user-search.php. The manipulation of the argument searchdata leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257468.	3.5	More Details
CVE-2024-28584	Null Pointer Dereference vulnerability in open source FreeImage v.3.19.0 [r1909] allows a local attacker to cause a denial of service (DoS) via the J2KImageToFIBITMAP() function when reading images in J2K format.	3.3	More Details
CVE-2024-2971	Out-of-bounds array write in Xpdf 4.05 and earlier, triggered by negative object number in indirect reference in the input PDF file.	2.9	More Details
CVE-2024-30204	In Emacs before 29.3, LaTeX preview is enabled by default for e-mail attachments.	2.8	More Details
CVE-2022-32756	IBM Security Verify Directory 10.0.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 228507.	2.7	More Details
CVE-2023-52620	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: disallow timeout for anonymous sets Never used from userspace, disallow these parameters.	2.5	More Details
CVE-2024-29338	Anchor CMS v0.12.7 was discovered to contain a Cross-Site Request Forgery (CSRF) via /anchor/admin/categories/delete/2.	2.4	More Details
CVE-2023-23349	Kaspersky has fixed a security issue in Kaspersky Password Manager (KPM) for Windows that allowed a local user to recover the auto-filled credentials from a memory dump when the KPM extension for Google Chrome is used. To exploit the issue, an attacker must trick a user into visiting a login form of a website with the saved credentials, and the KPM extension must autofill these credentials. The attacker must then launch a malware module to steal those specific credentials.	2.2	More Details
CVE-2024-26642	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: disallow anonymous set with timeout flag Anonymous sets are never used with timeout from userspace, reject this. Exception to this rule is NFT_SET_EVAL to ensure legacy meters still work.	N/A	More Details
CVE-2021-36759	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-35342. Reason: This candidate is a reservation duplicate of CVE-2021-35342. Notes: All CVE users should reference CVE-2021-35342 instead of this candidate. 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-2023-41696	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-24272	An issue in iTop DualSafe Password Manager & Digital Vault before 1.4.24 allows a local attacker to obtain sensitive information via leaked credentials as plaintext in a log file that can be accessed by the local user without knowledge of the master secret.	N/A	More Details
CVE-2024-2167	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-2041. Reason: This candidate is a reservation duplicate of CVE-2024-2041. Notes: All CVE users should reference CVE-2024-2041 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-29442	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2024-1727	A Cross-Site Request Forgery (CSRF) vulnerability in gradio-app/gradio allows attackers to upload multiple large files to a victim's system if they are running Gradio locally. By crafting a malicious HTML page that triggers an unauthorized file upload to the victim's server, an attacker can deplete the system's disk space, potentially leading to a denial of service. This issue affects the file upload functionality as implemented in gradio/routes.py.	N/A	More Details
CVE-2024-30161	In Qt 6.5.4, 6.5.5, and 6.6.2, QNetworkReply header data might be accessed via a dangling pointer in Qt for WebAssembly (wasm). (Earlier and later versions are unaffected.)	N/A	More Details
CVE-2024-26557	Codiad v2.8.4 allows reflected XSS via the components/market/dialog.php type parameter.	N/A	More Details
CVE-2023-49837	Uncontrolled Resource Consumption vulnerability in David Artiss Code Embed.This issue affects Code Embed: from n/a through 2.3.6.	N/A	More Details
CVE-2024-29179	phpMyFAQ is an open source FAQ web application for PHP 8.1+ and MySQL, PostgreSQL and other databases. An attacker with admin privileges can upload an attachment containing JS code without extension and the application will render it as HTML which allows for XSS attacks.	N/A	More Details
CVE-2024-29473	OneBlog v2.3.4 was discovered to contain a stored cross-site scripting (XSS) vulnerability via the Role Management module.	N/A	More Details
CVE-2023-4063	Certain HP OfficeJet Pro printers are potentially vulnerable to a Denial of Service when using an improper eSCL URL GET request.	N/A	More Details
CVE-2024-1455	A vulnerability in the langchain-ai/langchain repository allows for a Billion Laughs Attack, a type of XML External Entity (XXE) exploitation. By nesting multiple layers of entities within an XML document, an attacker can cause the XML parser to consume excessive CPU and memory resources, leading to a denial of service (DoS).	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1231	The CM Download Manager WordPress plugin before 2.9.0 does not have CSRF checks in some places, which could allow attackers to make logged in admins unpublish downloads via a CSRF attack	N/A	More Details
CVE-2020-36827	The XAO::Web module before 1.84 for Perl mishandles < and > characters in JSON output during use of json-embed in Web::Action.	N/A	More Details
CVE-2024-26643	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: mark set as dead when unbinding anonymous set with timeout While the rhashtable set gc runs asynchronously, a race allows it to collect elements from anonymous sets with timeouts while it is being released from the commit path. Mingi Cho originally reported this issue in a different path in 6.1.x with a pipapo set with low timeouts which is not possible upstream since 7395dfacfff6 ("netfilter: nf_tables: use timestamp to check for set element timeout"). Fix this by setting on the dead flag for anonymous sets to skip async gc in this case. According to 08e4c8c5919f ("netfilter: nf_tables: mark newset as dead on transaction abort"), Florian plans to accelerate abort path by releasing objects via workqueue, therefore, this sets on the dead flag for abort path too.	N/A	More Details
CVE-2024-1603	paddlepaddle/paddle 2.6.0 allows arbitrary file read via paddle.vision.ops.read_file.	N/A	More Details
CVE-2024-2802	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-1166. Reason: This candidate is a reservation duplicate of CVE-2024-1166. Notes: All CVE users should reference CVE-2024-1166 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-29865	Logpoint before 7.1.0 allows Self-XSS on the LDAP authentication page via the username to the LDAP login form.	N/A	More Details
CVE-2024-29440	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that there was not reasonable evidence to determine the existence of a vulnerability.	N/A	More Details
CVE-2021-47177	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Fix sysfs leak in alloc_iommu() iommu_device_sysfs_add() is called before, so is has to be cleaned on subsequent errors.	N/A	More Details
CVE-2021-47176	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: add missing discipline function Fix crash with illegal operation exception in dasd_device_tasklet. Commit b72949328869 ("s390/dasd: Prepare for additional path event handling") renamed the verify_path function for ECKD but not for FBA and DIAG. This leads to a panic when the path verification function is called for a FBA or DIAG device. Fix by defining a wrapper function for dasd_generic_verify_path().	N/A	More Details
CVE-2021-47159	In the Linux kernel, the following vulnerability has been resolved: net: dsa: fix a crash if ->get_sset_count() fails If ds->ops->get_sset_count() fails then it "count" is a negative error code such as -EOPNOTSUPP. Because "i" is an unsigned int, the negative error code is type promoted to a very high value and the loop will corrupt memory until the system crashes. Fix this by checking for error codes and changing the type of "i" to just int.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47175	In the Linux kernel, the following vulnerability has been resolved: net/sched: fq_pie: fix OOB access in the traffic path the following script: # tc qdisc add dev eth0 handle 0x1 root fq_pie flows 2 # tc qdisc add dev eth0 clsact # tc filter add dev eth0 egress matchall action skbedit priority 0x10002 # ping 192.0.2.2 -I eth0 -c2 -w1 -q produces the following splat: BUG: KASAN: slab-out-of-bounds in fq_pie_qdisc_enqueue+0x1314/0x19d0 [sch_fq_pie] Read of size 4 at addr ffff888171306924 by task ping/942 CPU: 3 PID: 942 Comm: ping Not tainted 5.12.0+ #441 Hardware name: Red Hat KVM, BIOS 1.11.1-4.module+el8.1.0+4066+0f1aadab 04/01/2014 Call Trace: dump_stack+0x92/0xc1 print_address_description.constprop.7+0x1a/0x150 kasan_report.cold.13+0x7f/0x111 fq_pie_qdisc_enqueue+0x1314/0x19d0 [sch_fq_pie] __dev_queue_xmit+0x1034/0x2b10 ip_finish_output2+0xc62/0x2120 __ip_finish_output+0x553/0xea0 ip_output+0x1ca/0x4d0 ip_send_skb+0x37/0xa0 raw_sendmsg+0x1c4b/0x2d00 sock_sendmsg+0xdb/0x110 __sys_sendto+0x1d7/0x2b0 __x64_sys_sendto+0xdd/0x1b0 do_syscall_64+0x3c/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7fe69735c3eb Code: 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 f3 0f 1e fa 48 8d 05 75 42 2c 00 41 89 ca 8b 00 85 c0 75 14 b8 2c 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 75 c3 0f 1f 40 00 41 57 4d 89 c7 41 56 41 89 RSP: 002b:00007fff06d7fb38 EFLAGS: 00000246 ORIG_RAX: 000000000000002c RAX: ffffffffffffffda RBX: 000055e961413700 RCX: 00007fe69735c3eb RDX: 0000000000000040 RSI: 000055e961413700 RDI: 0000000000000003 RBP: 0000000000000040 R08: 000055e961410500 R09: 0000000000000010 R10: 0000000000000000 R11: 0000000000000246 R12: 00007fff06d81260 R13: 00007fff06d7fb40 R14: 00007fff06d7fc30 R15: 000055e96140f0a0 Allocated by task 917: kasan_save_stack+0x19/0x40 __kasan_kmalloc+0x7f/0xa0 __kmalloc_node+0x139/0x280 fq_pie_init+0x555/0x8e8 [sch_fq_pie] qdisc_create+0x407/0x11b0 tc_modify_qdisc+0x3c2/0x17e0 rtnetlink_rcv_msg+0x346/0x8e0 netlink_rcv_skb+0x120/0x380 netlink_unicast+0x439/0x630 netlink_sendmsg+0x719/0xbf0 sock_sendmsg+0xe2/0x110 ____sys_sendmsg+0x5ba/0x890 ___sys_sendmsg+0xe9/0x160 __sys_sendmsg+0xd3/0x170 do_syscall_64+0x3c/0x80 entry_SYSCALL_64_after_hwframe+0x44/0xae The buggy address belongs to the object at ffff888171306800 which belongs to the cache kmalloc-256 of size 256 The buggy address is located 36 bytes to the right of 256-byte region [ffff888171306800, ffff888171306900) The buggy address belongs to the page: page:00000000bcfb624e refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x171306 head:00000000bcfb624e order:1 compound_mapcount:0 flags: 0x17ffffc0010200(slablheadlnode=0lzone=2llastcpupid=0x1fffff) raw: 0017ffffc0010200 dead000000000100 dead000000000122 ffff888100042b40 raw: 0000000000000000 0000000000100010 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff888171306800: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ffff888171306880: 00 00 00 00 00 00 00 00 00 00 00 00 00 fc fc fc >ffff888171306900: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ^ ffff888171306980: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ffff888171306a00: fa fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fix fq_pie traffic path to avoid selecting 'q->flows + q->flows_cnt' as a valid flow: it's an address beyond the allocated memory.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47174	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_set_pipapo_avx2: Add irq_fpu_usable() check, fallback to non-AVX2 version Arturo reported this backtrace: [709732.358791] WARNING: CPU: 3 PID: 456 at arch/x86/kernel/fpu/core.c:128 kernel_fpu_begin_mask+0xae/0xe0 [709732.358793] Modules linked in: binfmt_misc nft_nat nft_chain_nat nf_nat nft_counter nft_ct nf_tables nf_conntrack_netlink nfnetlink 8021q garp stp mrp llc vrf intel_rapl_msr intel_rapl_common skx_edac nfit libnvdimm ipmi_ssif x86_pkg_temp_thermal intel_powerclamp coretemp crc32_pclmul mgag200 ghash_clmulni_intel drm_kms_helper cec aesni_intel drm libaes crypto_simd cryptd glue_helper mei_me dell_smbios iTCO_wdt evdev intel_pmc_bxt iTCO_vendor_support dcdbas pcspkr rapl dell_wmi_descriptor wmi_bmof sg i2c_algo_bit watchdog mei acpi_ipmi ipmi_si button nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 ipmi_devintf ipmi_msghandler ip_tables x_tables autofs4 ext4 crc16 mbcache jbd2 dm_mod raid10 raid456 async_raid6_recov async_memcpy async_pq async_xor async_tx xor sd_mod t10_pi crc_t10dif crct10dif_generic raid6_pq libcrc32c crc32c_generic raid1 raid0 multipath linear md_mod ahci libahci tg3 libata xhci_pci libphy xhci_hcd ptp usbcore crct10dif_pclmul crct10dif_common bnxt_en crc32c_intel scsi_mod [709732.358941] pps_core i2c_i801 lpc_ich i2c_smbus wmi usb_common [709732.358957] CPU: 3 PID: 456 Comm: jbd2/dm-0-8 Not tainted 5.10.0-0.bpo.5-amd64 #1 Debian 5.10.24-1~bpo10+1 [709732.358959] Hardware name: Dell Inc. PowerEdge R440/04JN2K, BIOS 2.9.3 09/23/2020 [709732.358964] RIP: 0010:kernel_fpu_begin_mask+0xae/0xe0 [709732.358969] Code: ae 54 24 04 83 e3 01 75 38 48 8b 44 24 08 65 48 33 04 25 28 00 00 00 75 33 48 83 c4 10 5b c3 65 8a 05 5e 21 5e 76 84 c0 74 92 <0f> 0b eb 8e f0 80 4f 01 40 48 81 c7 00 14 00 00 e8 dd fb ff ff eb [709732.358972] RSP: 0018:ffffbb9700304740 EFLAGS: 00010202 [709732.358976] RAX: 0000000000000001 RBX: 0000000000000003 RCX: 0000000000000001 [709732.358979] RDX: ffffbb9700304970 RSI: ffff922fe1952e00 RDI: 0000000000000003 [709732.358981] RBP: ffffbb9700304970 R08: ffff922fc868a600 R09: ffff922fc711e462 [709732.358984] R10: 000000000000005f R11: ffff922ff0b27180 R12: ffffbb9700304960 [709732.358987] R13: ffffbb9700304b08 R14: ffff922fc664b6c8 R15: ffff922fc664b660 [709732.358990] FS: 0000000000000000(0000) GS:ffff92371fec0000(0000) knlGS:0000000000000000 [709732.358993] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [709732.358996] CR2: 0000557a6655bdd0 CR3: 000000026020a001 CR4: 00000000007706e0 [709732.358999] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [709732.359001] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [709732.359003] PKRU: 55555554 [709732.359005] Call Trace: [709732.359009] <IRQ> [709732.359035] nft_pipapo_avx2_lookup+0x4c/0x1cba [nf_tables] [709732.359046] ? sched_clock+0x5/0x10 [709732.359054] ? sched_clock_cpu+0xc/0xb0 [709732.359061] ? record_times+0x16/0x80 [709732.359068] ? plist_add+0xc1/0x100 [709732.359073] ? psi_group_change+0x47/0x230 [709732.359079] ? skb_clone+0x4d/0xb0 [709732.359085] ? enqueue_task_rt+0x22b/0x310 [709732.359098] ? bnxt_start_xmit+0x1e8/0xaf0 [bnxt_en] [709732.359102] ? packet_rcv+0x40/0x4a0 [709732.359121] nft_lookup_eval+0x59/0x160 [nf_tables] [709732.359133] nft_do_chain+0x350/0x500 [nf_tables] [709732.359152] ? nft_lookup_eval+0x59/0x160 [nf_tables] [709732.359163] ? nft_do_chain+0x364/0x500 [nf_tables] [709732.359172] ? fib4_rule_action+0x6d/0x80 [709732.359178] ? fib_rules_lookup+0x107/0x250 [709732.359184] nft_nat_do_chain+0x8a/0xf2 [nft_chain_nat] [709732.359193] nf_nat_inet_fn+0xea/0x210 [nf_nat] [709732.359202] nf_nat_ipv4_out+0x14/0xa0 [nf_nat] [709732.359207] nf_hook_slow+0x44/0xc0 [709732.359214] ip_output+0xd2/0x100 [709732.359221] ? __ip_finish_output+0x210/0x210 [709732.359226] ip_forward+0x37d/0x4a0 [709732.359232] ? ip4_key_hashfn+0xb0/0xb0 [709732.359238] ip_subli ---truncated---	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47170	In the Linux kernel, the following vulnerability has been resolved: USB: usbfs: Don't WARN about excessively large memory allocations Syzbot found that the kernel generates a WARNing if the user tries to submit a bulk transfer through usbfs with a buffer that is way too large. This isn't a bug in the kernel; it's merely an invalid request from the user and the usbfs code does handle it correctly. In theory the same thing can happen with async transfers, or with the packet descriptor table for isochronous transfers. To prevent the MM subsystem from complaining about these bad allocation requests, add the __GFP_NOWARN flag to the kmalloc calls for these buffers.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47169	In the Linux kernel, the following vulnerability has been resolved: serial: rp2: use 'request_firmware' instead of 'request_firmware_nowait' In 'rp2_probe', the driver registers 'rp2_uart_interrupt' then calls 'rp2_fw_cb' through 'request_firmware_nowait'. In 'rp2_fw_cb', if the firmware don't exists, function just return without initializing ports of 'rp2_card'. But now the interrupt handler function has been registered, and when an interrupt comes, 'rp2_uart_interrupt' may access those ports then causing NULL pointer dereference or other bugs. Because the driver does some initialization work in 'rp2_fw_cb', in order to make the driver ready to handle interrupts, 'request_firmware' should be used instead of asynchronous 'request_firmware_nowait'. This report reveals it: INFO: trying to register non-static key. the code is fine but needs lockdep annotation. turning off the locking correctness validator. CPU: 2 PID: 0 Comm: swapper/2 Not tainted 4.19.177-gdba4159c14ef-dirty #45 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.12.0-59- gc9ba5276e321-prebuilt.qemu.org 04/01/2014 Call Trace: <IRQ> __dump_stack lib/dump_stack.c:77 [inline] dump_stack+0xec/0x156 lib/dump_stack.c:118 assign_lock_key kernel/locking/lockdep.c:727 [inline] register_lock_class+0x14e5/0x1ba0 kernel/locking/lockdep.c:753 __lock_acquire+0x187/0x3750 kernel/locking/lockdep.c:3303 lock_acquire+0x124/0x340 kernel/locking/lockdep.c:3907 __raw_spin_lock include/linux/spinlock_api_smp.h:142 [inline] _raw_spin_lock+0x32/0x50 kernel/locking/spinlock.c:144 spin_lock include/linux/spinlock.h:329 [inline] rp2_ch_interrupt drivers/tty/serial/rp2.c:466 [inline] rp2_asic_interrupt.isra.9+0x15d/0x990 drivers/tty/serial/rp2.c:493 rp2_uart_interrupt+0x49/0xe0 drivers/tty/serial/rp2.c:504 __handle_irq_event_percpu+0xfb/0x770 kernel/irq/handle.c:149 handle_irq_event_percpu+0x79/0x150 kernel/irq/handle.c:189 handle_irq_event+0xac/0x140 kernel/irq/handle.c:206 handle_fasteoi_irq+0x232/0x5c0 kernel/irq/chip.c:725 generic_handle_irq_desc include/linux/irqdesc.h:155 [inline] handle_irq+0x230/0x3a0 arch/x86/kernel/irq_64.c:87 do_IRQ+0xa7/0x1e0 arch/x86/kernel/irq.c:247 common_interrupt+0xf/0xf arch/x86/entry/entry_64.S:670 </IRQ> RIP: 0010:native_safe_halt+0x28/0x30 arch/x86/include/asm/irqflags.h:61 Code: 00 00 55 be 04 00 00 00 48 c7 c7 00 c2 2f 8c 48 89 e5 e8 fb 31 e7 f8 8b 05 75 af 8d 03 85 c0 7e 07 0f 00 2d 8a 61 65 00 fb f4 <5d> c3 90 90 90 90 90 90 0f 1f 44 00 00 55 48 89 e5 41 57 41 56 41 RSP: 0018:ffff88806b71fcc8 EFLAGS: 00000246 ORIG_RAX: ffffffffffffffde RAX: 0000000000000000 RBX: ffffffff8bde7e48 RCX: ffffffff88a21285 RDX: 0000000000000000 RSI: 0000000000000004 RDI: ffffffff8c2fc200 RBP: ffff88806b71fcc8 R08: fffffbfff185f840 R09: fffffbfff185f840 R10: 0000000000000001 R11: fffffbfff185f840 R12: 0000000000000002 R13: ffffffff8bea18a0 R14: 0000000000000000 R15: 0000000000000000 arch_safe_halt arch/x86/include/asm/paravirt.h:94 [inline] default_idle+0x6f/0x360 arch/x86/kernel/process.c:557 arch_cpu_idle+0xf/0x20 arch/x86/kernel/process.c:548 default_idle_call+0x3b/0x60 kernel/sched/idle.c:93 cpuidle_idle_call kernel/sched/idle.c:153 [inline] do_idle+0x2ab/0x3c0 kernel/sched/idle.c:263 cpu_startup_entry+0xcb/0xe0 kernel/sched/idle.c:369 start_secondary+0x3b8/0x4e0 arch/x86/kernel/smpboot.c:271 secondary_startup_64+0xa4/0xb0 arch/x86/kernel/head_64.S:243 BUG: unable to handle kernel NULL pointer dereference at 0000000000000010 PGD 8000000056d27067 P4D 8000000056d27067 PUD 56d28067 PMD 0 Oops: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 2 PID: 0 Comm: swapper/2 Not tainted 4.19.177-gdba4159c14ef-dirty #45 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.12.0-59- gc9ba5276e321-prebuilt.qemu.org 04/01/2014 RIP: 0010:readl arch/x86/include/asm/io.h:59 [inline] RIP: 0010:rp2_ch_interrupt drivers/tty/serial/rp2.c:472 [inline] RIP: 0010:rp2_asic_interrupt.isra.9+0x181/0x990 drivers/tty/serial/rp2.c: 493 Co ---truncated---	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47168	In the Linux kernel, the following vulnerability has been resolved: NFS: fix an incorrect limit in filelayout_decode_layout() The "sizeof(struct nfs_fh)" is two bytes too large and could lead to memory corruption. It should be NFS_MAXFHSIZE because that's the size of the ->data[] buffer. I reversed the size of the arguments to put the variable on the left.	N/A	More Details
CVE-2021-47167	In the Linux kernel, the following vulnerability has been resolved: NFS: Fix an Oopsable condition in __nfs_pageio_add_request() Ensure that nfs_pageio_error_cleanup() resets the mirror array contents, so that the structure reflects the fact that it is now empty. Also change the test in nfs_pageio_do_add_request() to be more robust by checking whether or not the list is empty rather than relying on the value of pg_count.	N/A	More Details
CVE-2021-47166	In the Linux kernel, the following vulnerability has been resolved: NFS: Don't corrupt the value of pg_bytes_written in nfs_do_recoalesce() The value of mirror->pg_bytes_written should only be updated after a successful attempt to flush out the requests on the list.	N/A	More Details
CVE-2024-1992	Rejected reason: Rejected as duplicate of CVE-2024-2306	N/A	More Details
CVE-2021-47165	In the Linux kernel, the following vulnerability has been resolved: drm/meson: fix shutdown crash when component not probed When main component is not probed, by example when the dw-hdmi module is not loaded yet or in probe defer, the following crash appears on shutdown: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000038 ... pc : meson_drv_shutdown+0x24/0x50 lr : platform_drv_shutdown+0x20/0x30 ... Call trace: meson_drv_shutdown+0x24/0x50 platform_drv_shutdown+0x20/0x30 device_shutdown+0x158/0x360 kernel_restart_prepare+0x38/0x48 kernel_restart+0x18/0x68 __do_sys_reboot+0x224/0x250 __arm64_sys_reboot+0x24/0x30 ... Simply check if the priv struct has been allocated before using it.	N/A	More Details
CVE-2021-47163	In the Linux kernel, the following vulnerability has been resolved: tipc: wait and exit until all work queues are done On some host, a crash could be triggered simply by repeating these commands several times: # modprobe tipc # tipc bearer enable media udp name UDP1 localip 127.0.0.1 # rmmod tipc [] BUG: unable to handle kernel paging request at ffffffffc096bb00 [] Workqueue: events 0xffffffffc096bb00 [] Call Trace: [] ? process_one_work+0x1a7/0x360 [] ? worker_thread+0x30/0x390 [] ? create_worker+0x1a0/0x1a0 [] ? kthread+0x116/0x130 [] ? kthread_flush_work_fn+0x10/0x10 [] ? ret_from_fork+0x35/0x40 When removing the TIPC module, the UDP tunnel sock will be delayed to release in a work queue as sock_release() can't be done in rtnl_lock(). If the work queue is schedule to run after the TIPC module is removed, kernel will crash as the work queue function cleanup_beareri() code no longer exists when trying to invoke it. To fix it, this patch introduce a member wq_count in tipc_net to track the numbers of work queues in schedule, and wait and exit until all work queues are done in tipc_exit_net().	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47178	In the Linux kernel, the following vulnerability has been resolved: scsi: target: core: Avoid smp_processor_id() in preemptible code The BUG message "BUG: using smp_processor_id() in preemptible [00000000] code" was observed for TCMU devices with kernel config DEBUG_PREEMPT. The message was observed when blktests block/005 was run on TCMU devices with fileio backend or user:zbc backend [1]. The commit 1130b499b4a7 ("scsi: target: tcm_loop: Use LIO wq cmd submission helper") triggered the symptom. The commit modified work queue to handle commands and changed 'current->nr_cpu_allowed' at smp_processor_id() call. The message was also observed at system shutdown when TCMU devices were not cleaned up [2]. The function smp_processor_id() was called in SCSI host work queue for abort handling, and triggered the BUG message. This symptom was observed regardless of the commit 1130b499b4a7 ("scsi: target: tcm_loop: Use LIO wq cmd submission helper"). To avoid the preemptible code check at smp_processor_id(), get CPU ID with raw_smp_processor_id() instead. The CPU ID is used for performance improvement then thread move to other CPU will not affect the code. [1] [56.468103] run blktests block/005 at 2021-05-12 14:16:38 [57.369473] check_preemption_disabled: 85 callbacks suppressed [57.369480] BUG: using smp_processor_id() in preemptible [00000000] code: fio/1511 [57.369506] BUG: using smp_processor_id() in preemptible [00000000] code: fio/1510 [57.369512] BUG: using smp_processor_id() in preemptible [00000000] code: fio/1506 [57.369552] caller is __target_init_cmd+0x157/0x170 [target_core_mod] [57.369606] CPU: 4 PID: 1506 Comm: fio Not tainted 5.13.0-rc1+ #34 [57.369613] Hardware name: System manufacturer System Product Name/PRIME Z270-A, BIOS 1302 03/15/2018 [57.369617] Call Trace: [57.369621] BUG: using smp_processor_id() in preemptible [00000000] code: fio/1507 [57.369628] dump_stack+0x6d/0x89 [57.369642] check_preemption_disabled+0xc8/0xd0 [57.369628] caller is __target_init_cmd+0x157/0x170 [target_core_mod] [57.369655] __target_init_cmd+0x157/0x170 [target_core_mod] [57.369695] target_init_cmd+0x76/0x90 [target_core_mod] [57.369732] tcm_loop_queuecommand+0x109/0x210 [tcm_loop] [57.369744] scsi_queue_rq+0x38e/0xc40 [57.369761] __blk_mq_try_issue_directly+0x109/0x1c0 [57.369779] blk_mq_try_issue_directly+0x43/0x90 [57.369790] blk_mq_submit_bio+0x4e5/0x5d0 [57.369812] submit_bio_noacct+0x46e/0x4e0 [57.369830] __blkdev_direct_IO_simple+0x1a3/0x2d0 [57.369859] ? set_init_blocksize.isra.0+0x60/0x60 [57.369880] generic_file_read_iter+0x89/0x160 [57.369898] blkdev_read_iter+0x44/0x60 [57.369906] new_sync_read+0x102/0x170 [57.369929] vfs_read+0xd4/0x160 [57.369941] __x64_sys_pread64+0x6e/0xa0 [57.369946] ? lockdep_hardirqs_on+0x79/0x100 [57.369958] do_syscall_64+0x3a/0x70 [57.369965] entry_SYSCALL_64_after_hwframe+0x44/0xae [57.369973] RIP: 0033:0x7f7ed4c1399f [57.369979] Code: 08 89 3c 24 48 89 4c 24 18 e8 7d f3 ff ff 4c 8b 54 24 18 48 8b 54 24 10 41 89 c0 48 8b 74 24 08 8b 3c 24 b8 11 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 31 44 89 c7 48 89 04 24 e8 cd f3 ff ff 48 8b [57.369983] RSP: 002b:00007ffd7918c580 EFLAGS: 00000293 ORIG_RAX: 0000000000000011 [57.369990] RAX: ffffffffffffffda RBX: 00000000015b4540 RCX: 00007f7ed4c1399f [57.369993] RDX: 0000000000001000 RSI: 00000000015de000 RDI: 0000000000000009 [57.369996] RBP: 00000000015b4540 R08: 0000000000000000 R09: 0000000000000001 [57.369999] R10: 0000000000e5c000 R11: 0000000000000293 R12: 00007f7eb5269a70 [57.370002] R13: 0000000000000000 R14: 0000000000001000 R15: 00000000015b4568 [57.370031] CPU: 7 PID: 1507 Comm: fio Not tainted 5.13.0-rc1+ #34 [57.370036] Hardware name: System manufacturer System Product Name/PRIME Z270-A, BIOS 1302 03/15/2018 [57.370039] Call Trace: [57.370045] dump_stack+0x6d/0x89 [57.370056] ch ---truncated---	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47160	In the Linux kernel, the following vulnerability has been resolved: net: dsa: mt7530: fix VLAN traffic leaks PCR_MATRIX field was set to all 1's when VLAN filtering is enabled, but was not reset when it is disabled, which may cause traffic leaks: ip link add br0 type bridge vlan_filtering 1 ip link add br1 type bridge vlan_filtering 1 ip link set swp0 master br0 ip link set swp1 master br1 ip link set br0 type bridge vlan_filtering 0 ip link set br1 type bridge vlan_filtering 0 # traffic in br0 and br1 will start leaking to each other As port_bridge_{add,del} have set up PCR_MATRIX properly, remove the PCR_MATRIX write from mt7530_port_set_vlan_aware.	N/A	More Details
CVE-2023-52621	In the Linux kernel, the following vulnerability has been resolved: bpf: Check rcu_read_lock_trace_held() before calling bpf map helpers These three bpf_map_{lookup,update,delete}_elem() helpers are also available for sleepable bpf program, so add the corresponding lock assertion for sleepable bpf program, otherwise the following warning will be reported when a sleepable bpf program manipulates bpf map under interpreter mode (aka bpf_jit_enable=0): WARNING: CPU: 3 PID: 4985 at kernel/bpf/helpers.c:40 ..... CPU: 3 PID: 4985 Comm: test_progs Not tainted 6.6.0+ #2 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996) ..... RIP: 0010:bpf_map_lookup_elem+0x54/0x60 ..... Call Trace: <TASK> ? __warn+0xa5/0x240 ? bpf_map_lookup_elem+0x54/0x60 ? report_bug+0x1ba/0x1f0 ? handle_bug+0x40/0x80 ? exc_invalid_op+0x18/0x50 ? asm_exc_invalid_op+0x1b/0x20 ? __pfx_bpf_map_lookup_elem+0x10/0x10 ? rcu_lockdep_current_cpu_online+0x65/0xb0 ? rcu_is_watching+0x23/0x50 ? bpf_map_lookup_elem+0x54/0x60 ? __pfx_bpf_map_lookup_elem+0x10/0x10 ___bpf_prog_run+0x513/0x3b70 __bpf_prog_run32+0x9d/0xd0 ? __bpf_prog_enter_sleepable_recur+0xad/0x120 ? __bpf_prog_enter_sleepable_recur+0x3e/0x120 bpf_trampoline_6442580665+0x4d/0x1000 __x64_sys_getpgid+0x5/0x30 ? do_syscall_64+0x36/0xb0 entry_SYSCALL_64_after_hwframe+0x6e/0x76 </TASK>	N/A	More Details
CVE-2023-52622	In the Linux kernel, the following vulnerability has been resolved: ext4: avoid online resizing failures due to oversized flex bg When we online resize an ext4 filesystem with a oversized flexbg_size, mkfs.ext4 -F -G 67108864 $dev -b 4096 100M mount $dev $dir resize2fs $dev 16G the following WARN_ON is triggered: == WARNING: CPU: 0 PID: 427 at mm/page_alloc.c:4402 __alloc_pages+0x411/0x550 Modules linked in: sg(E) CPU: 0 PID: 427 Comm: resize2fs Tainted: G E 6.6.0-rc5+ #314 RIP: 0010:__alloc_pages+0x411/0x550 Call Trace: <TASK> __kmalloc_large_node+0xa2/0x200 __kmalloc+0x16e/0x290 ext4_resize_fs+0x481/0xd80 __ext4_ioctl+0x1616/0x1d90 ext4_ioctl+0x12/0x20 __x64_sys_ioctl+0xf0/0x150 do_syscall_64+0x3b/0x90 == This is because flexbg_size is too large and the size of the new_group_data array to be allocated exceeds MAX_ORDER. Currently, the minimum value of MAX_ORDER is 8, the minimum value of PAGE_SIZE is 4096, the corresponding maximum number of groups that can be allocated is: (PAGE_SIZE << MAX_ORDER) / sizeof(struct ext4_new_group_data) ≈ 21845 And the value that is down-aligned to the power of 2 is 16384. Therefore, this value is defined as MAX_RESIZE_BG, and the number of groups added each time does not exceed this value during resizing, and is added multiple times to complete the online resizing. The difference is that the metadata in a flex_bg may be more dispersed.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52624	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Wake DMCUB before executing GPINT commands [Why] DMCUB can be in idle when we attempt to interface with the HW through the GPINT mailbox resulting in a system hang. [How] Add dc_wake_and_execute_gpint() to wrap the wake, execute, sleep sequence. If the GPINT executes successfully then DMCUB will be put back into sleep after the optional response is returned. It functions similar to the inbox command interface.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47136	In the Linux kernel, the following vulnerability has been resolved: net: zero-initialize tc skb extension on allocation Function skb_ext_add() doesn't initialize created skb extension with any value and leaves it up to the user. However, since extension of type TC_SKB_EXT originally contained only single value tc_skb_ext->chain its users used to just assign the chain value without setting whole extension memory to zero first. This assumption changed when TC_SKB_EXT extension was extended with additional fields but not all users were updated to initialize the new fields which leads to use of uninitialized memory afterwards. UBSAN log: [778.299821] UBSAN: invalid-load in net/openvswitch/flow.c:899:28 [778.301495] load of value 107 is not a valid value for type '_Bool' [778.303215] CPU: 0 PID: 0 Comm: swapper/0 Not tainted 5.12.0-rc7+ #2 [778.304933] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 [778.307901] Call Trace: [778.308680] <IRQ> [778.309358] dump_stack+0xbb/0x107 [778.310307] ubsan_epilogue+0x5/0x40 [778.311167] __ubsan_handle_load_invalid_value.cold+0x43/0x48 [778.312454] ? memset+0x20/0x40 [778.313230] ovs_flow_key_extract.cold+0xf/0x14 [openvswitch] [778.314532] ovs_vport_receive+0x19e/0x2e0 [openvswitch] [778.315749] ? ovs_vport_find_upcall_portid+0x330/0x330 [openvswitch] [778.317188] ? create_prof_cpu_mask+0x20/0x20 [778.318220] ? arch_stack_walk+0x82/0xf0 [778.319153] ? secondary_startup_64_no_verify+0xb0/0xbb [778.320399] ? stack_trace_save+0x91/0xc0 [778.321362] ? stack_trace_consume_entry+0x160/0x160 [778.322517] ? lock_release+0x52e/0x760 [778.323444] netdev_frame_hook+0x323/0x610 [openvswitch] [778.324668] ? ovs_netdev_get_vport+0xe0/0xe0 [openvswitch] [778.325950] __netif_receive_skb_core+0x771/0x2db0 [778.327067] ? lock_downgrade+0x6e0/0x6f0 [778.328021] ? lock_acquire+0x565/0x720 [778.328940] ? generic_xdp_tx+0x4f0/0x4f0 [778.329902] ? inet_gro_receive+0x2a7/0x10a0 [778.330914] ? lock_downgrade+0x6f0/0x6f0 [778.331867] ? udp4_gro_receive+0x4c4/0x13e0 [778.332876] ? lock_release+0x52e/0x760 [778.333808] ? dev_gro_receive+0xcc8/0x2380 [778.334810] ? lock_downgrade+0x6f0/0x6f0 [778.335769] __netif_receive_skb_list_core+0x295/0x820 [778.336955] ? process_backlog+0x780/0x780 [778.337941] ? mlx5e_rep_tc_netdevice_event_unregister+0x20/0x20 [mlx5_core] [778.339613] ? seqcount_lockdep_reader_access.constprop.0+0xa7/0xc0 [778.341033] ? kvm_clock_get_cycles+0x14/0x20 [778.342072] netif_receive_skb_list_internal+0x5f5/0xcb0 [778.343288] ? __kasan_kmalloc+0x7a/0x90 [778.344234] ? mlx5e_handle_rx_cqe_mpwrq+0x9e0/0x9e0 [mlx5_core] [778.345676] ? mlx5e_xmit_xdp_frame_mpwqe+0x14d0/0x14d0 [mlx5_core] [778.347140] ? __netif_receive_skb_list_core+0x820/0x820 [778.348351] ? mlx5e_post_rx_mpwqes+0xa6/0x25d0 [mlx5_core] [778.349688] ? napi_gro_flush+0x26c/0x3c0 [778.350641] napi_complete_done+0x188/0x6b0 [778.351627] mlx5e_napi_poll+0x373/0x1b80 [mlx5_core] [778.352853] __napi_poll+0x9f/0x510 [778.353704] ? mlx5_flow_namespace_set_mode+0x260/0x260 [mlx5_core] [778.355158] net_rx_action+0x34c/0xa40 [778.356060] ? napi_threaded_poll+0x3d0/0x3d0 [778.357083] ? sched_clock_cpu+0x18/0x190 [778.358041] ? __common_interrupt+0x8e/0x1a0 [778.359045] __do_softirq+0x1ce/0x984 [778.359938] __irq_exit_rcu+0x137/0x1d0 [778.360865] irq_exit_rcu+0xa/0x20 [778.361708] common_interrupt+0x80/0xa0 [778.362640] </IRQ> [778.363212] asm_common_interrupt+0x1e/0x40 [778.364204] RIP: 0010:native_safe_halt+0xe/0x10 [778.365273] Code: 4f ff ff ff 4c 89 e7 e8 50 3f 40 fe e9 dc fe ff ff 48 89 df e8 43 3f 40 fe eb 90 cc e9 07 00 00 00 0f 00 2d 74 05 62 00 fb f4 <c3> 90 e9 07 00 00 00 0f 00 2d 64 05 62 00 f4 c3 cc cc 0f 1f 44 00 [778.369355] RSP: 0018:ffffffff84407e48 EFLAGS: 00000246 [778.370570] RAX ---truncated---	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52625	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Refactor DMCUB enter/exit idle interface [Why] We can hang in place trying to send commands when the DMCUB isn't powered on. [How] We need to exit out of the idle state prior to sending a command, but the process that performs the exit also invokes a command itself. Fixing this issue involves the following: 1. Using a software state to track whether or not we need to start the process to exit idle or notify idle. It's possible for the hardware to have exited an idle state without driver knowledge, but entering one is always restricted to a driver allow - which makes the SW state vs HW state mismatch issue purely one of optimization, which should seldomly be hit, if at all. 2. Refactor any instances of exit/notify idle to use a single wrapper that maintains this SW state. This works simialr to dc_allow_idle_optimizations, but works at the DMCUB level and makes sure the state is marked prior to any notify/exit idle so we don't enter an infinite loop. 3. Make sure we exit out of idle prior to sending any commands or waiting for DMCUB idle. This patch takes care of 1/2. A future patch will take care of wrapping DMCUB command submission with calls to this new interface.	N/A	More Details
CVE-2023-52626	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix operation precedence bug in port timestamping napi_poll context Indirection (*) is of lower precedence than postfix increment (++). Logic in napi_poll context would cause an out-of-bound read by first increment the pointer address by byte address space and then dereference the value. Rather, the intended logic was to dereference first and then increment the underlying value.	N/A	More Details
CVE-2021-47152	In the Linux kernel, the following vulnerability has been resolved: mptcp: fix data stream corruption Maxim reported several issues when forcing a TCP transparent proxy to use the MPTCP protocol for the inbound connections. He also provided a clean reproducer. The problem boils down to 'mptcp_frag_can_collapse_to()' assuming that only MPTCP will use the given page_frag. If others - e.g. the plain TCP protocol - allocate page fragments, we can end-up re-using already allocated memory for mptcp_data_frag. Fix the issue ensuring that the to-be-expanded data fragment is located at the current page frag end. v1 -> v2: - added missing fixes tag (Mat)	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26645	In the Linux kernel, the following vulnerability has been resolved: tracing: Ensure visibility when inserting an element into tracing_map Running the following two commands in parallel on a multi-processor AArch64 machine can sporadically produce an unexpected warning about duplicate histogram entries: $ while true; do echo hist:key=id.syscall:val=hitcount > \ /sys/kernel/debug/tracing/events/raw_syscalls/sys_enter/trigger cat /sys/kernel/debug/tracing/events/raw_syscalls/sys_enter/hist sleep 0.001 done $ stress-ng --sysbadaddr $(nproc) The warning looks as follows: [2911.172474] ------------[cut here]------------ [2911.173111] Duplicates detected: 1 [2911.173574] WARNING: CPU: 2 PID: 12247 at kernel/trace/tracing_map.c:983 tracing_map_sort_entries+0x3e0/0x408 [2911.174702] Modules linked in: iscsi_ibft(E) iscsi_boot_sysfs(E) rfkill(E) af_packet(E) nls_iso8859_1(E) nls_cp437(E) vfat(E) fat(E) ena(E) tiny_power_button(E) qemu_fw_cfg(E) button(E) fuse(E) efi_pstore(E) ip_tables(E) x_tables(E) xfs(E) libcrc32c(E) aes_ce_blk(E) aes_ce_cipher(E) crct10dif_ce(E) polyval_ce(E) polyval_generic(E) ghash_ce(E) gf128mul(E) sm4_ce_gcm(E) sm4_ce_ccm(E) sm4_ce(E) sm4_ce_cipher(E) sm4(E) sm3_ce(E) sm3(E) sha3_ce(E) sha512_ce(E) sha512_arm64(E) sha2_ce(E) sha256_arm64(E) nvme(E) sha1_ce(E) nvme_core(E) nvme_auth(E) t10_pi(E) sg(E) scsi_mod(E) scsi_common(E) efivarfs(E) [2911.174738] Unloaded tainted modules: cppc_cpufreq(E):1 [2911.180985] CPU: 2 PID: 12247 Comm: cat Kdump: loaded Tainted: G E 6.7.0-default #2 1b58bbb22c97e4399dc09f92d309344f69c44a01 [2911.182398] Hardware name: Amazon EC2 c7g.8xlarge/, BIOS 1.0 11/1/2018 [2911.183208] pstate: 61400005 (nZCv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=--) [2911.184038] pc : tracing_map_sort_entries+0x3e0/0x408 [2911.184667] lr : tracing_map_sort_entries+0x3e0/0x408 [2911.185310] sp : ffff8000a1513900 [2911.185750] x29: ffff8000a1513900 x28: ffff0003f272fe80 x27: 0000000000000001 [2911.186600] x26: ffff0003f272fe80 x25: 0000000000000030 x24: 0000000000000008 [2911.187458] x23: ffff0003c5788000 x22: ffff0003c16710c8 x21: ffff80008017f180 [2911.188310] x20: ffff80008017f000 x19: ffff80008017f180 x18: ffffffffffffffff [2911.189160] x17: 0000000000000000 x16: 0000000000000000 x15: ffff8000a15134b8 [2911.190015] x14: 0000000000000000 x13: 205d373432323154 x12: 5b5d313131333731 [2911.190844] x11: 00000000fffeffff x10: 00000000fffeffff x9 : ffffd1b78274a13c [2911.191716] x8 : 000000000017ffe8 x7 : c0000000fffeffff x6 : 000000000057ffa8 [2911.192554] x5 : ffff0012f6c24ec0 x4 : 0000000000000000 x3 : ffff2e5b72b5d000 [2911.193404] x2 : 0000000000000000 x1 : 0000000000000000 x0 : ffff0003ff254480 [2911.194259] Call trace: [2911.194626] tracing_map_sort_entries+0x3e0/0x408 [2911.195220] hist_show+0x124/0x800 [2911.195692] seq_read_iter+0x1d4/0x4e8 [2911.196193] seq_read+0xe8/0x138 [2911.196638] vfs_read+0xc8/0x300 [2911.197078] ksys_read+0x70/0x108 [2911.197534] __arm64_sys_read+0x24/0x38 [2911.198046] invoke_syscall+0x78/0x108 [2911.198553] el0_svc_common.constprop.0+0xd0/0xf8 [2911.199157] do_el0_svc+0x28/0x40 [2911.199613] el0_svc+0x40/0x178 [2911.200048] el0t_64_sync_handler+0x13c/0x158 [2911.200621] el0t_64_sync+0x1a8/0x1b0 [2911.201115] ---[end trace 0000000000000000]--- The problem appears to be caused by CPU reordering of writes issued from __tracing_map_insert(). The check for the presence of an element with a given key in this function is: val = READ_ONCE(entry->val); if (val && keys_match(key, val->key, map->key_size)) ... The write of a new entry is: elt = get_free_elt(map); memcpy(elt->key, key, map->key_size); entry->val = elt; The "memcpy(elt->key, key, map->key_size);" and "entry->val = elt;" stores may become visible in the reversed order on another CPU. This second CPU might then incorrectly determine that a new key doesn't match an already present val->key and subse ---truncated---	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26646	In the Linux kernel, the following vulnerability has been resolved: thermal: intel: hfi: Add syscore callbacks for system-wide PM The kernel allocates a memory buffer and provides its location to the hardware, which uses it to update the HFI table. This allocation occurs during boot and remains constant throughout runtime. When resuming from hibernation, the restore kernel allocates a second memory buffer and reprograms the HFI hardware with the new location as part of a normal boot. The location of the second memory buffer may differ from the one allocated by the image kernel. When the restore kernel transfers control to the image kernel, its HFI buffer becomes invalid, potentially leading to memory corruption if the hardware writes to it (the hardware continues to use the buffer from the restore kernel). It is also possible that the hardware "forgets" the address of the memory buffer when resuming from "deep" suspend. Memory corruption may also occur in such a scenario. To prevent the described memory corruption, disable HFI when preparing to suspend or hibernate. Enable it when resuming. Add syscore callbacks to handle the package of the boot CPU (packages of non-boot CPUs are handled via CPU offline). Syscore ops always run on the boot CPU. Additionally, HFI only needs to be disabled during "deep" suspend and hibernation. Syscore ops only run in these cases. [rjw: Comment adjustment, subject and changelog edits]	N/A	More Details
CVE-2024-26647	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix late derefrence 'dsc' check in 'link_set_dsc_pps_packet()' In link_set_dsc_pps_packet(), 'struct display_stream_compressor *dsc' was dereferenced in a DC_LOGGER_INIT(dsc->ctx->logger); before the 'dsc' NULL pointer check. Fixes the below: drivers/gpu/drm/amd/amdgpu/../display/dc/link/link_dpms.c:905 link_set_dsc_pps_packet() warn: variable dereferenced before check 'dsc' (see line 903)	N/A	More Details
CVE-2021-47143	In the Linux kernel, the following vulnerability has been resolved: net/smc: remove device from smcd_dev_list after failed device_add() If the device_add() for a smcd_dev fails, there's no cleanup step that rolls back the earlier list_add(). The device subsequently gets freed, and we end up with a corrupted list. Add some error handling that removes the device from the list.	N/A	More Details
CVE-2024-26649	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix the null pointer when load rlc firmware If the RLC firmware is invalid because of wrong header size, the pointer to the rlc firmware is released in function amdgpu_ucode_request. There will be a null pointer error in subsequent use. So skip validation to fix it.	N/A	More Details
CVE-2024-26650	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-29419	There is a Cross-site scripting (XSS) vulnerability in the Wireless settings under the Easy Setup Page of TOTOLINK X2000R before v1.0.0-B20231213.1013.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47139	In the Linux kernel, the following vulnerability has been resolved: net: hns3: put off calling register_netdev() until client initialize complete Currently, the netdevice is registered before client initializing complete. So there is a timewindow between netdevice available and usable. In this case, if user try to change the channel number or ring param, it may cause the hns3_set_rx_cpu_rmap() being called twice, and report bug. [47199.416502] hns3 0000:35:00.0 eth1: set channels: tqp_num=1, rxfh=0 [47199.430340] hns3 0000:35:00.0 eth1: already uninitialized [47199.438554] hns3 0000:35:00.0: rss changes from 4 to 1 [47199.511854] hns3 0000:35:00.0: Channels changed, rss_size from 4 to 1, tqps from 4 to 1 [47200.163524] ------------[cut here]------------ [47200.171674] kernel BUG at lib/cpu_rmap.c:142! [47200.177847] Internal error: Oops - BUG: 0 [#1] PREEMPT SMP [47200.185259] Modules linked in: hclge(+) hns3(-) hns3_cae(O) hns_roce_hw_v2 hnae3 vfio_iommu_type1 vfio_pci vfio_virqfd vfio pv680_mii(O) [last unloaded: hclge] [47200.205912] CPU: 1 PID: 8260 Comm: ethtool Tainted: G O 5.11.0-rc3+ #1 [47200.215601] Hardware name: , xxxxxx 02/04/2021 [47200.223052] pstate: 60400009 (nZCv daif +PAN -UAO -TCO BTYPE=--) [47200.230188] pc : cpu_rmap_add+0x38/0x40 [47200.237472] lr : irq_cpu_rmap_add+0x84/0x140 [47200.243291] sp : ffff800010e93a30 [47200.247295] x29: ffff800010e93a30 x28: ffff082100584880 [47200.254155] x27: 0000000000000000 x26: 0000000000000000 [47200.260712] x25: 0000000000000000 x24: 0000000000000004 [47200.267241] x23: ffff08209ba03000 x22: ffff08209ba038c0 [47200.273789] x21: 000000000000003f x20: ffff0820e2bc1680 [47200.280400] x19: ffff0820c970ec80 x18: 00000000000000c0 [47200.286944] x17: 0000000000000000 x16: ffffb43debe4a0d0 [47200.293456] x15: ffffc2082990600 x14: dead000000000122 [47200.300059] x13: ffffffffffffffff x12: 000000000000003e [47200.306606] x11: ffff0820815b8080 x10: ffff53e411988000 [47200.313171] x9 : 0000000000000000 x8 : ffff0820e2bc1700 [47200.319682] x7 : 0000000000000000 x6 : 000000000000003f [47200.326170] x5 : 0000000000000040 x4 : ffff800010e93a20 [47200.332656] x3 : 0000000000000004 x2 : ffff0820c970ec80 [47200.339168] x1 : ffff0820e2bc1680 x0 : 0000000000000004 [47200.346058] Call trace: [47200.349324] cpu_rmap_add+0x38/0x40 [47200.354300] hns3_set_rx_cpu_rmap+0x6c/0xe0 [hns3] [47200.362294] hns3_reset_notify_init_enet+0x1cc/0x340 [hns3] [47200.370049] hns3_change_channels+0x40/0xb0 [hns3] [47200.376770] hns3_set_channels+0x12c/0x2a0 [hns3] [47200.383353] ethtool_set_channels+0x140/0x250 [47200.389772] dev_ethtool+0x714/0x23d0 [47200.394440] dev_ioctl+0x4cc/0x640 [47200.399277] sock_do_ioctl+0x100/0x2a0 [47200.404574] sock_ioctl+0x28c/0x470 [47200.409079] __arm64_sys_ioctl+0xb4/0x100 [47200.415217] el0_svc_common.constprop.0+0x84/0x210 [47200.422088] do_el0_svc+0x28/0x34 [47200.426387] el0_svc+0x28/0x70 [47200.431308] el0_sync_handler+0x1a4/0x1b0 [47200.436477] el0_sync+0x174/0x180 [47200.441562] Code: 11000405 79000c45 f8247861 d65f03c0 (d4210000) [47200.448869] ---[end trace a01efe4ce42e5f34]--- The process is like below: excuting hns3_client_init l register_netdev() l hns3_set_channels() l l hns3_set_rx_cpu_rmap() hns3_reset_notify_uninit_enet() l l l quit without calling function l hns3_free_rx_cpu_rmap for flag l HNS3_NIC_STATE_INITED is unset. l l l hns3_reset_notify_init_enet() l l set HNS3_NIC_STATE_INITED call hns3_set_rx_cpu_rmap()-- crash Fix it by calling register_netdev() at the end of function hns3_client_init().	N/A	More Details
CVE-2021-47138	In the Linux kernel, the following vulnerability has been resolved: cxgb4: avoid accessing registers when clearing filters Hardware register having the server TID base can contain invalid values when adapter is in bad state (for example, due to AER fatal error). Reading these invalid values in the register can lead to out-of-bound memory access. So, fix by using the saved server TID base when clearing filters.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26644	In the Linux kernel, the following vulnerability has been resolved: btrfs: don't abort filesystem when attempting to snapshot deleted subvolume If the source file descriptor to the snapshot ioctl refers to a deleted subvolume, we get the following abort: BTRFS: Transaction aborted (error -2) WARNING: CPU: 0 PID: 833 at fs/btrfs/transaction.c:1875 create_pending_snapshot+0x1040/0x1190 [btrfs] Modules linked in: pata_acpi btrfs ata_piix libata scsi_mod virtio_net blake2b_generic xor net_failover virtio_rng failover scsi_common rng_core raid6_pq libcrc32c CPU: 0 PID: 833 Comm: t_snapshot_dele Not tainted 6.7.0-rc6 #2 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-1.fc39 04/01/2014 RIP: 0010:create_pending_snapshot+0x1040/0x1190 [btrfs] RSP: 0018:ffffa09c01337af8 EFLAGS: 00010282 RAX: 0000000000000000 RBX: ffff9982053e7c78 RCX: 0000000000000027 RDX: ffff99827dc20848 RSI: 0000000000000001 RDI: ffff99827dc20840 RBP: ffffa09c01337c00 R08: 0000000000000000 R09: ffffa09c01337998 R10: 0000000000000003 R11: ffffffffb96da248 R12: fffffffffffffffe R13: ffff99820535bb28 R14: ffff99820b7bd000 R15: ffff99820381ea80 FS: 00007fe20aadabc0(0000) GS:ffff99827dc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000559a120b502f CR3: 00000000055b6000 CR4: 00000000000006f0 Call Trace: <TASK> ? create_pending_snapshot+0x1040/0x1190 [btrfs] ? __warn+0x81/0x130 ? create_pending_snapshot+0x1040/0x1190 [btrfs] ? report_bug+0x171/0x1a0 ? handle_bug+0x3a/0x70 ? exc_invalid_op+0x17/0x70 ? asm_exc_invalid_op+0x1a/0x20 ? create_pending_snapshot+0x1040/0x1190 [btrfs] ? create_pending_snapshot+0x1040/0x1190 [btrfs] create_pending_snapshots+0x92/0xc0 [btrfs] btrfs_commit_transaction+0x66b/0xf40 [btrfs] btrfs_mksubvol+0x301/0x4d0 [btrfs] btrfs_mksnapshot+0x80/0xb0 [btrfs] __btrfs_ioctl_snap_create+0x1c2/0x1d0 [btrfs] btrfs_ioctl_snap_create_v2+0xc4/0x150 [btrfs] btrfs_ioctl+0x8a6/0x2650 [btrfs] ? kmem_cache_free+0x22/0x340 ? do_sys_openat2+0x97/0xe0 __x64_sys_ioctl+0x97/0xd0 do_syscall_64+0x46/0xf0 entry_SYSCALL_64_after_hwframe+0x6e/0x76 RIP: 0033:0x7fe20abe83af RSP: 002b:00007ffe6eff1360 EFLAGS: 00000246 ORIG_RAX: 0000000000000010 RAX: ffffffffffffffda RBX: 0000000000000004 RCX: 00007fe20abe83af RDX: 00007ffe6eff23c0 RSI: 0000000050009417 RDI: 0000000000000003 RBP: 0000000000000003 R08: 0000000000000000 R09: 00007fe20ad16cd0 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007ffe6eff13c0 R14: 00007fe20ad45000 R15: 0000559a120b6d58 </TASK> ---[end trace 0000000000000000]--- BTRFS: error (device vdc: state A) in create_pending_snapshot:1875: errno=-2 No such entry BTRFS info (device vdc: state EA): forced readonly BTRFS warning (device vdc: state EA): Skipping commit of aborted transaction. BTRFS: error (device vdc: state EA) in cleanup_transaction:2055: errno=-2 No such entry This happens because create_pending_snapshot() initializes the new root item as a copy of the source root item. This includes the refs field, which is 0 for a deleted subvolume. The call to btrfs_insert_root() therefore inserts a root with refs == 0. btrfs_get_new_fs_root() then finds the root and returns -ENOENT if refs == 0, which causes create_pending_snapshot() to abort. Fix it by checking the source root's refs before attempting the snapshot, but after locking subvol_sem to avoid racing with deletion.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47180	In the Linux kernel, the following vulnerability has been resolved: NFC: nci: fix memory leak in nci_allocate_device nfcmrvl_disconnect fails to free the hci_dev field in struct nci_dev. Fix this by freeing hci_dev in nci_free_device. BUG: memory leak unreferenced object 0xffff888111ea6800 (size 1024): comm "kworker/1:0", pid 19, jiffies 4294942308 (age 13.580s) hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 60 fd 0c 81 88 ff ff ff ....`..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace: [<000000004bc25d43>] kmalloc include/linux/slab.h:552 [inline] [<000000004bc25d43>] kzalloc include/linux/slab.h:682 [inline] [<000000004bc25d43>] nci_hci_allocate+0x21/0xd0 net/nfc/nci/hci.c:784 [<00000000c59cff92>] nci_allocate_device net/nfc/nci/core.c:1170 [inline] [<00000000c59cff92>] nci_allocate_device+0x10b/0x160 net/nfc/nci/core.c:1132 [<00000000006e0a8e>] nfcmrvl_nci_register_dev+0x10a/0x1c0 drivers/nfc/nfcmrvl/main.c:153 [<000000004da1b57e>] nfcmrvl_probe+0x223/0x290 drivers/nfc/nfcmrvl/usb.c:345 [<00000000d506aed9>] usb_probe_interface+0x177/0x370 drivers/usb/core/driver.c:396 [<00000000bc632c92>] really_probe+0x159/0x4a0 drivers/base/dd.c:554 [<00000000f5009125>] driver_probe_device+0x84/0x100 drivers/base/dd.c:740 [<000000000ce658ca>] __device_attach_driver+0xee/0x110 drivers/base/dd.c:846 [<000000007067d05f>] bus_for_each_drv+0xb7/0x100 drivers/base/bus.c:431 [<00000000f8e13372>] __device_attach+0x122/0x250 drivers/base/dd.c:914 [<000000009cf68860>] bus_probe_device+0xc6/0xe0 drivers/base/bus.c:491 [<00000000359c965a>] device_add+0x5be/0xc30 drivers/base/core.c:3109 [<00000000086e4bd3>] usb_set_configuration+0x9d9/0xb90 drivers/usb/core/message.c:2164 [<00000000ca036872>] usb_generic_driver_probe+0x8c/0xc0 drivers/usb/core/generic.c:238 [<00000000d40d36f6>] usb_probe_device+0x5c/0x140 drivers/usb/core/driver.c:293 [<00000000bc632c92>] really_probe+0x159/0x4a0 drivers/base/dd.c:554	N/A	More Details
CVE-2021-47162	In the Linux kernel, the following vulnerability has been resolved: tipc: skb_linearize the head skb when reassembling msgs It's not a good idea to append the frag skb to a skb's frag_list if the frag_list already has skbs from elsewhere, such as this skb was created by pskb_copy() where the frag_list was cloned (all the skbs in it were skb_get'ed) and shared by multiple skbs. However, the new appended frag skb should have been only seen by the current skb. Otherwise, it will cause use after free crashes as this appended frag skb are seen by multiple skbs but it only got skb_get called once. The same thing happens with a skb updated by pskb_may_pull() with a skb_cloned skb. Li Shuang has reported quite a few crashes caused by this when doing testing over macvlan devices: [] kernel BUG at net/core/skbuff.c:1970! [] Call Trace: [] skb_clone+0x4d/0xb0 [] macvlan_broadcast+0xd8/0x160 [macvlan] [] macvlan_process_broadcast+0x148/0x150 [macvlan] [] process_one_work+0x1a7/0x360 [] worker_thread+0x30/0x390 [] kernel BUG at mm/usercopy.c:102! [] Call Trace: [] __check_heap_object+0xd3/0x100 [] __check_object_size+0xff/0x16b [] simple_copy_to_iter+0x1c/0x30 [] __skb_datagram_iter+0x7d/0x310 [] __skb_datagram_iter+0x2a5/0x310 [] skb_copy_datagram_iter+0x3b/0x90 [] tipc_recvmsg+0x14a/0x3a0 [tipc] [] ____sys_recvmsg+0x91/0x150 [] ___sys_recvmsg+0x7b/0xc0 [] kernel BUG at mm/slub.c:305! [] Call Trace: [] <IRQ> [] kmem_cache_free+0x3ff/0x400 [] __netif_receive_skb_core+0x12c/0xc40 [] ? kmem_cache_alloc+0x12e/0x270 [] netif_receive_skb_internal+0x3d/0xb0 [] ? get_rx_page_info+0x8e/0xa0 [be2net] [] be_poll+0x6ef/0xd00 [be2net] [] ? irq_exit+0x4f/0x100 [] net_rx_action+0x149/0x3b0 ... This patch is to fix it by linearizing the head skb if it has frag_list set in tipc_buf_append(). Note that we choose to do this before calling skb_unshare(), as __skb_linearize() will avoid skb_copy(). Also, we can not just drop the frag_list either as the early time.	N/A	More Details