SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 20 November 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
CVE-2024-48966	The software tools used by service personnel to test & calibrate the ventilator do not support user authentication. An attacker with access to the Service PC where the t through the test tool or manipulate the ventilator's settings and embedded software via the calibration tool, without having to authenticate to either tool. This could result have unintended impacts on device settings and performance.
CVE-2024-52380	Unrestricted Upload of File with Dangerous Type vulnerability in Softpulse Infotech Picsmize allows Upload a Web Shell to a Web Server.This issue affects Picsmize: fr
CVE-2024-52379	Unrestricted Upload of File with Dangerous Type vulnerability in Kinetic Innovative Technologies Sdn Bhd kineticPay for WooCommerce allows Upload a Web Shell to a WooCommerce: from n/a through 2.0.8.
CVE-2024-52377	Unrestricted Upload of File with Dangerous Type vulnerability in BdThemes Instant Image Generator allows Upload a Web Shell to a Web Server.This issue affects Inst
CVE-2024-52376	Unrestricted Upload of File with Dangerous Type vulnerability in cmsMinds Boat Rental Plugin for WordPress allows Upload a Web Shell to a Web Server.This issue af through 1.0.1.
CVE-2024-52375	Unrestricted Upload of File with Dangerous Type vulnerability in Arttia Creative Datasets Manager by Arttia Creative.This issue affects Datasets Manager by Arttia Crea
CVE-2024-42450	The Versa Director uses PostgreSQL (Postgres) to store operational and configuration data. It is also needed for High Availability function of the Versa Director. The de all instances of Versa Director. By default, Versa Director configures Postgres to listen on all network interfaces. This combination allows an unauthenticated attacker to filesystem contents to escalate privileges on the system. Exploitation Status: Versa Networks is not aware of this exploitation in any production systems. A proof of con Mitigation: Starting with the latest 22.1.4 version of Versa Director, the software will automatically restrict access to the Postgres and HA ports to only the local and pee recommends performing manual hardening of HA ports. Please refer to the following link for the steps https://docs.versa-networks.com/Solutions/System_Hardening/Perform_Manual_Hardening_for_Versa_Director#Secure_HA_Ports This vulnerability is not exploitable on Versa Directors have validated that no Versa-hosted head ends have been affected by this vulnerability. All Versa-hosted head ends are patched and hardened. Please contact Versa further assistance. Software Download Links: 22.1.4: https://support.versa-networks.com/support/solutions/articles/23000026708-release-22-1-4
CVE-2024-52374	Unrestricted Upload of File with Dangerous Type vulnerability in DoThatTask Do That Task allows Upload a Web Shell to a Web Server.This issue affects Do That Task
CVE-2024-52373	Unrestricted Upload of File with Dangerous Type vulnerability in Team Devexhub Devexhub Gallery allows Upload a Web Shell to a Web Server.This issue affects Dev
CVE-2024-52416	Missing Authorization vulnerability in Eugen Bobrowski Debug Tool allows Upload a Web Shell to a Web Server.This issue affects Debug Tool: from n/a through 2.2.
CVE-2024-48967	The ventilator and the Service PC lack sufficient audit logging capabilities to allow for detection of malicious activity and subsequent forensic examination. An attacker v could, without detection, make unauthorized changes to ventilator settings that result in unauthorized disclosure of information and/or have unintended impacts on devi

CVE Number	Description
CVE-2024-52372	Unrestricted Upload of File with Dangerous Type vulnerability in WebTechGlobal Easy CSV Importer BETA allows Upload a Web Shell to a Web Server.This issue affe
CVE-2024-52399	Unrestricted Upload of File with Dangerous Type vulnerability in Clarisse K. Writer Helper allows Upload a Web Shell to a Web Server.This issue affects Writer Helper:
CVE-2024-52369	Unrestricted Upload of File with Dangerous Type vulnerability in Optimal Access Inc. KBucket allows Upload a Web Shell to a Web Server.This issue affects KBucket: f
CVE-2024-52370	Unrestricted Upload of File with Dangerous Type vulnerability in Hive Support Hive Support – WordPress Help Desk allows Upload a Web Shell to a Web Server.This is from n/a through 1.1.1.
CVE-2024-52427	Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Saso Nikolov Event Tickets with Ticket Scanner allows Server Side Include (SS Ticket Scanner: from n/a through 2.3.11.
CVE-2024-52384	Unrestricted Upload of File with Dangerous Type vulnerability in Sage AI Sage AI: Chatbots, OpenAI GPT-4 Bulk Articles, Dalle-3 Image Generation allows Upload a W Chatbots, OpenAI GPT-4 Bulk Articles, Dalle-3 Image Generation: from n/a through 2.4.9.
CVE-2023-20036	A vulnerability in the web UI of Cisco IND could allow an authenticated, remote attacker to execute arbitrary commands with administrative privileges on the underlying vulnerability is due to improper input validation when uploading a Device Pack. An attacker could exploit this vulnerability by altering the request that is sent wher allow the attacker to execute arbitrary commands as NT AUTHORITY\SYSTEM on the underlying operating system of an affected device. Cisco has released software workarounds that address this vulnerability.
CVE-2024-52408	Unrestricted Upload of File with Dangerous Type vulnerability in Team PushAssist Push Notifications for WordPress by PushAssist allows Upload a Web Shell to a Wel WordPress by PushAssist: from n/a through 3.0.8.
CVE-2024-52407	Unrestricted Upload of File with Dangerous Type vulnerability in codeSavory BasePress Migration Tools allows Upload a Web Shell to a Web Server.This issue affects
CVE-2024-52406	Unrestricted Upload of File with Dangerous Type vulnerability in Wibergs Web CSV to html allows Upload a Web Shell to a Web Server.This issue affects CSV to html:
CVE-2024-52405	Unrestricted Upload of File with Dangerous Type vulnerability in Bikram Joshi B-Banner Slider allows Upload a Web Shell to a Web Server.This issue affects B-Banner
CVE-2024-52404	Unrestricted Upload of File with Dangerous Type vulnerability in Bigfive CF7 Reply Manager.This issue affects CF7 Reply Manager: from n/a through 1.2.3.
CVE-2024-52403	Unrestricted Upload of File with Dangerous Type vulnerability in WPExperts User Management allows Upload a Web Shell to a Web Server.This issue affects User Ma
CVE-2024-52429	Unrestricted Upload of File with Dangerous Type vulnerability in Anton Hoelstad WP Quick Setup allows Upload a Web Shell to a Web Server.This issue affects WP Qu
CVE-2024-52400	Unrestricted Upload of File with Dangerous Type vulnerability in Subhasis Laha Gallerio allows Upload a Web Shell to a Web Server.This issue affects Gallerio: from n/
CVE-2024-52430	Deserialization of Untrusted Data vulnerability in Lis Lis Video Gallery allows Object Injection.This issue affects Lis Video Gallery: from n/a through 0.2.1.
CVE-2024-52432	Deserialization of Untrusted Data vulnerability in NIX Solutions Ltd NIX Anti-Spam Light allows Object Injection.This issue affects NIX Anti-Spam Light: from n/a through
CVE-2024-52714	Tenda AC6 v2.0 v15.03.06.50 was discovered to contain a buffer overflow in the function 'fromSetSysTime.
CVE-2024-48694	File Upload vulnerability in Xi'an Daxi Information technology OfficeWeb365 v.8.6.1.0 and v7.18.23.0 allows a remote attacker to execute arbitrary code via the pw/save

CVE Number	Description
CVE-2024-48072	Weaver Ecology v9.* was discovered to contain a SQL injection vulnerability via the component /mobilemode/Action.jsp?invoker=com.weaver.formmodel.mobile.mec.servlet.MECAction&action=getFieldTriggerValue&searchField=*&fromTable=HrmResourceManager&whereClause=1%3d
CVE-2024-48070	An issue in Weaver E-cology v. attackers construct special requests to insert remote malicious code and to trigger malicious code execution, and control server privileg
CVE-2024-48069	A vulnerability was found in Weaver E-cology allows attackers use race conditions to bypass security mechanisms to upload malicious files and control server privilege
CVE-2024-52675	SourceCodester Sentiment Based Movie Rating System 1.0 is vulnerable to SQL Injection in /msrps/movies.php.
CVE-2024-52409	Deserialization of Untrusted Data vulnerability in Phan An AJAX Random Posts allows Object Injection.This issue affects AJAX Random Posts: from n/a through 0.3.3.
CVE-2024-52410	Deserialization of Untrusted Data vulnerability in Phoenixheart Referrer Detector allows Object Injection.This issue affects Referrer Detector: from n/a through 4.2.1.0.
CVE-2024-51051	AVSCMS v8.2.0 was discovered to contain weak default credentials for the Administrator account.
CVE-2024-52411	Deserialization of Untrusted Data vulnerability in Flowcraft UX Design Studio Advanced Personalization allows Object Injection.This issue affects Advanced Personaliz
CVE-2024-52412	Deserialization of Untrusted Data vulnerability in Stephen Cui Xin allows Object Injection.This issue affects Xin: from n/a through 1.0.8.1.
CVE-2024-52413	Deserialization of Untrusted Data vulnerability in DMC Airin Blog allows Object Injection.This issue affects Airin Blog: from n/a through 1.6.1.
CVE-2024-52414	Deserialization of Untrusted Data vulnerability in Anthony Carbon WDES Responsive Mobile Menu allows Object Injection.This issue affects WDES Responsive Mobile
CVE-2024-51053	An arbitrary file upload vulnerability in the component /main/fileupload.php of AVSCMS v8.2.0 allows attackers to execute arbitrary code via uploading a crafted file.
CVE-2023-43091	A flaw was found in GNOME Maps, which is vulnerable to a code injection attack via its service.json configuration file. If the configuration file is malicious, it may execut
CVE-2015-20111	miniupnp before 4c90b87, as used in Bitcoin Core before 0.12 and other products, lacks checks for snprintf return values, leading to a buffer overflow and significant da 12107. In Bitcoin Core before 0.12, remote code execution was possible in conjunction with CVE-2015-6031 exploitation.
CVE-2024-11311	The DVC from TRCore has a Path Traversal vulnerability and does not restrict the types of uploaded files. This allows unauthenticated remote attackers to upload arbit execution by uploading webshells.
CVE-2024-11312	The DVC from TRCore has a Path Traversal vulnerability and does not restrict the types of uploaded files. This allows unauthenticated remote attackers to upload arbit execution by uploading webshells.
CVE-2024-11313	The DVC from TRCore has a Path Traversal vulnerability and does not restrict the types of uploaded files. This allows unauthenticated remote attackers to upload arbit execution by uploading webshells.
CVE-2024-11314	The DVC from TRCore has a Path Traversal vulnerability and does not restrict the types of uploaded files. This allows unauthenticated remote attackers to upload arbit execution by uploading webshells.
CVE-2024-11315	The DVC from TRCore has a Path Traversal vulnerability and does not restrict the types of uploaded files. This allows unauthenticated remote attackers to upload arbit execution by uploading webshells.

CVE Number	Description
CVE-2024-50919	Jpress until v5.1.1 has arbitrary file uploads on the windows platform, and the construction of non-standard file formats such as .jsp. can lead to arbitrary command exe
CVE-2024-47533	Cobbler, a Linux installation server that allows for rapid setup of network installation environments, has an improper authentication vulnerability starting in version 3.0.0 `utils.get_shared_secret()` always returns `-1`, which allows anyone to connect to cobbler XML-RPC as user `"` password `-1` and make any changes. This gives anyo of the server. Versions 3.2.3 and 3.3.7 fix the issue.
CVE-2024-47208	Server-Side Request Forgery (SSRF), Improper Control of Generation of Code ('Code Injection') vulnerability in Apache OFBiz. This issue affects Apache OFBiz: befor version 18.12.17, which fixes the issue.
CVE-2024-52316	Unchecked Error Condition vulnerability in Apache Tomcat. If Tomcat is configured to use a custom Jakarta Authentication (formerly JASPIC) ServerAuthContext comp authentication process without explicitly setting an HTTP status to indicate failure, the authentication may not fail, allowing the user to bypass the authentication proces components that behave in this way. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M26, from 10.1.0-M1 through 10.1.30, from 9.0.0-M1 through 9 11.0.0, 10.1.31 or 9.0.96, which fix the issue.
CVE-2024-0012	An authentication bypass in Palo Alto Networks PAN-OS software enables an unauthenticated attacker with network access to the management web interface to gain P administrative actions, tamper with the configuration, or exploit other authenticated privilege escalation vulnerabilities like CVE-2024-9474 https://security.paloaltonetwo greatly reduced if you secure access to the management web interface by restricting access to only trusted internal IP addresses according to our recommended best https://live.paloaltonetworks.com/t5/community-blogs/tips-amp-tricks-how-to-secure-the-management-access-of-your-palo/ba-p/464431 . This issue is applicable only to PAN-OS 11.2 software. Cloud NGFW and Prisma Access are not impacted by this vulnerability.
CVE-2024-52433	Deserialization of Untrusted Data vulnerability in Mindstien Technologies My Geo Posts Free allows Object Injection.This issue affects My Geo Posts Free: from n/a thr
CVE-2024-45971	Multiple Buffer overflows in the MMS Client in MZ Automation LibIEC61850 before commit 1f52be9ddeae00e69cd43e4cac3cb4f0c880c4f0 allow a malicious server to c IdentifyResponse message.
CVE-2024-52759	D-LINK DI-8003 v16.07.26A1 was discovered to contain a buffer overflow via the ip parameter in the ip_position_asp function.
CVE-2024-31695	A misconfiguration in the fingerprint authentication mechanism of Binance: BTC, Crypto and NFTS v2.85.4, allows attackers to bypass authentication when adding a ne
CVE-2022-1884	A remote command execution vulnerability exists in gogs/gogs versions <=0.12.7 when deployed on a Windows server. The vulnerability arises due to improper validat An attacker can set `tree_path=.git.` to upload a file into the .git directory, allowing them to write or rewrite the `.git/config` file. If the `core.sshCommand` is set, this can
CVE-2024-10571	The Chartify – WordPress Chart Plugin plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.9.5 via the 'source' parameter. Tl include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can be used to bypass access controls, obtain sensitive da and other “safe” file types can be uploaded and included.
CVE-2024-50833	A SQL Injection vulnerability was found in /login.php in KASHIPARA E-learning Management System Project 1.0 via the username and password parameters.
CVE-2024-48510	Directory Traversal vulnerability in DotNetZip v.1.16.0 and before allows a remote attacker to execute arbitrary code via the src/Zip.Shared/ZipEntry.Extract.cs compon are no longer supported by the maintainer.
CVE-2024-4343	A Python command injection vulnerability exists in the `SagemakerLLM` class's `complete()` method within `./private_gpt/components/llm/custom/sagemaker.py` of the including 0.3.0. The vulnerability arises due to the use of the `eval()` function to parse a string received from a remote AWS SageMaker LLM endpoint into a dictionary. arbitrary Python code contained within the response. An attacker can exploit this vulnerability by manipulating the response from the AWS SageMaker LLM endpoint to execution of arbitrary commands on the system hosting the application. The issue is fixed in version 0.6.0.
CVE-2024-50823	A SQL Injection vulnerability was found in /admin/login.php in kashipara E-learning Management System Project 1.0 via the username and password parameters.
CVE-2024-52382	Missing Authorization vulnerability in Medma Technologies Matix Popup Builder allows Privilege Escalation.This issue affects Matix Popup Builder: from n/a through 1.0
CVE-2024-8856	The Backup and Staging by WP Time Capsule plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the the UploadHandler.pl versions up to, and including, 1.22.21. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote
CVE-2024-43091	In filterMask of SkEmbossMaskFilter.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additiona needed for exploitation.

CVE Number	Description
CVE-2024-10924	The Really Simple Security (Free, Pro, and Pro Multisite) plugins for WordPress are vulnerable to authentication bypass in versions 9.0.0 to 9.1.1.1. This is due to impr API actions with the 'check_login_and_get_user' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an adn setting is enabled (disabled by default).
CVE-2021-3838	DomPDF before version 2.0.0 is vulnerable to PHAR deserialization due to a lack of checking on the protocol before passing it into the file_get_contents() function. An a can pass in the phar:// protocol to unserialize the uploaded file and instantiate arbitrary PHP objects. This can lead to remote code execution, especially when DOMPdf chains like Laravel or vulnerable developer code.
CVE-2024-11028	The MultiManager WP – Manage All Your WordPress Sites Easily plugin for WordPress is vulnerable to Authentication Bypass in all versions up to, and including, 1.0.5 inappropriately determining the current user via user-supplied input. This makes it possible for unauthenticated attackers to generate an impersonation link that will allo administrator. NOTE: The user impersonation feature was disabled in version 1.1.0 and re-enabled with a patch in version 1.1.2.
CVE-2021-3902	An improper restriction of external entities (XXE) vulnerability in dompdf/dompdf's SVG parser allows for Server-Side Request Forgery (SSRF) and deserialization attac vulnerability can be exploited even if the isRemoteEnabled option is set to false. It allows attackers to perform SSRF, disclose internal image files, and cause PHAR de
CVE-2024-11120	Certain EOL GeoVision devices have an OS Command Injection vulnerability. Unauthenticated remote attackers can exploit this vulnerability to inject and execute arbit vulnerability has already been exploited by attackers, and we have received related reports.
CVE-2024-10443	Improper neutralization of special elements used in a command ('Command Injection') vulnerability in Task Manager component in Synology BeePhotos before 1.0.2-1(1.6.2-0720 and 1.7.0-0795 allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2024-50724	KASO v9.0 was discovered to contain a SQL injection vulnerability via the person_id parameter at /cardcase/editcard.jsp.
CVE-2024-44758	An arbitrary file upload vulnerability in the component /Production/UploadFile of NUS-M9 ERP Management Software v3.0.0 allows attackers to execute arbitrary code
CVE-2024-10934	In OpenBSD 7.5 before errata 008 and OpenBSD 7.4 before errata 021, avoid possible mbuf double free in NFS client and server implementation, do not use uninitializ
CVE-2024-10820	The WooCommerce Upload Files plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the upload_files() function in all versio for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.
CVE-2024-45970	Multiple Buffer overflows in the MMS Client in MZ Automation LibIEC61850 before commit ac925fae8e281ac6defcd630e9dd756264e9c5bc allow a malicious server to FileDirResponse message.
CVE-2024-10575	CWE-862: Missing Authorization vulnerability exists that could cause unauthorized access when enabled on the network and potentially impacting connected devices.
CVE-2024-10534	Origin Validation Error vulnerability in Dataprom Informatics Personnel Attendance Control Systems (PACS) / Access Control Security Systems (ACSS) allows Traffic I Control Systems (PACS) / Access Control Security Systems (ACSS): before 2024.
CVE-2024-40404	Cybele Software Thinfinity Workspace before v7.0.2.113 was discovered to contain an access control issue in the API endpoint where Web Sockets connections are es
CVE-2024-50649	The user avatar upload function in python_book V1.0 has an arbitrary file upload vulnerability.
CVE-2024-50648	yshopmall V1.0 has an arbitrary file upload vulnerability, which can enable RCE or even take over the server when improperly configured to parse JSP files.
CVE-2024-11150	The WordPress User Extra Fields plugin for WordPress is vulnerable to arbitrary file deletion due to insufficient file path validation in the delete_tmp_uploaded_file() fun makes it possible for unauthenticated attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such
CVE-2024-52402	Cross-Site Request Forgery (CSRF) vulnerability in Cliconomics Exclusive Content Password Protect allows Upload a Web Shell to a Web Server.This issue affects Ex 1.1.0.
CVE-2024-52401	Cross-Site Request Forgery (CSRF) vulnerability in 荒野无灯 Hacklog DownloadManager allows Upload a Web Shell to a Web Server.This issue affects Hacklog Down

CVE Number	Description
CVE-2024-48970	The ventilator's microcontroller lacks memory protection. An attacker could connect to the internal JTAG interface and read or write to flash memory using an off-the-sh the device and/or cause unauthorized information disclosure.
CVE-2024-9834	Improper data protection on the ventilator's serial interface could allow an attacker to send and receive messages that result in unauthorized disclosure of information a and performance.
CVE-2024-48971	The Clinician Password and Serial Number Clinician Password are hard-coded into the ventilator in plaintext form. This could allow an attacker to obtain the password access to the device, with clinician privileges.
CVE-2024-48973	The debug port on the ventilator's serial interface is enabled by default. This could allow an attacker to send and receive messages over the debug port (which are une disclosure of information and/or have unintended impacts on device settings and performance.
CVE-2024-52431	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pressaholic WordPress Video Robot - The Ultimate Video Impo WordPress Video Robot - The Ultimate Video Importer: from n/a through 1.20.0.
CVE-2024-48974	The ventilator does not perform proper file integrity checks when adopting firmware updates. This makes it possible for an attacker to force unauthorized changes to the device functionality by pushing a compromised/illegitimate firmware file. This could disrupt the function of the device and/or cause unauthorized information disclosure.
CVE-2024-11263	When the Global Pointer (GP) relative addressing is enabled (CONFIG_RISCV_GP=y), the gp reg points at 0x800 bytes past the start of the .sdata section which is the symbols.
CVE-2024-9832	There is no limit on the number of failed login attempts permitted with the Clinician Password or the Serial Number Clinician Password. An attacker could execute a bru ventilator, and then make changes to device settings that could disrupt the function of the device and/or result in unauthorized information disclosure.
CVE-2022-45157	A vulnerability has been identified in the way that Rancher stores vSphere's CPI (Cloud Provider Interface) and CSI (Container Storage Interface) credentials used to d This issue leads to the vSphere CPI and CSI passwords being stored in a plaintext object inside Rancher. This vulnerability is only applicable to users that deploy clust
CVE-2024-52398	Unrestricted Upload of File with Dangerous Type vulnerability in Halyra CDI.This issue affects CDI: from n/a through 5.5.3.
CVE-2024-50306	Unchecked return value can allow Apache Traffic Server to retain privileges on startup. This issue affects Apache Traffic Server: from 9.2.0 through 9.2.5, from 10.0.0 t to version 9.2.6 or 10.0.2, which fixes the issue.
CVE-2024-37285	A deserialization issue in Kibana can lead to arbitrary code execution when Kibana attempts to parse a YAML document containing a crafted payload. A successful atta both specific Elasticsearch indices privileges https://www.elastic.co/guide/en/elasticsearch/reference/current/defining-roles.html#roles-indices-priv and Kibana privilege roles-and-privileges.html assigned to them. The following Elasticsearch indices permissions are required * write privilege on the system indices .kibana_ingest* * The following Kibana privileges are additionally required * Under Fleet the All privilege is granted * Under Integration the Read or All privilege is granted * Access to the flee service account token
CVE-2024-52434	Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Supsystic Popup by Supsystic allows Command Injection.This issue affects Pop
CVE-2024-52393	Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Podlove Podlove Podcast Publisher.This issue affects Podlove Podcast Publish
CVE-2024-52397	Unrestricted Upload of File with Dangerous Type vulnerability in Davor Zeljkovic Convert Docx2post allows Upload a Web Shell to a Web Server.This issue affects Con
CVE-2023-20154	A vulnerability in the external authentication mechanism of Cisco Modeling Labs could allow an unauthenticated, remote attacker to access the web interface with admi improper handling of certain messages that are returned by the associated external authentication server. An attacker could exploit this vulnerability by logging in to the conditions, the authentication mechanism would be bypassed and the attacker would be logged in as an administrator. A successful exploit could allow the attacker to an affected server, including the ability to access and modify every simulation and all user-created data. To exploit this vulnerability, the attacker would need valid user authentication server. Cisco has released software updates that address this vulnerability. There are workarounds that address this vulnerability.
CVE-2024-51164	Multiple parameters have SQL injection vulnerability in JEPaaS 7.2.8 via /je/login/btnLog/insertBtnLog, which could allow a remote user to submit a specially crafted qu stored in the DB.
CVE-2024-38656	Argument injection in Ivanti Connect Secure before version 22.7R2.2 and 9.1R18.9 and Ivanti Policy Secure before version 22.7R1.2 allows a remote authenticated atta execution.

CVE Number	Description
CVE-2024-52300	macro-pdfviewer is a PDF Viewer Macro for XWiki using Mozilla pdf.js. The width parameter of the PDF viewer macro isn't properly escaped, allowing XSS for any user confidentiality, integrity and availability of the whole XWiki installation when an admin visits the page with the malicious code. This is fixed in 2.5.6.

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-9192	The WordPress Video Robot - The Ultimate Video Importer plugin for WordPress is vulnerable to privilege escalation due to insufficient validation on user meta that can be updated in the wpvr_rate_request_result() function in all versions up to, and including, 1.20.0. This makes it possible for authenticated attackers, with subscriber-level access and above, to update their user meta on a WordPress site. This can be leveraged to update their capabilities to that of an administrator.	8.8	More Details
CVE-2024-10800	The WordPress User Extra Fields plugin for WordPress is vulnerable to privilege escalation due to a missing capability check on the ajax_save_fields() function in all versions up to, and including, 16.6. This makes it possible for authenticated attackers, with subscriber-level access and above, to add custom fields that can be updated and then use the check_and_overwrite_wp_or_woocommerce_fields function to update the wp_capabilities field to have administrator privileges.	8.8	More Details
CVE-2024-11248	A vulnerability was found in Tenda AC10 16.03.10.13 and classified as critical. Affected by this issue is the function formSetRebootTimer of the file /goform/SetSysAutoRebbotCfg. The manipulation of the argument rebootTime leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2022-20655	A vulnerability in the implementation of the CLI on a device that is running ConfD could allow an authenticated, local attacker to perform a command injection attack. The vulnerability is due to insufficient validation of a process argument on an affected device. An attacker could exploit this vulnerability by injecting commands during the execution of this process. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privilege level of ConfD, which is commonly root.	8.8	More Details
CVE-2021-3742	A Server-Side Request Forgery (SSRF) vulnerability was discovered in chatwoot/chatwoot, affecting all versions prior to 2.5.0. The vulnerability allows an attacker to upload an SVG file containing a malicious SSRF payload. When the SVG file is used as an avatar and opened in a new tab, it can trigger the SSRF, potentially leading to host redirection.	8.8	More Details
CVE-2024-49778	A heap-based buffer overflow in tsMuxer version nightly-2024-05-12-02-01-18 allows attackers to cause Denial of Service (DoS) and Code Execution via a crafted MOV video file.	8.8	More Details
CVE-2024-49777	A heap-based buffer overflow in tsMuxer version nightly-2024-03-14-01-51-12 allows attackers to cause Denial of Service (DoS), Information Disclosure and Code Execution via a crafted MKV video file.	8.8	More Details
CVE-2024-41209	A heap-based buffer overflow in tsMuxer version nightly-2024-03-14-01-51-12 allows attackers to cause Denial of Service (DoS) and Code Execution via a crafted MOV video file.	8.8	More Details
CVE-2024-10962	The Migration, Backup, Staging – WPvivid plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 0.9.107 via deserialization of untrusted input in the 'replace_row_data' and 'replace_serialize_data' functions. This makes it possible for unauthenticated attackers to inject a PHP Object. No known POP chain is present in the vulnerable software. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code. An administrator must create a staging site to trigger the exploit.	8.8	More Details
CVE-2024-10979	Incorrect control of environment variables in PostgreSQL PL/Perl allows an unprivileged database user to change sensitive process environment variables (e.g. PATH). That often suffices to enable arbitrary code execution, even if the attacker lacks a database server operating system user. Versions before PostgreSQL 17.1, 16.5, 15.9, 14.14, 13.17, and 12.21 are affected.	8.8	More Details
CVE-2024-52554	Jenkins Shared Library Version Override Plugin 17.v786074c9fce7 and earlier declares folder-scoped library overrides as trusted, so that they're not executed in the Script Security sandbox, allowing attackers with Item/Configure permission on a folder to configure a folder-scoped library override that runs without sandbox protection.	8.8	More Details
CVE-2024-52553	Jenkins OpenId Connect Authentication Plugin 4.418.vccc7061f5b_6d and earlier does not invalidate the previous session on login.	8.8	More Details
CVE-2024-36242	Protection mechanism failure in the SPP for some Intel(R) Processors may allow an authenticated user to potentially enable escalation of privilege via local access.	8.8	More Details
CVE-2024-23918	Improper conditions check in some Intel(R) Xeon(R) processor memory controller configurations when using Intel(R) SGX may allow a privileged user to potentially enable escalation of privilege via local access.	8.8	More Details
CVE-2024-50970	A SQL injection vulnerability in orderview1.php of Itsourcecode Online Furniture Shopping Project 1.0 allows remote attackers to execute arbitrary SQL commands via the id parameter.	8.8	More Details
CVE-2024-50854	Tenda G3 v3.0 v15.11.0.20 was discovered to contain a stack overflow via the formSetPortMapping function.	8.8	More Details
CVE-2024-50853	Tenda G3 v3.0 v15.11.0.20 was discovered to contain a command injection vulnerability via the formSetDebugCfg function.	8.8	More Details
CVE-2024-44625	Gogs <=0.13.0 is vulnerable to Directory Traversal via the editFilePost function of internal/route/repo/editor.go.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49060	Azure Stack HCI Elevation of Privilege Vulnerability	8.8	More Details
CVE-2024-9849	The 3D FlipBook, PDF Viewer, PDF Embedder – Real 3D FlipBook WordPress Plugin plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'r3dfb_save_thumbnail_callback' function in all versions up to, and including, 4.6. This makes it possible for authenticated attackers, with Author-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-2024-52587	StepSecurity's Harden-Runner provides network egress filtering and runtime security for GitHub-hosted and self-hosted runners. Versions of step-security/harden-runner prior to v2.10.2 contain multiple command injection weaknesses via environment variables that could potentially be exploited under specific conditions. However, due to the current execution order of pre-steps in GitHub Actions and the placement of harden-runner as the first step in a job, the likelihood of exploitation is low as the Harden-Runner action reads the environment variable during the pre-step stage. There are no known exploits at this time. Version 2.10.2 contains a patch.	8.8	More Details
CVE-2018-9433	In ArrayConcatVisitor of builtins-array.cc, there is a possible type confusion due to improper input validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.	8.8	More Details
CVE-2018-9411	In decrypt of ClearKeyCasPlugin.cpp there is a possible out-of-bounds write due to a missing bounds check. This could lead to remote arbitrary code execution with no additional execution privileges needed. User interaction is needed for exploitation.	8.8	More Details
CVE-2018-9365	In smp_data_received of smp_l2c.cc, there is a possible out of bounds read followed by code execution due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.	8.8	More Details
CVE-2024-11395	Type Confusion in V8 in Google Chrome prior to 131.0.6778.85 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-11075	A vulnerability in the Incoming Goods Suite allows a user with unprivileged access to the underlying system (e.g. local or via SSH) a privilege escalation to the administrative level due to the usage of component vendor Docker images running with root permissions. Exploiting this misconfiguration leads to the fact that an attacker can gain administrative control. over the whole system.	8.8	More Details
CVE-2024-11194	The Classified Listing – Classified ads & Business Directory Plugin plugin for WordPress is vulnerable to unauthorized modification of data that can lead to privilege escalation due to a misconfigured check on the 'rtcl_import_settings' function in all versions up to, and including, 3.1.15.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update limited arbitrary options on the WordPress site. This can be leveraged to update the Subscriber role with Administrator-level capabilities to gain administrative user access to a vulnerable site. The vulnerability is limited in that the option updated must have a value that is an array.	8.8	More Details
CVE-2024-51743	MarkUs is a web application for the submission and grading of student assignments. In versions prior to 2.4.8, an arbitrary file write vulnerability in the update/upload/create file methods in Controllers allows authenticated instructors to write arbitrary files to any location on the web server MarkUs is running on (depending on the permissions of the underlying filesystem). e.g. This can lead to a delayed remote code execution in case an attacker is able to write a Ruby file into the config/initializers/ subfolder of the Ruby on Rails application. MarkUs v2.4.8 has addressed this issue. No known workarounds are available at the application level aside from upgrading.	8.8	More Details
CVE-2024-10728	The Post Grid Gutenberg Blocks and WordPress Blog Plugin – PostX plugin for WordPress is vulnerable to unauthorized plugin installation/activation due to a missing capability check on the 'install_required_plugin_callback' function in all versions up to, and including, 4.1.16. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install and activate arbitrary plugins which can be leveraged to achieve remote code execution if another vulnerable plugin is installed and activated.	8.8	More Details
CVE-2024-48292	An issue in the wssrvc.exe service of QuickHeal Antivirus Pro Version v24.0 and Quick Heal Total Security v24.0 allows authenticated attackers to escalate privileges.	8.8	More Details
CVE-2024-45505	Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in Apache HertzBeat (incubating). This vulnerability can only be exploited by authorized attackers. This issue affects Apache HertzBeat (incubating): before 1.6.1. Users are recommended to upgrade to version 1.6.1, which fixes the issue.	8.8	More Details
CVE-2024-41969	A low privileged remote attacker may modify the configuration of the CODESYS V3 service through a missing authentication vulnerability which could lead to full system access and/or DoS.	8.8	More Details
CVE-2024-41151	Deserialization of Untrusted Data vulnerability in Apache HertzBeat. This vulnerability can only be exploited by authorized attackers. This issue affects Apache HertzBeat: before 1.6.1. Users are recommended to upgrade to version 1.6.1, which fixes the issue.	8.8	More Details
CVE-2024-52946	An issue was discovered in LemonLDAP::NG before 2.20.1. An Improper Check during session refresh allows an authenticated user to raise their authentication level if the admin configured an "Adaptative authentication rule" with an increment instead of an absolute value.	8.8	More Details
CVE-2024-52415	Cross-Site Request Forgery (CSRF) vulnerability in Skpstorm SK WP Settings Backup allows Object Injection.This issue affects SK WP Settings Backup: from n/a through 1.0.	8.8	More Details
CVE-2024-50852	Tenda G3 v3.0 v15.11.0.20 was discovered to contain a command injection vulnerability via the formSetUSBPartitionUmount function.	8.8	More Details
CVE-2018-9466	In the xmlSnprintfElementContent function of valid.c, there is a possible out of bounds write. This could lead to remote escalation of privilege in an unprivileged app with no additional execution privileges needed. User interaction is needed for exploitation.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10629	The GPX Viewer plugin for WordPress is vulnerable to arbitrary file creation due to a missing capability check and file type validation in the gpxv_file_upload() function in all versions up to, and including, 2.2.8. This makes it possible for authenticated attackers, with subscriber-level access and above, to create arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2024-3370	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Egebilgi Software Website Template allows SQL Injection.This issue affects Website Template: before 29.04.2024.	8.6	More Details
CVE-2024-9186	The Recover WooCommerce Cart Abandonment, Newsletter, Email Marketing, Marketing Automation By FunnelKit WordPress plugin before 3.3.0 does not sanitize and escape the bwfan-track-id parameter before using it in a SQL statement, allowing unauthenticated users to perform SQL injection attacks	8.6	More Details
CVE-2020-27124	A vulnerability in the SSL/TLS handler of Cisco Adaptive Security Appliance (ASA) Software could allow an unauthenticated, remote attacker to cause the affected device to reload unexpectedly, leading to a denial of service (DoS) condition. The vulnerability is due to improper error handling on established SSL/TLS connections. An attacker could exploit this vulnerability by establishing an SSL/TLS connection with the affected device and then sending a malicious SSL/TLS message within that connection. A successful exploit could allow the attacker to cause the device to reload.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	8.6	More Details
CVE-2023-20125	A vulnerability in the local interface of Cisco BroadWorks Network Server could allow an unauthenticated, remote attacker to exhaust system resources, causing a denial of service (DoS) condition. This vulnerability exists because rate limiting does not occur for certain incoming TCP connections. An attacker could exploit this vulnerability by sending a high rate of TCP connections to the server. A successful exploit could allow the attacker to cause TCP connection resources to grow rapidly until the Cisco BroadWorks Network Server becomes unusable. Note: To recover from this vulnerability, either Cisco BroadWorks Network Server software must be restarted or the Cisco BroadWorks Network Server node must be rebooted. For more information, see the section of this advisory. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	8.6	More Details
CVE-2024-52371	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in DonnellC Global Gateway e4 l Payeezy Gateway.This issue affects Global Gateway e4 l Payeezy Gateway: from n/a through 2.0.	8.6	More Details
CVE-2024-9693	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.0 prior to 17.3.7, starting from 17.4 prior to 17.4.4, and starting from 17.5 prior to 17.5.2, which could have allowed unauthorized access to the Kubernetes agent in a cluster under specific configurations.	8.5	More Details
CVE-2020-26071	A vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to create or overwrite arbitrary files on an affected device, which could result in a denial of service (DoS) condition. The vulnerability is due to insufficient input validation for specific commands. An attacker could exploit this vulnerability by including crafted arguments to those specific commands. A successful exploit could allow the attacker to create or overwrite arbitrary files on the affected device, which could result in a DoS condition.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	8.4	More Details
CVE-2024-34023	Untrusted pointer dereference in some Intel(R) Graphics Drivers may allow an authenticated user to potentially enable escalation of privilege via local access.	8.4	More Details
CVE-2024-38665	Out-of-bounds write in some Intel(R) Graphics Drivers may allow an authenticated user to potentially enable escalation of privilege via local access.	8.4	More Details
CVE-2024-43704	Software installed and run as a non-privileged user may conduct improper GPU system calls to gain access to the graphics buffers of a parent process.	8.4	More Details
CVE-2024-52291	Craft is a content management system (CMS). A vulnerability in CraftCMS allows an attacker to bypass local file system validation by utilizing a double file:// scheme (e.g., file://file:////). This enables the attacker to specify sensitive folders as the file system, leading to potential file overwriting through malicious uploads, unauthorized access to sensitive files, and, under certain conditions, remote code execution (RCE) via Server-Side Template Injection (SSTI) payloads. Note that this will only work if you have an authenticated administrator account with allowAdminChanges enabled. This is fixed in 5.4.6 and 4.12.5.	8.4	More Details
CVE-2024-49574	Zohocorp ManageEngine ADAudit Plus versions below 8123 are vulnerable to SQL Injection in the reports module.	8.3	More Details
CVE-2024-32483	Improper access control for some Intel(R) EMA software before version 1.13.1.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2024-52508	Nextcloud Mail is the mail app for Nextcloud, a self-hosted productivity platform. When a user is trying to set up a mail account with an email address like user@example.tld that does not support auto configuration, and an attacker managed to register autoconfig.tld, the used email details would be send to the server of the attacker. It is recommended that the Nextcloud Mail app is upgraded to 1.14.6, 1.15.4, 2.2.11, 3.6.3, 3.7.7 or 4.0.0.	8.2	More Details
CVE-2024-52583	The WesHacks GitHub repository provides the official Hackathon competition website source code for the Muweilah Wesgreen Hackathon. The page `schedule.html` before 17 November 2024 or commit 93dfb83 contains links to `Leostop`, a site that hosts a malicious injected JavaScript file that occurs when bootstrap is run as well as jquery. `Leostop` may be a tracking malware and creates 2 JavaScript files, but little else is known about it. The WesHacks website remove all references to `Leostop` as of 17 November 2024.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42386	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and produce a segmentation fault on the application.	8.2	More Details
CVE-2024-36282	Improper input validation in the Intel(R) Server Board S2600ST Family BIOS and Firmware Update software all versions may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2024-36482	Improper input validation in some Intel(R) CIP software before version 2.4.10852 may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2024-39726	IBM Engineering Lifecycle Optimization - Engineering Insights 7.0.2 and 7.0.3 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	8.2	More Details
CVE-2024-10828	The Advanced Order Export For WooCommerce plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.5.5 via deserialization of untrusted input during Order export when the "Try to convert serialized values" option is enabled. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain allows attackers to delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	8.1	More Details
CVE-2024-3501	In lunary-ai/lunary versions up to and including 1.2.5, an information disclosure vulnerability exists due to the inclusion of single-use tokens in the responses of `GET /v1/users/me` and `GET /v1/users/me/org` API endpoints. These tokens, intended for sensitive operations such as password resets or account verification, are exposed to unauthorized actors, potentially allowing them to perform actions on behalf of the user. This issue was addressed in version 1.2.6, where the exposure of single-use tokens in user-facing queries was mitigated.	8.1	More Details
CVE-2024-52867	guix-daemon in GNU Guix before 5ab3c4c allows privilege escalation because build outputs are accessible by local users before file metadata concerns (e.g., for setuid and setgid programs) are properly addressed. The vulnerability can be remediated within the product via certain pull, reconfigure, and restart actions. Both 5ab3c4c and 5582241 are needed to resolve the vulnerability.	8.1	More Details
CVE-2024-3379	In lunary-ai/lunary versions 1.2.2 through 1.2.6, an incorrect authorization vulnerability allows unprivileged users to re-generate the private key for projects they do not have access to. Specifically, a user with a 'Member' role can issue a request to regenerate the private key of a project without having the necessary permissions or being assigned to that project. This issue was fixed in version 1.2.7.	8.1	More Details
CVE-2024-41967	A low privileged remote attacker may modify the boot mode configuration setup of the device, leading to modification of the firmware upgrade process or a denial-of-service attack.	8.1	More Details
CVE-2024-3502	In lunary-ai/lunary versions up to and including 1.2.5, an information disclosure vulnerability exists where account recovery hashes of users are inadvertently exposed to unauthorized actors. This issue occurs when authenticated users inspect responses from `GET /v1/users/me` and `GET /v1/users/me/org` endpoints. The exposed account recovery hashes, while not directly related to user passwords, represent sensitive information that should not be accessible to unauthorized parties. Exposing these hashes could potentially facilitate account recovery attacks or other malicious activities. The vulnerability was addressed in version 1.2.6.	8.1	More Details
CVE-2024-45419	Improper input validation in some Zoom Apps may allow an unauthenticated user to conduct a disclosure of information via network access.	8.1	More Details
CVE-2024-40638	GLPI is a free asset and IT management software package. An authenticated user can exploit multiple SQL injection vulnerabilities. One of them can be used to alter another user account data and take control of it. Upgrade to 10.0.17.	8.1	More Details
CVE-2024-41971	A low privileged remote attacker can overwrite an arbitrary file on the filesystem leading to a DoS and data loss.	8.1	More Details
CVE-2024-40405	Incorrect access control in Cybele Software Thinfinity Workspace before v7.0.3.109 allows attackers to gain access to a secondary broker via a crafted request.	8.1	More Details
CVE-2022-20649	A vulnerability in Cisco RCM for Cisco StarOS Software could allow an unauthenticated, remote attacker to perform remote code execution on the application with root-level privileges in the context of the configured container. This vulnerability exists because the debug mode is incorrectly enabled for specific services. An attacker could exploit this vulnerability by connecting to the device and navigating to the service with debug mode enabled. A successful exploit could allow the attacker to execute arbitrary commands as the root user. The attacker would need to perform detailed reconnaissance to allow for unauthenticated access. The vulnerability can also be exploited by an authenticated attacker. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	8.1	More Details
CVE-2024-52428	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Scripteo Ads Booster by Ads Pro allows PHP Local File Inclusion.This issue affects Ads Booster by Ads Pro: from n/a through 1.12.	8.1	More Details
CVE-2024-41973	A low privileged remote attacker can specify an arbitrary file on the filesystem which may lead to an arbitrary file writes with root privileges.	8.1	More Details
CVE-2024-52381	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Shoaib Rehmat ZIJ KART allows PHP Local File Inclusion.This issue affects ZIJ KART: from n/a through 1.1.	8.1	More Details
CVE-2024-8938	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause a potential arbitrary code execution after a successful Man-In-The-Middle attack followed by sending a crafted Modbus function call to tamper with memory area involved in memory size computation.	8.1	More Details
CVE-2024-52789	Tenda W30E v2.0 V16.01.0.8 was discovered to contain a hardcoded password vulnerability in /etc_ro/shadow, which allows attackers to log in as root.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-52550	Jenkins Pipeline: Groovy Plugin 3990.vd281dd77a_388 and earlier, except 3975.3977.v478dd9e956c3 does not check whether the main (Jenkinsfile) script for a rebuilt build is approved, allowing attackers with Item/Build permission to rebuild a previous build whose (Jenkinsfile) script is no longer approved.	8.0	More Details
CVE-2024-52788	Tenda W9 v1.0.0.7(4456) was discovered to contain a hardcoded password vulnerability in /etc_ro/shadow, which allows attackers to log in as root.	8.0	More Details
CVE-2024-52551	Jenkins Pipeline: Declarative Plugin 2.2214.vb_b_34b_2ea_9b_83 and earlier does not check whether the main (Jenkinsfile) script used to restart a build from a specific stage is approved, allowing attackers with Item/Build permission to restart a previous build whose (Jenkinsfile) script is no longer approved.	8.0	More Details
CVE-2024-9413	The transport_message_handler function in SCP-Firmware release versions 2.11.0-2.15.0 does not properly handle errors, potentially allowing an Application Processor (AP) to cause a buffer overflow in System Control Processor (SCP) firmware.	8.0	More Details
CVE-2024-52552	Jenkins Authorize Project Plugin 1.7.2 and earlier evaluates a string containing the job name with JavaScript on the Authorization view, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	8.0	More Details
CVE-2024-51503	A security agent manual scan command injection vulnerability in the Trend Micro Deep Security 20 Agent could allow an attacker to escalate privileges and execute arbitrary code on an affected machine. In certain circumstances, attackers that have legitimate access to the domain may be able to remotely inject commands to other machines in the same domain. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability locally and must have domain user privileges to affect other machines.	8.0	More Details
CVE-2024-52308	The GitHub CLI version 2.6.1 and earlier are vulnerable to remote code execution through a malicious codespace SSH server when using `gh codespace ssh` or `gh codespace logs` commands. This has been patched in the cli v2.62.0. Developers connect to remote codespaces through an SSH server running within the devcontainer, which is generally provided through the [default devcontainer image](https://docs.github.com/en/codespaces/setting-up-your-project-for-codespaces/adding-a-dev-container-... https://docs.github.com/en/codespaces/setting-up-your-project-for-codespaces/adding-a-dev-container-configuration/introduction-to-dev-containers#using-the-default-dev-container-configuration) . GitHub CLI [retrieves SSH connection details](https://github.com/cli/cli/blob/30066b0042d0c5928d959e288144300cb28196c9/internal/codespaces/rpc/inv... https://github.com/cli/cli/blob/30066b0042d0c5928d959e288144300cb28196c9/internal/codespaces/rpc/invoker.go#L230-L244), such as remote username, which is used in [executing `ssh` commands](https://github.com/cli/cli/blob/e356c69a6f0125cfaac782c35acf77314f18908d/pkg/cmd/codespace/ssh.go#L2... https://github.com/cli/cli/blob/e356c69a6f0125cfaac782c35acf77314f18908d/pkg/cmd/codespace/ssh.go#L263) for `gh codespace ssh` or `gh codespace logs` commands. This exploit occurs when a malicious third-party devcontainer contains a modified SSH server that injects `ssh` arguments within the SSH connection details. `gh codespace ssh` and `gh codespace logs` commands could execute arbitrary code on the user's workstation if the remote username contains something like `-oProxyCommand="echo hacked" #`. The `-oProxyCommand` flag causes `ssh` to execute the provided command while `#` shell comment causes any other `ssh` arguments to be ignored. In `2.62.0`, the remote username information is being validated before being used.	8.0	More Details
CVE-2024-8979	The Essential Addons for Elementor – Best Elementor Addon, Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 6.0.9 via the 'init_content_lostpassword_user_email_controls' function. This makes it possible for authenticated attackers, with Author-level access and above, to extract sensitive data including usernames and passwords of any user, including Administrators, as long as that user opens the email notification for a password change request and images are not blocked by the email client.	8.0	More Details
CVE-2024-39368	Improper neutralization of special elements used in an SQL command ('SQL Injection') in some Intel(R) Neural Compressor software before version v3.0 may allow an authenticated user to potentially enable escalation of privilege via adjacent access.	8.0	More Details
CVE-2024-50264	In the Linux kernel, the following vulnerability has been resolved: vsock/virtio: Initialization of the dangling pointer occurring in vsk->trans During loopback communication, a dangling pointer can be created in vsk->trans, potentially leading to a Use-After-Free condition. This issue is resolved by initializing vsk->trans to NULL.	7.8	More Details
CVE-2023-52921	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix possible UAF in amdgpu_cs_pass1() Since the gang_size check is outside of chunk parsing loop, we need to reset i before we free the chunk data. Suggested by Ye Zhang (@VAR10CK) of Baidu Security.	7.8	More Details
CVE-2024-43093	In shouldHideDocument of ExternalStorageProvider.java, there is a possible bypass of a file path filter designed to prevent access to sensitive directories due to incorrect unicode normalization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2018-9338	In ResStringPool::setTo of ResourceTypes.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2017-13315	In writeToParcel and createFromParcel of DcParamObject.java, there is a permission bypass due to a write size mismatch. This could lead to an elevation of privileges where the user can start an activity with system privileges, with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-48992	Qualys discovered that needrestart, before version 3.8, allows local attackers to execute arbitrary code as root by tricking needrestart into running the Ruby interpreter with an attacker-controlled RUBYLIB environment variable.	7.8	More Details
CVE-2023-21270	In restorePermissionState of PermissionManagerServiceImpl.java, there is a possible way for an app to keep permissions that should be revoked due to incorrect permission flags cleared during an update. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-11003	Qualys discovered that needrestart, before version 3.8, passes unsanitized data to a library (Modules::ScanDeps) which expects safe input. This could allow a local attacker to execute arbitrary shell commands. Please see the related CVE-2024-10224 in Modules::ScanDeps.	7.8	More Details
CVE-2024-48991	Qualys discovered that needrestart, before version 3.8, allows local attackers to execute arbitrary code as root by winning a race condition and tricking needrestart into running their own, fake Python interpreter (instead of the system's real Python interpreter). The initial security fix (6ce6136) introduced a regression which was subsequently resolved (42af5d3).	7.8	More Details
CVE-2024-53057	In the Linux kernel, the following vulnerability has been resolved: net/sched: stop qdisc_tree_reduce_backlog on TC_H_ROOT In qdisc_tree_reduce_backlog, Qdiscs with major handle ffff: are assumed to be either root or ingress. This assumption is bogus since it's valid to create egress qdiscs with major handle ffff: Budimir Markovic found that for qdiscs like DRR that maintain an active class list, it will cause a UAF with a dangling class pointer. In 066a3b5b2346, the concern was to avoid iterating over the ingress qdisc since its parent is itself. The proper fix is to stop when parent TC_H_ROOT is reached because the only way to retrieve ingress is when a hierarchy which does not contain a ffff: major handle call into qdisc_lookup with TC_H_MAJ(TC_H_ROOT). In the scenario where major ffff: is an egress qdisc in any of the tree levels, the updates will also propagate to TC_H_ROOT, which then the iteration must stop. net/sched/sch_api.c | 2 +- 1 file changed, 1 insertion(+), 1 deletion(-)	7.8	More Details
CVE-2024-53059	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: Fix response handling in iwl_mvm_send_recovery_cmd() 1. The size of the response packet is not validated. 2. The response buffer is not freed. Resolve these issues by switching to iwl_mvm_send_cmd_status(), which handles both size validation and frees the buffer.	7.8	More Details
CVE-2024-53061	In the Linux kernel, the following vulnerability has been resolved: media: s5p-jpeg: prevent buffer overflows The current logic allows word to be less than 2. If this happens, there will be buffer overflows, as reported by smatch. Add extra checks to prevent it. While here, remove an unused word = 0 assignment.	7.8	More Details
CVE-2024-53068	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Fix slab-use-after-free in scmi_bus_notifier() The scmi_dev->name is released prematurely in __scmi_device_destroy(), which causes slab-use-after-free when accessing scmi_dev->name in scmi_bus_notifier(). So move the release of scmi_dev->name to scmi_device_release() to avoid slab-use-after-free. | BUG: KASAN: slab-use-after-free in strncmp+0xe4/0xec | Read of size 1 at addr ffffff80a482bcc0 by task swapper/0/1 | | CPU: 1 PID: 1 Comm: swapper/0 Not tainted 6.6.38-debug #1 | Hardware name: Qualcomm Technologies, Inc. SA8775P Ride (DT) | Call trace: | dump_backtrace+0x94/0x114 | show_stack+0x18/0x24 | dump_stack_lvl+0x48/0x60 | print_report+0xf4/0x5b0 | kasan_report+0xa4/0xec | __asan_report_load1_noabort+0x20/0x2c | strncmp+0xe4/0xec | scmi_bus_notifier+0x5c/0x54c | notifier_call_chain+0xb4/0x31c | blocking_notifier_call_chain+0x68/0x9c | bus_notify+0x54/0x78 | device_del+0x1bc/0x840 | device_unregister+0x20/0xb4 | __scmi_device_destroy+0xac/0x280 | scmi_device_destroy+0x94/0xd0 | scmi_chan_setup+0x524/0x750 | scmi_probe+0x7fc/0x1508 | platform_probe+0xc4/0x19c | really_probe+0x32c/0x99c | __driver_probe_device+0x15c/0x3c4 | driver_probe_device+0x5c/0x170 | __driver_attach+0x1c8/0x440 | bus_for_each_dev+0xf4/0x178 | driver_attach+0x3c/0x58 | bus_add_driver+0x234/0x4d4 | driver_register+0xf4/0x3c0 | __platform_driver_register+0x60/0x88 | scmi_driver_init+0xb0/0x104 | do_one_initcall+0xb4/0x664 | kernel_init_freeable+0x3c8/0x894 | kernel_init+0x24/0x1e8 | ret_from_fork+0x10/0x20 | | Allocated by task 1: | kasan_save_stack+0x2c/0x54 | kasan_set_track+0x2c/0x40 | kasan_save_alloc_info+0x24/0x34 | __kasan_kmalloc+0xa0/0xb8 | __kmalloc_node_track_caller+0x6c/0x104 | kstrdup+0x48/0x84 | kstrdup_const+0x34/0x40 | __scmi_device_create.part.0+0x8c/0x408 | scmi_device_create+0x104/0x370 | scmi_chan_setup+0x2a0/0x750 | scmi_probe+0x7fc/0x1508 | platform_probe+0xc4/0x19c | really_probe+0x32c/0x99c | __driver_probe_device+0x15c/0x3c4 | driver_probe_device+0x5c/0x170 | __driver_attach+0x1c8/0x440 | bus_for_each_dev+0xf4/0x178 | driver_attach+0x3c/0x58 | bus_add_driver+0x234/0x4d4 | driver_register+0xf4/0x3c0 | __platform_driver_register+0x60/0x88 | scmi_driver_init+0xb0/0x104 | do_one_initcall+0xb4/0x664 | kernel_init_freeable+0x3c8/0x894 | kernel_init+0x24/0x1e8 | ret_from_fork+0x10/0x20 | | Freed by task 1: | kasan_save_stack+0x2c/0x54 | kasan_set_track+0x2c/0x40 | kasan_save_free_info+0x38/0x5c | __kasan_slab_free+0xe8/0x164 | __kmem_cache_free+0x11c/0x230 | kfree+0x70/0x130 | kfree_const+0x20/0x40 | __scmi_device_destroy+0x70/0x280 | scmi_device_destroy+0x94/0xd0 | scmi_chan_setup+0x524/0x750 | scmi_probe+0x7fc/0x1508 | platform_probe+0xc4/0x19c | really_probe+0x32c/0x99c | __driver_probe_device+0x15c/0x3c4 | driver_probe_device+0x5c/0x170 | __driver_attach+0x1c8/0x440 | bus_for_each_dev+0xf4/0x178 | driver_attach+0x3c/0x58 | bus_add_driver+0x234/0x4d4 | driver_register+0xf4/0x3c0 | __platform_driver_register+0x60/0x88 | scmi_driver_init+0xb0/0x104 | do_one_initcall+0xb4/0x664 | kernel_init_freeable+0x3c8/0x894 | kernel_init+0x24/0x1e8 | ret_from_fork+0x10/0x20	7.8	More Details
CVE-2024-46467	By default, dedicated folders of ZONEPOINT for Windows up to 2024.1 can be accessed by other users to misuse technical files and make them perform tasks with higher privileges. Configuration of ZONEPOINT has to be modified to prevent this vulnerability.	7.8	More Details
CVE-2024-50267	In the Linux kernel, the following vulnerability has been resolved: USB: serial: io_edgeport: fix use after free in debug printk The "dev_dbg(&urb->dev->dev, ..." which happens after usb_free_urb(urb) is a use after free of the "urb" pointer. Store the "dev" pointer at the start of the function to avoid this issue.	7.8	More Details
CVE-2024-50269	In the Linux kernel, the following vulnerability has been resolved: usb: musb: sunxi: Fix accessing an released usb phy Commit 6ed05c68cbca ("usb: musb: sunxi: Explicitly release USB PHY on exit") will cause that usb phy @glue->xceiv is accessed after released. 1) register platform driver @sunxi_musb_driver // get the usb phy @glue->xceiv sunxi_musb_probe() -> devm_usb_get_phy(). 2) register and unregister platform driver @musb_driver musb_probe() -> sunxi_musb_init() use the phy here //the phy is released here musb_remove() -> sunxi_musb_exit() -> devm_usb_put_phy() 3) register @musb_driver again musb_probe() -> sunxi_musb_init() use the phy here but the phy has been released at 2). ... Fixed by reverting the commit, namely, removing devm_usb_put_phy() from sunxi_musb_exit().	7.8	More Details
CVE-2024-39709	Incorrect file permissions in Ivanti Connect Secure before version 22.6R2 (Not Applicable to 9.1Rx) and Ivanti Policy Secure before version 22.7R1 (Not Applicable to 9.1Rx) allow a local authenticated attacker to escalate their privileges.	7.8	More Details
CVE-2024-37398	Insufficient validation in Ivanti Secure Access Client before 22.7R4 allows a local authenticated attacker to escalate their privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46462	By default, dedicated folders of ZEDMAIL for Windows up to 2024.3 can be accessed by other users to misuse technical files and make them perform tasks with higher privileges. Configuration of ZEDMAIL has to be modified to prevent this vulnerability.	7.8	More Details
CVE-2024-46463	By default, dedicated folders of ORIZON for Windows up to 2024.3 can be accessed by other users to misuse technical files and make them perform tasks with higher privileges. Configuration of ORIZON has to be modified to prevent this vulnerability.	7.8	More Details
CVE-2024-46465	By default, dedicated folders of CRYHOD for Windows up to 2024.3 can be accessed by other users to misuse technical files and make them perform tasks with higher privileges. Configuration of CRYHOD has to be modified to prevent this vulnerability.	7.8	More Details
CVE-2024-46466	By default, dedicated folders of ZONECENTRAL for Windows up to 2024.3 or up to Q.2021.2 (ANSSI qualification submission) can be accessed by other users to misuse technical files and make them perform tasks with higher privileges. Configuration of ZONECENTRAL has to be modified to prevent this vulnerability.	7.8	More Details
CVE-2024-43089	In updateInternal of MediaProvider.java , there is a possible access of another app's files due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-10204	Heap-based Buffer Overflow and Uninitialized Variable vulnerabilities exist in the X_B and SAT file reading procedure in eDrawings from Release SOLIDWORKS 2024 through Release SOLIDWORKS 2025. These vulnerabilities could allow an attacker to execute arbitrary code while opening a specially crafted X_B or SAT file.	7.8	More Details
CVE-2024-51141	An issue in TOTOLINK Bluetooth Wireless Adapter A600UB allows a local attacker to execute arbitrary code via the WifiAutoInstallDriver.exe and MSASN1.dll components.	7.8	More Details
CVE-2017-13310	In createFromParcel of ViewPager.java, there is a possible read/write serialization issue leading to a permissions bypass. This could lead to local escalation of privilege where an app can start an activity with system privileges with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2017-13312	In createFromParcel of MediaCas.java, there is a possible parcel read/write mismatch due to improper input validation. This could lead to local escalation of privilege where an app can start an activity with system privileges with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2017-13314	In setAllowOnlyVpnForUids of NetworkManagementService.java, there is a possible security settings bypass due to a missing permission check. This could lead to local escalation of privilege allowing users to access non-VPN networks, when they are supposed to be restricted to the VPN networks, with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-50283	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix slab-use-after-free in smb3_preauth_hash_rsp ksmbd_user_session_put should be called under smb3_preauth_hash_rsp(). It will avoid freeing session before calling smb3_preauth_hash_rsp().	7.8	More Details
CVE-2024-50282	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: add missing size check in amdgpu_debugfs_gprwave_read() Avoid a possible buffer overflow if size is larger than 4K. (cherry picked from commit f5d873f5825b40d886d03bd2aede91d4cf002434)	7.8	More Details
CVE-2024-50280	In the Linux kernel, the following vulnerability has been resolved: dm cache: fix flushing uninitialized delayed_work on cache_ctr error An unexpected WARN_ON from flush_work() may occur when cache creation fails, caused by destroying the uninitialized delayed_work waker in the error path of cache_create(). For example, the warning appears on the superblock checksum error. Reproduce steps: dmsetup create cmeta --table "0 8192 linear /dev/sdc 0" dmsetup create cdata --table "0 65536 linear /dev/sdc 8192" dmsetup create corig --table "0 524288 linear /dev/sdc 262144" dd if=/dev/urandom of=/dev/mapper/cmeta bs=4k count=1 oflag=direct dmsetup create cache --table "0 524288 cache /dev/mapper/cmeta \ /dev/mapper/cdata /dev/mapper/corig 128 2 metadata2 writethrough smq 0" Kernel logs: (snip) WARNING: CPU: 0 PID: 84 at kernel/workqueue.c:4178 __flush_work+0x5d4/0x890 Fix by pulling out the cancel_delayed_work_sync() from the constructor's error path. This patch doesn't affect the use-after-free fix for concurrent dm_resume and dm_destroy (commit 6a459d8edbdb ("dm cache: Fix UAF in destroy()")) as cache_dtr is not changed.	7.8	More Details
CVE-2024-50276	In the Linux kernel, the following vulnerability has been resolved: net: vertexcom: mse102x: Fix possible double free of TX skb The scope of the TX skb is wider than just mse102x_tx_frame_spi(), so in case the TX skb room needs to be expanded, we should free the the temporary skb instead of the original skb. Otherwise the original TX skb pointer would be freed again in mse102x_tx_work(), which leads to crashes: Internal error: Oops: 0000000096000004 [#2] PREEMPT SMP CPU: 0 PID: 712 Comm: kworker/0:1 Tainted: G D 6.6.23 Hardware name: chargebyte Charge SOM DC-ONE (DT) Workqueue: events mse102x_tx_work [mse102x] pstate: 20400009 (nzCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : skb_release_data+0xb8/0x1d8 lr : skb_release_data+0x1ac/0x1d8 sp : ffff8000819a3cc0 x29: ffff8000819a3cc0 x28: ffff0000046daa60 x27: ffff0000057f2dc0 x26: ffff000005386c00 x25: 0000000000000002 x24: 00000000ffffffff x23: 0000000000000000 x22: 0000000000000001 x21: ffff0000057f2e50 x20: 0000000000000006 x19: 0000000000000000 x18: ffff00003fdacfcc x17: e69ad452d0c49def x16: 84a005feff870102 x15: 0000000000000000 x14: 000000000000024a x13: 0000000000000002 x12: 0000000000000000 x11: 0000000000000400 x10: 0000000000000930 x9 : ffff00003fd913e8 x8 : fffffc00001bc008 x7 : 0000000000000000 x6 : 0000000000000008 x5 : ffff00003fd91340 x4 : 0000000000000000 x3 : 0000000000000009 x2 : 00000000fffffffe x1 : 0000000000000000 x0 : 0000000000000000 Call trace: skb_release_data+0xb8/0x1d8 kfree_skb_reason+0x48/0xb0 mse102x_tx_work+0x164/0x35c [mse102x] process_one_work+0x138/0x260 worker_thread+0x32c/0x438 kthread+0x118/0x11c ret_from_fork+0x10/0x20 Code: aa1303e0 97fffab6 72001c1f 54000141 (f9400660)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50274	In the Linux kernel, the following vulnerability has been resolved: idpf: avoid vport access in idpf_get_link_ksettings When the device control plane is removed or the platform running device control plane is rebooted, a reset is detected on the driver. On driver reset, it releases the resources and waits for the reset to complete. If the reset fails, it takes the error path and releases the vport lock. At this time if the monitoring tools tries to access link settings, it call traces for accessing released vport pointer. To avoid it, move link_speed_mbps to netdev_priv structure which removes the dependency on vport pointer and the vport lock in idpf_get_link_ksettings. Also use netif_carrier_ok() to check the link status and adjust the offsetof to use link_up instead of link_speed_mbps.	7.8	More Details
CVE-2018-9339	In writeTypedArrayList and readTypedArrayList of Parcel.java, there is a possible escalation of privilege due to type confusion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-48990	Qualys discovered that needrestart, before version 3.8, allows local attackers to execute arbitrary code as root by tricking needrestart into running the Python interpreter with an attacker-controlled PYTHONPATH environment variable.	7.8	More Details
CVE-2024-43088	In multiple functions in AppInfoBase.java, there is a possible way to manipulate app permission settings belonging to another user on the device due to a missing permission check. This could lead to local escalation of privilege across user boundaries with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2018-9367	In FT_ACDK_CCT_V2_OP_ISP_SET_TUNING_PARAS of Meta_CCAP_Para.cpp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-35659	In DevmemIntChangeSparse of devicemem_server.c, there is a possible arbitrary code execution due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2018-9432	In createPhonebookDialogView and createMapDialogView of BluetoothPermissionActivity.java, there is a possible permissions bypass. This could lead to local escalation of privilege due to hiding and bypassing the user's ability to disable access to contacts, with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2018-9428	In startDevice of AAudioServiceStreamBase.cpp there is a possible out of bounds write due to a use after free. This could lead to local arbitrary code execution with no additional execution privileges needed. User interaction is needed for exploitation. https://source.android.com/security/bulletin/2018-07-01	7.8	More Details
CVE-2024-52565	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Teamcenter Visualization V2406 (All versions < V2406.0005), Tecnomatix Plant Simulation V2302 (All versions < V2302.0018), Tecnomatix Plant Simulation V2404 (All versions < V2404.0007). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24231)	7.8	More Details
CVE-2024-52945	An issue was discovered in Veritas NetBackup before 10.5. This only applies to NetBackup components running on a Windows Operating System. If a user executes specific NetBackup commands or an attacker uses social engineering techniques to impel the user to execute the commands, a malicious DLL could be loaded, resulting in execution of the attacker's code in the user's security context.	7.8	More Details
CVE-2024-52566	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Teamcenter Visualization V2406 (All versions < V2406.0005), Tecnomatix Plant Simulation V2302 (All versions < V2302.0018), Tecnomatix Plant Simulation V2404 (All versions < V2404.0007). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24233)	7.8	More Details
CVE-2018-9366	In IMSA_Recv_Thread and VT_IMCB_Thread of ImsaClient.cpp and VideoTelephony.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-52567	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Teamcenter Visualization V2406 (All versions < V2406.0005), Tecnomatix Plant Simulation V2302 (All versions < V2302.0018), Tecnomatix Plant Simulation V2404 (All versions < V2404.0007). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24237)	7.8	More Details
CVE-2024-52568	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Teamcenter Visualization V2406 (All versions < V2406.0005), Tecnomatix Plant Simulation V2302 (All versions < V2302.0018), Tecnomatix Plant Simulation V2404 (All versions < V2404.0007). The affected applications contain a use-after-free vulnerability that could be triggered while parsing specially crafted WRL files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-24244)	7.8	More Details
CVE-2024-52569	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Teamcenter Visualization V2406 (All versions < V2406.0005), Tecnomatix Plant Simulation V2302 (All versions < V2302.0018), Tecnomatix Plant Simulation V2404 (All versions < V2404.0007). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24260)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-9424	In CryptoPlugin::decrypt of CryptoPlugin.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-52570	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Teamcenter Visualization V2406 (All versions < V2406.0005), Tecnomatix Plant Simulation V2302 (All versions < V2302.0018), Tecnomatix Plant Simulation V2404 (All versions < V2404.0007). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24365)	7.8	More Details
CVE-2024-23715	In PMRWritePMPageList of pmr.c, there is a possible out of bounds write due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2018-9368	In mtkscoaudio debugfs there is a possible arbitrary kernel memory write due to missing bounds check and weakened SELinux policies. This could lead to local escalation of privilege with system execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-43087	In getInstalledAccessibilityPreferences of AccessibilitySettings.java, there is a possible way to hide an enabled accessibility service in the accessibility service settings due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2024-52571	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Teamcenter Visualization V2406 (All versions < V2406.0005), Tecnomatix Plant Simulation V2302 (All versions < V2302.0018), Tecnomatix Plant Simulation V2404 (All versions < V2404.0007). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24485)	7.8	More Details
CVE-2024-10013	In Progress Telerik UI for WinForms versions prior to 2024 Q4 (2024.4.1113), a code execution attack is possible through an insecure deserialization vulnerability.	7.8	More Details
CVE-2024-10012	In Progress Telerik UI for WPF versions prior to 2024 Q4 (2024.4.1111), a code execution attack is possible through an insecure deserialization vulnerability.	7.8	More Details
CVE-2018-9417	In f_hidg_read and hidg_disable of f_hid.c, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-47574	A authentication bypass using an alternate path or channel in Fortinet FortiClientWindows version 7.4.0, versions 7.2.4 through 7.2.0, versions 7.0.12 through 7.0.0, and 6.4.10 through 6.4.0 allows low privilege attacker to execute arbitrary code with high privilege via spoofed named pipe messages.	7.8	More Details
CVE-2024-52574	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Teamcenter Visualization V2406 (All versions < V2406.0005), Tecnomatix Plant Simulation V2302 (All versions < V2302.0018), Tecnomatix Plant Simulation V2404 (All versions < V2404.0007). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24543)	7.8	More Details
CVE-2018-9372	In cmd_flash_mmc_sparse_img of dl_commands.c, there is a possible out of bounds write due to a missing bounds check. This could lead to a local escalation of privilege in the bootloader with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2018-9409	In HWCSession::SetColorModeById of hwc_session.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-52573	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Teamcenter Visualization V2406 (All versions < V2406.0005), Tecnomatix Plant Simulation V2302 (All versions < V2302.0018), Tecnomatix Plant Simulation V2404 (All versions < V2404.0007). The affected applications contain an out of bounds write vulnerability when parsing a specially crafted WRL file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24521)	7.8	More Details
CVE-2023-35686	In PVRSRVRGXKickTA3DKM of rgxta3d.c, there is a possible arbitrary code execution due to improper input validation. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-50804	Insecure Permissions vulnerability in Micro-star International MSI Center Pro 2.1.37.0 allows a local attacker to execute arbitrary code via the Device_DeviceID.dat.bak file within the C:\ProgramData\MSI\One Dragon Center\Data folder	7.8	More Details
CVE-2024-52572	A vulnerability has been identified in Teamcenter Visualization V14.2 (All versions < V14.2.0.14), Teamcenter Visualization V14.3 (All versions < V14.3.0.12), Teamcenter Visualization V2312 (All versions < V2312.0008), Teamcenter Visualization V2406 (All versions < V2406.0005), Tecnomatix Plant Simulation V2302 (All versions < V2302.0018), Tecnomatix Plant Simulation V2404 (All versions < V2404.0007). The affected applications contain a stack based overflow vulnerability while parsing specially crafted WRL files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-24486)	7.8	More Details
CVE-2024-34729	In multiple locations, there is a possible arbitrary code execution due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-26074	A vulnerability in system file transfer functions of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to gain escalated privileges on the underlying operating system. The vulnerability is due to improper validation of path input to the system file transfer functions. An attacker could exploit this vulnerability by sending requests that contain specially crafted path variables to the vulnerable system. A successful exploit could allow the attacker to overwrite arbitrary files, allowing the attacker to modify the system in such a way that could allow the attacker to gain escalated privileges.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	7.8	More Details
CVE-2024-40661	In mayAdminGrantPermission of AdminRestrictedPermissionsUtils.java, there is a possible way to access the microphone due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-43080	In onReceive of AppRestrictionsFragment.java, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2024-40660	In setTransactionState of SurfaceFlinger.cpp, there is a possible way to change protected display attributes due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-43081	In installExistingPackageAsUser of InstallPackageHelper.java, there is a possible carrier restriction bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-31337	In PVRSRVRGXKickTA3DKM of rgxta3d.c, there is a possible arbitrary code execution due to improper input validation. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2018-9344	In several functions of DescramblerImpl.cpp, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-43085	In handleMessage of UsbDeviceManager.java, there is a possible method to access device contents over USB without unlocking the device due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-40671	In DevmemIntChangeSparse2 of devicemem_server.c, there is a possible way to achieve arbitrary code execution due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2018-9341	In impeg2d_mc_fullx_fully of impeg2d_mc.c there is a possible out of bound write due to missing bounds check. This could lead to remote arbitrary code execution with no additional execution privileges needed. User interaction is needed for exploitation.	7.8	More Details
CVE-2024-34747	In DevmemXIntMapPages of devicemem_server.c, there is a possible use-after-free due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-34719	In multiple locations, there is a possible permissions bypass due to a missing null check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-0793	A flaw was found in kube-controller-manager. This issue occurs when the initial application of a HPA config YAML lacking a .spec.behavior.scaleUp block causes a denial of service due to KCM pods going into restart churn.	7.7	More Details
CVE-2022-31666	Harbor fails to validate user permissions while deleting Webhook policies, allowing malicious users to view, update and delete Webhook policies of other users. The attacker could modify Webhook policies configured in other projects.	7.7	More Details
CVE-2024-49362	Joplin is a free, open source note taking and to-do application. Joplin-desktop has a vulnerability that leads to remote code execution (RCE) when a user clicks on an <a> link within untrusted notes. The issue arises due to insufficient sanitization of <a> tag attributes introduced by the Mermaid. This vulnerability allows the execution of untrusted HTML content within the Electron window, which has full access to Node.js APIs, enabling arbitrary shell command execution.	7.7	More Details
CVE-2024-52292	Craft is a content management system (CMS). The dataUrl function can be exploited if an attacker has write permissions on system notification templates. This function accepts an absolute file path, reads the file's content, and converts it into a Base64-encoded string. By embedding this function within a system notification template, the attacker can exfiltrate the Base64-encoded file content through a triggered system email notification. Once the email is received, the Base64 payload can be decoded, allowing the attacker to read arbitrary files on the server. This is fixed in 5.4.9 and 4.12.8.	7.7	More Details
CVE-2024-52595	lxml_html_clean is a project for HTML cleaning functionalities copied from `lxml.html.clean`. Prior to version 0.4.0, the HTML Parser in lxml does not properly handle context-switching for special HTML tags such as `<svg>`, `<math>` and `<noscript>`. This behavior deviates from how web browsers parse and interpret such tags. Specifically, content in CSS comments is ignored by lxml_html_clean but may be interpreted differently by web browsers, enabling malicious scripts to bypass the cleaning process. This vulnerability could lead to Cross-Site Scripting (XSS) attacks, compromising the security of users relying on lxml_html_clean in default configuration for sanitizing untrusted HTML content. Users employing the HTML cleaner in a security-sensitive context should upgrade to lxml 0.4.0, which addresses this issue. As a temporary mitigation, users can configure lxml_html_clean with the following settings to prevent the exploitation of this vulnerability. Via `remove_tags`, one may specify tags to remove - their content is moved to their parents' tags. Via `kill_tags`, one may specify tags to be removed completely. Via `allow_tags`, one may restrict the set of permissible tags, excluding context-switching tags like `<svg>`, `<math>` and `<noscript>`.	7.7	More Details
CVE-2024-45594	Decidim is a participatory democracy framework. The meeting embeds feature used in the online or hybrid meetings is subject to potential XSS attack through a malformed URL. This vulnerability is fixed in 0.28.3 and 0.29.0.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31670	Harbor fails to validate the user permissions when updating tag retention policies. By sending a request to update a tag retention policy with an id that belongs to a project that the currently authenticated user doesn't have access to, the attacker could modify tag retention policies configured in other projects.	7.7	More Details
CVE-2024-52360	IBM Concert Software 1.0.0, 1.0.1, 1.0.2, and 1.0.2.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify, or delete information in the back-end database.	7.6	More Details
CVE-2024-52436	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Post SMTP allows Blind SQL Injection.This issue affects Post SMTP: from n/a through 2.9.9.	7.6	More Details
CVE-2024-52435	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in W3 Eden, Inc. Premium Packages allows SQL Injection.This issue affects Premium Packages: from n/a through 5.9.3.	7.6	More Details
CVE-2024-52306	FileManager provides a Backpack admin interface for files and folder. Prior to 3.0.9, deserialization of untrusted data from the mimes parameter could lead to remote code execution. This vulnerability is fixed in 3.0.9.	7.6	More Details
CVE-2022-20685	A vulnerability in the Modbus preprocessor of the Snort detection engine could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to an integer overflow while processing Modbus traffic. An attacker could exploit this vulnerability by sending crafted Modbus traffic through an affected device. A successful exploit could allow the attacker to cause the Snort process to hang, causing traffic inspection to stop.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	7.5	More Details
CVE-2024-41784	IBM Sterling Secure Proxy 6.0.0.0, 6.0.0.1, 6.0.0.2, 6.0.0.3, and 6.1.0.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot dot" sequences (/.../) to view arbitrary files on the system.	7.5	More Details
CVE-2024-45254	VaeMendis - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	7.5	More Details
CVE-2024-47915	VaeMendis - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	7.5	More Details
CVE-2024-49754	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the API-Access page allows authenticated users to inject arbitrary JavaScript through the "token" parameter when creating a new API token. This vulnerability can result in the execution of malicious code in the context of other users' sessions, compromising their accounts and enabling unauthorized actions. This vulnerability is fixed in 24.10.0.	7.5	More Details
CVE-2024-47916	Boa web server - CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7.5	More Details
CVE-2024-28058	In RSA NetWitness (NW) Platform before 12.5.1, even when an administrator revokes the access of a specific user with an active session, an internal threat actor could impersonate the revoked user and gain unauthorized access to sensitive data.	7.5	More Details
CVE-2024-42384	Integer Overflow or Wraparound vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and produce a segmentation fault on the application.	7.5	More Details
CVE-2024-11237	A vulnerability, which was classified as critical, has been found in TP-Link VN020 F3v(T) TT_V6.2.1021. Affected by this issue is some unknown functionality of the component DHCP DISCOVER Packet Parser. The manipulation of the argument hostname leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.5	More Details
CVE-2024-50305	Valid Host header field can cause Apache Traffic Server to crash on some platforms. This issue affects Apache Traffic Server: from 9.2.0 through 9.2.5. Users are recommended to upgrade to version 9.2.6, which fixes the issue, or 10.0.2, which does not have the issue.	7.5	More Details
CVE-2024-10311	The External Database Based Actions plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 0.1. This is due to a missing capability check in the 'edba_admin_handle' function. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to update the plugin settings and log in as any existing user on the site, such as an administrator.	7.5	More Details
CVE-2024-45784	Apache Airflow versions before 2.10.3 contain a vulnerability that could expose sensitive configuration variables in task logs. This vulnerability allows DAG authors to unintentionally or intentionally log sensitive configuration variables. Unauthorized users could access these logs, potentially exposing critical data that could be exploited to compromise the security of the Airflow deployment. In version 2.10.3, secrets are now masked in task logs to prevent sensitive configuration variables from being exposed in the logging output. Users should upgrade to Airflow 2.10.3 or the latest version to eliminate this vulnerability. If you suspect that DAG authors could have logged the secret values to the logs and that your logs are not additionally protected, it is also recommended that you update those secrets.	7.5	More Details
CVE-2024-50968	A business logic vulnerability exists in the Add to Cart function of itsourcecode Agri-Trading Online Shopping System 1.0, which allows remote attackers to manipulate the quant parameter when adding a product to the cart. By setting the quantity value to -0, an attacker can exploit a flaw in the application's total price calculation logic. This vulnerability causes the total price to be reduced to zero, allowing the attacker to add items to the cart and proceed to checkout.	7.5	More Details
CVE-2024-3760	In lunary-ai/lunary version 1.2.7, there is a lack of rate limiting on the forgot password page, leading to an email bombing vulnerability. Attackers can exploit this by automating forgot password requests to flood targeted user accounts with a high volume of password reset emails. This not only overwhelms the victim's mailbox, making it difficult to manage and locate legitimate emails, but also significantly impacts mail servers by consuming their resources. The increased load can cause performance degradation and, in severe cases, make the mail servers unresponsive or unavailable, disrupting email services for the entire organization.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-52383	Missing Authorization vulnerability in KCT Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ai Auto Tool Content Writing Assistant (Gemini Writer, ChatGPT) All in One: from n/a through 2.1.2.	7.5	More Details
CVE-2022-2232	A flaw was found in the Keycloak package. This flaw allows an attacker to utilize an LDAP injection to bypass the username lookup or potentially perform other malicious actions.	7.5	More Details
CVE-2024-52378	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Labs64 DigiPass allows Absolute Path Traversal.This issue affects DigiPass: from n/a through 0.3.0.	7.5	More Details
CVE-2024-50647	The python_food ordering system V1.0 has an unauthorized vulnerability that leads to the leakage of sensitive user information. Attackers can access it through https://ip:port/api/myapp/index/user/info?id=1 And modify the ID value to obtain sensitive user information beyond authorization.	7.5	More Details
CVE-2024-11318	An IDOR (Insecure Direct Object Reference) vulnerability has been discovered in AbsysNet, affecting version 2.3.1. This vulnerability could allow a remote attacker to obtain the session of an unauthenticated user by brute-force attacking the session identifier on the "/cgi-bin/ocap/" endpoint.	7.5	More Details
CVE-2020-26073	A vulnerability in the application data endpoints of Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to gain access to sensitive information. The vulnerability is due to improper validation of directory traversal character sequences within requests to application programmatic interfaces (APIs). An attacker could exploit this vulnerability by sending malicious requests to an API within the affected application. A successful exploit could allow the attacker to conduct directory traversal attacks and gain access to sensitive information including credentials or user tokens.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	7.5	More Details
CVE-2024-45969	NULL pointer dereference in the MMS Client in MZ Automation LibIEC1850 before commit 7afa40390b26ad1f4cf93deaa0052fe7e357ef33 allows a malicious server to Cause a Denial-of-Service via the MMS InitiationResponse message.	7.5	More Details
CVE-2024-50650	python_book V1.0 is vulnerable to Incorrect Access Control, which allows attackers to obtain sensitive information of users with different IDs by modifying the ID parameter.	7.5	More Details
CVE-2024-50653	CRMEB <=5.4.0 is vulnerable to Incorrect Access Control. Users can bypass the front-end restriction of only being able to claim coupons once by capturing packets and sending a large number of data packets for coupon collection, achieving unlimited coupon collection.	7.5	More Details
CVE-2024-52303	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. In versions starting with 3.10.6 and prior to 3.10.11, a memory leak can occur when a request produces a MatchInfoError. This was caused by adding an entry to a cache on each request, due to the building of each MatchInfoError producing a unique cache entry. An attacker may be able to exhaust the memory resources of a server by sending a substantial number (100,000s to millions) of such requests. Those who use any middlewares with aiohttp.web should upgrade to version 3.10.11 to receive a patch.	7.5	More Details
CVE-2024-11310	The DVC from TRCore has a Path Traversal vulnerability, allowing unauthenticated remote attackers to exploit this vulnerability to read arbitrary system files.	7.5	More Details
CVE-2024-11309	The DVC from TRCore has a Path Traversal vulnerability, allowing unauthenticated remote attackers to exploit this vulnerability to read arbitrary system files.	7.5	More Details
CVE-2024-9935	The PDF Generator Addon for Elementor Page Builder plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 1.7.5 via the rtw_pgaepb_dwnld_pdf() function. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	7.5	More Details
CVE-2024-10645	The Blogger 301 Redirect plugin for WordPress is vulnerable to blind time-based SQL Injection via the ‘br’ parameter in all versions up to, and including, 2.5.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2024-52871	In Flagsmith before 2.134.1, it is possible to bypass the ALLOW_REGISTRATION_WITHOUT_INVITE setting.	7.5	More Details
CVE-2024-52876	Holy Stone Remote ID Module HSRID01, firmware distributed with the Drone Go2 mobile application before 1.1.8, allows unauthenticated "remote power off" actions (in broadcast mode) via multiple read operations on the ASTM Remote ID (0xFFFA) GATT.	7.5	More Details
CVE-2020-25720	A vulnerability was found in Samba where a delegated administrator with permission to create objects in Active Directory can write to all attributes of the newly created object, including security-sensitive attributes, even after the object's creation. This issue occurs because the administrator owns the object due to the lack of an Access Control List (ACL) at the time of creation and later being recognized as the 'creator owner.' The retained significant rights of the delegated administrator may not be well understood, potentially leading to unintended privilege escalation or security risks.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-25220	Bitcoin Core before 24.0.1 allows remote attackers to cause a denial of service (daemon crash) via a flood of low-difficulty header chains (aka a "Chain Width Expansion" attack) because a node does not first verify that a presented chain has enough work before committing to store it.	7.5	More Details
CVE-2024-38479	Improper Input Validation vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.11, from 9.0.0 through 9.2.5. Users are recommended to upgrade to version 9.2.6, which fixes the issue, or 10.0.2, which does not have the issue.	7.5	More Details
CVE-2024-52912	Bitcoin Core before 0.21.0 allows a network split that is resultant from an integer overflow (calculating the time offset for newly connecting peers) and an abs64 logic bug.	7.5	More Details
CVE-2024-21287	Vulnerability in the Oracle Agile PLM Framework product of Oracle Supply Chain (component: Software Development Kit, Process Extension). The supported version that is affected is 9.3.6. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Agile PLM Framework. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Agile PLM Framework accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2024-52914	In Bitcoin Core before 0.18.0, a node could be stalled for hours when processing the orphans of a crafted unconfirmed transaction.	7.5	More Details
CVE-2024-52915	Bitcoin Core before 0.20.0 allows remote attackers to cause a denial of service (memory consumption) via a crafted INV message.	7.5	More Details
CVE-2024-52916	Bitcoin Core before 0.15.0 allows a denial of service (OOM kill of a daemon process) via a flood of minimum difficulty headers.	7.5	More Details
CVE-2024-52920	Bitcoin Core before 0.20.0 allows remote attackers to cause a denial of service (infinite loop) via a malformed GETDATA message.	7.5	More Details
CVE-2024-52940	AnyDesk through 8.1.0 on Windows, when Allow Direct Connections is enabled, inadvertently exposes a public IP address within network traffic. The attacker must know the victim's AnyDesk ID.	7.5	More Details
CVE-2024-48917	PhpSpreadsheet is a PHP library for reading and writing spreadsheet files. The `XmlScanner` class has a scan method which should prevent XXE attacks. However, in a bypass of the previously reported `CVE-2024-47873`, the regexes from the `findCharSet` method, which is used for determining the current encoding can be bypassed by using a payload in the encoding UTF-7, and adding at end of the file a comment with the value `encoding="UTF-8"` with `"`, which is matched by the first regex, so that `encoding='UTF-7'` with single quotes `'` in the XML header is not matched by the second regex. An attacker can bypass the sanitizer and achieve an XML external entity attack. Versions 1.9.4, 2.1.3, 2.3.2, and 3.4.0 fix the issue.	7.5	More Details
CVE-2023-49952	Mastodon 4.1.x before 4.1.17 and 4.2.x before 4.2.9 allows a bypass of rate limiting via a crafted HTTP request header.	7.5	More Details
CVE-2024-47873	PhpSpreadsheet is a PHP library for reading and writing spreadsheet files. The XmlScanner class has a scan method which should prevent XXE attacks. However, prior to versions 1.9.4, 2.1.3, 2.3.2, and 3.4.0, the regexes used in the `scan` method and the findCharSet method can be bypassed by using UCS-4 and encoding guessing. An attacker can bypass the sanitizer and achieve an XML external entity attack. Versions 1.9.4, 2.1.3, 2.3.2, and 3.4.0 fix the issue.	7.5	More Details
CVE-2024-24453	An invalid memory access when handling the ProtocolIE_ID field of E-RAB NotToBeModifiedBearerModInd information element in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	7.5	More Details
CVE-2024-50654	lilishop <=4.2.4 is vulnerable to Incorrect Access Control, which can allow attackers to obtain coupons beyond the quantity limit by capturing and sending the data packets for coupon collection in high concurrency.	7.5	More Details
CVE-2023-39179	A flaw was found within the handling of SMB2 read requests in the kernel ksmbd module. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this to disclose sensitive information on affected installations of Linux. Only systems with ksmbd enabled are vulnerable to this CVE.	7.5	More Details
CVE-2024-45791	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache HertzBeat. This issue affects Apache HertzBeat: before 1.6.1. Users are recommended to upgrade to version 1.6.1, which fixes the issue.	7.5	More Details
CVE-2024-43416	GLPI is a free asset and IT management software package. Starting in version 0.80 and prior to version 10.0.17, an unauthenticated user can use an application endpoint to check if an email address corresponds to a valid GLPI user. Version 10.0.17 fixes the issue.	7.5	More Details
CVE-2024-24426	Reachable assertions in the NGAP_FIND_PROTOCOLIE_BY_ID function of OpenAirInterface Magma v1.8.0 and OAI EPC Federation v1.2.0 allow attackers to cause a Denial of Service (DoS) via a crafted NGAP packet.	7.5	More Details
CVE-2024-24431	A reachable assertion in the ogs_nas_emm_decode function of Open5GS v2.7.0 allows attackers to cause a Denial of Service (DoS) via a crafted NAS packet with a zero-length EMM message length.	7.5	More Details
CVE-2024-24452	An invalid memory access when handling the ProtocolIE_ID field of E-RAB Release Indication messages in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	7.5	More Details
CVE-2024-24454	An invalid memory access when handling the ProtocolIE_ID field of E-RAB Modify Request messages in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21539	Versions of the package @eslint/plugin-kit before 0.2.3 are vulnerable to Regular Expression Denial of Service (ReDoS) due to improper input sanitization. An attacker can increase the CPU usage and crash the program by exploiting this vulnerability.	7.5	More Details
CVE-2024-24455	An invalid memory access when handling a UE Context Release message containing an invalid UE identifier in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	7.5	More Details
CVE-2024-24457	An invalid memory access when handling the ProtocolIE_ID field of E-RAB Setup List Context SURes messages in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	7.5	More Details
CVE-2024-24458	An invalid memory access when handling the ENB Configuration Transfer messages containing invalid PLMN Identities in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	7.5	More Details
CVE-2024-24459	An invalid memory access when handling the ProtocolIE_ID field of S1Setup Request messages in Athonet vEPC MME v11.4.0 allows attackers to cause a Denial of Service (DoS) to the cellular network by repeatedly initiating connections and sending a crafted payload.	7.5	More Details
CVE-2024-44759	An arbitrary file download vulnerability in the component /Doc/DownloadFile of NUS-M9 ERP Management Software v3.0.0 allows attackers to download arbitrary files and access sensitive information via a crafted interface request.	7.5	More Details
CVE-2024-44757	An arbitrary file download vulnerability in the component /Basics/DownloadInpFile of NUS-M9 ERP Management Software v3.0.0 allows attackers to download arbitrary files and access sensitive information via a crafted interface request.	7.5	More Details
CVE-2024-8403	Improper Validation of Specified Type of Input vulnerability in Mitsubishi Electric Corporation MELSEC iQ-F Series FX5-ENET versions 1.100 and later and FX5-ENET/IP versions 1.100 to 1.104 allows a remote attacker to cause a Denial of Service condition in Ethernet communication of the products by sending specially crafted SLMP packets.	7.5	More Details
CVE-2024-45253	Avigilon – CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7.5	More Details
CVE-2024-52872	In Flagsmith before 2.134.1, the get_document endpoint is not correctly protected by permissions.	7.5	More Details
CVE-2018-9419	In l2cble_process_sig_cmd of l2c_ble.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2024-8935	CWE-290: Authentication Bypass by Spoofing vulnerability exists that could cause a denial of service and loss of confidentiality and integrity of controllers when conducting a Man-In-The-Middle attack between the controller and the engineering workstation while a valid user is establishing a communication session. This vulnerability is inherent to Diffie Hellman algorithm which does not protect against Man-In-The-Middle attacks.	7.5	More Details
CVE-2024-41167	Improper input validation in UEFI firmware in some Intel(R) Server Board M10JNP2SB Family may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2024-31158	Improper input validation in UEFI firmware in some Intel(R) Server Board S2600BP Family may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2024-39609	Improper Access Control in UEFI firmware for some Intel(R) Server Board M70KLP may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2024-9409	CWE-400: An Uncontrolled Resource Consumption vulnerability exists that could cause the device to become unresponsive resulting in communication loss when a large amount of IGMP packets is present in the network.	7.5	More Details
CVE-2024-4741	Issue summary: Calling the OpenSSL API function SSL_free_buffers may cause memory to be accessed that was previously freed in some situations Impact summary: A use after free can have a range of potential consequences such as the corruption of valid data, crashes or execution of arbitrary code. However, only applications that directly call the SSL_free_buffers function are affected by this issue. Applications that do not call this function are not vulnerable. Our investigations indicate that this function is rarely used by applications. The SSL_free_buffers function is used to free the internal OpenSSL buffer used when processing an incoming record from the network. The call is only expected to succeed if the buffer is not currently in use. However, two scenarios have been identified where the buffer is freed even when still in use. The first scenario occurs where a record header has been received from the network and processed by OpenSSL, but the full record body has not yet arrived. In this case calling SSL_free_buffers will succeed even though a record has only been partially processed and the buffer is still in use. The second scenario occurs where a full record containing application data has been received and processed by OpenSSL but the application has only read part of this data. Again a call to SSL_free_buffers will succeed even though the buffer is still in use. While these scenarios could occur accidentally during normal operation a malicious attacker could attempt to engineer a stituation where this occurs. We are not aware of this issue being actively exploited. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.	7.5	More Details
CVE-2024-48989	A vulnerability in the PROFINET stack implementation of the IndraDrive (all versions) of Bosch Rexroth allows an attacker to cause a denial of service, rendering the device unresponsive by sending arbitrary UDP messages.	7.5	More Details
CVE-2024-28028	Improper input validation in some Intel(R) Neural Compressor software before version v3.0 may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8933	CWE-924: Improper Enforcement of Message Integrity During Transmission in a Communication Channel vulnerability exists that could cause retrieval of password hash that could lead to denial of service and loss of confidentiality and integrity of controllers. To be successful, the attacker needs to inject themself inside the logical network while a valid user uploads or downloads a project file into the controller.	7.5	More Details
CVE-2024-31154	Improper input validation in UEFI firmware for some Intel(R) Server S2600BPBR may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2024-50955	An issue in how XINJE XD5E-24R and XL5E-16T v3.5.3b handles TCP protocol messages allows attackers to cause a Denial of Service (DoS) via a crafted TCP message.	7.5	More Details
CVE-2024-10816	The LUNA RADIO PLAYER plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 6.24.01.24 via the js/fallback.php file. This makes it possible for unauthenticated attackers to read the contents of arbitrary files on the server, which can contain sensitive information.	7.5	More Details
CVE-2024-52298	macro-pdfviewer is a PDF Viewer Macro for XWiki using Mozilla pdf.js. The PDF Viewer macro allows an attacker to view any attachment using the "Delegate my view right" feature as long as the attacker can view a page whose last author has access to the attachment. For this, the attacker only needs to provide the reference to a PDF file to the macro. To obtain the reference of the desired attachment, the attacker can access the Page Index, Attachments tab. Even if the UI shows N/A, the user can inspect the page and check the HTTP request that fetches the live data entries. The attachment URL is available in the returned JSON for all attachments, including protected ones and allows getting the necessary values. This vulnerability is fixed in version 2.5.6.	7.5	More Details
CVE-2024-52299	macro-pdfviewer is a PDF Viewer Macro for XWiki using Mozilla pdf.js. Any user with view right on XWiki.PDFViewerService can access any attachment stored in the wiki as the "key" that is passed to prevent this is computed incorrectly, calling skip on the digest stream doesn't update the digest. This is fixed in 2.5.6.	7.5	More Details
CVE-2024-51996	Symphony process is a module for the Symphony PHP framework which executes commands in sub-processes. When consuming a persisted remember-me cookie, Symfony does not check if the username persisted in the database matches the username attached with the cookie, leading to authentication bypass. This vulnerability is fixed in 5.4.47, 6.4.15, and 7.1.8.	7.5	More Details
CVE-2024-11206	Unauthorized access vulnerability in the mobile application (com.transsion.phoenix) can lead to the leakage of user information.	7.5	More Details
CVE-2018-9364	In the LG LAF component, there is a special command that allowed modification of certain partitions. This could lead to bypass of secure boot. User interaction is not needed for exploitation.	7.5	More Details
CVE-2024-40407	A full path disclosure in Cybele Software Thinfinity Workspace before v7.0.2.113 allows attackers to obtain the root path of the application via unspecified vectors.	7.5	More Details
CVE-2018-9456	In sdpu_extract_attr_seq of sdp_utils.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	7.5	More Details
CVE-2024-7730	A heap buffer overflow was found in the virtio-snd device in QEMU. When reading input audio in the virtio-snd input callback, virtio_snd_pcm_in_cb, the function did not check whether the iov can fit the data buffer. This issue can trigger an out-of-bounds write if the size of the virtio queue element is equal to virtio_snd_pcm_status, which makes the available space for audio data zero.	7.4	More Details
CVE-2023-4639	A flaw was found in Undertow, which incorrectly parses cookies with certain value-delimiting characters in incoming requests. This issue could allow an attacker to construct a cookie value to exfiltrate HttpOnly cookie values or spoof arbitrary additional cookie values, leading to unauthorized data access or modification. The main threat from this flaw impacts data confidentiality and integrity.	7.4	More Details
CVE-2022-20853	A vulnerability in the REST API of Cisco Expressway Series and Cisco TelePresence VCS could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected system. An attacker could exploit this vulnerability by persuading a user of the REST API to follow a crafted link. A successful exploit could allow the attacker to cause the affected system to reload. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	7.4	More Details
CVE-2022-31671	Harbor fails to validate user permissions when reading and updating job execution logs through the P2P preheat execution logs. By sending a request that attempts to read/update P2P preheat execution logs and specifying different job IDs, malicious authenticated users could read all the job logs stored in the Harbor database.	7.4	More Details
CVE-2022-31668	Harbor fails to validate the user permissions when updating p2p preheat policies. By sending a request to update a p2p preheat policy with an id that belongs to a project that the currently authenticated user doesn't have access to, the attacker could modify p2p preheat policies configured in other projects.	7.4	More Details
CVE-2022-20814	A vulnerability in the certificate validation of Cisco Expressway-C and Cisco TelePresence VCS could allow an unauthenticated, remote attacker to gain unauthorized access to sensitive data. The vulnerability is due to a lack of validation of the SSL server certificate that an affected device receives when it establishes a connection to a Cisco Unified Communications Manager device. An attacker could exploit this vulnerability by using a man-in-the-middle technique to intercept the traffic between the devices, and then using a self-signed certificate to impersonate the endpoint. A successful exploit could allow the attacker to view the intercepted traffic in clear text or alter the contents of the traffic. Note: Cisco Expressway-E is not affected by this vulnerability.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21541	All versions of the package dom-iterator are vulnerable to Arbitrary Code Execution due to use of the Function constructor without complete input sanitization. Function generates a new function body and thus care must be given to ensure that the inputs to Function are not attacker-controlled. The risks involved are similar to that of allowing attacker-controlled input to reach eval.	7.3	More Details
CVE-2024-11257	A vulnerability classified as critical has been found in 1000 Projects Beauty Parlour Management System 1.0. This affects an unknown part of the file /admin/forgot-password.php. The manipulation of the argument 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.	7.3	More Details
CVE-2024-40408	Cybele Software Thinfinity Workspace before v7.0.2.113 was discovered to contain an access control issue in the Create Profile section. This vulnerability allows attackers to create arbitrary user profiles with elevated privileges.	7.3	More Details
CVE-2024-11038	The The WPB Popup for Contact Form 7 – Showing The Contact Form 7 Popup on Button Click – CF7 Popup plugin for WordPress is vulnerable to arbitrary shortcode execution via wpb_pcf_fire_contact_form AJAX action in all versions up to, and including, 1.7.5. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-10174	The WP Project Manager – Task, team, and project management plugin featuring kanban board and gantt charts plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.6.13 via the 'Abstract_Permission' class due to missing validation on the 'user_id' user controlled key. This makes it possible for unauthenticated attackers to spoof their identity to that of an administrator and access all of the plugins REST routes.	7.3	More Details
CVE-2024-36488	Improper Access Control in some Intel(R) DSA before version 24.3.26.8 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.3	More Details
CVE-2024-11036	The The GamiPress – The #1 gamification plugin to reward points, achievements, badges & ranks in WordPress plugin for WordPress is vulnerable to arbitrary shortcode execution via gamipress_get_user_earnings AJAX action in all versions up to, and including, 7.1.5. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-11256	A vulnerability was found in 1000 Projects Portfolio Management System MCA 1.0 and classified as critical. This issue affects some unknown processing of the file /login.php. The manipulation of the argument username leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-5125	parisneo/lollms-webui version 9.6 is vulnerable to Cross-Site Scripting (XSS) and Open Redirect due to inadequate input validation and processing of SVG files during the upload process. The XSS vulnerability allows attackers to embed malicious JavaScript code within SVG files, which is executed upon rendering, leading to potential credential theft and unauthorized data access. The Open Redirect vulnerability arises from insufficient URL validation within SVG files, enabling attackers to redirect users to malicious websites, thereby exposing them to phishing attacks, malware distribution, and reputation damage. These vulnerabilities are present in the application's functionality to send files to the AI module.	7.3	More Details
CVE-2018-9369	In bootloader there is fastboot command allowing user specified kernel command line arguments. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2018-9370	In download.c there is a special mode allowing user to download data into memory and causing possible memory corruptions due to missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	7.3	More Details
CVE-2024-6068	A memory corruption vulnerability exists in the affected products when parsing DFT files. Local threat actors can exploit this issue to disclose information and to execute arbitrary code. To exploit this vulnerability a legitimate user must open a malicious DFT file.	7.3	More Details
CVE-2024-11258	A vulnerability classified as critical was found in 1000 Projects Beauty Parlour Management System 1.0. 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.	7.3	More Details
CVE-2024-9839	The The Uix Slideshow plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.6.5. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-11241	A vulnerability was found in code-projects Job Recruitment 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file reset.php. The manipulation of the argument e leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-50986	An issue in Clementine v.1.3.1 allows a local attacker to execute arbitrary code via a crafted DLL file.	7.3	More Details
CVE-2024-50828	A SQL Injection vulnerability was found in /admin/edit_department.php in kashipara E-learning Management System Project 1.0 via the d parameter.	7.2	More Details
CVE-2024-50824	A SQL Injection vulnerability was found in /admin/class.php in kashipara E-learning Management System Project 1.0 via the class_name parameter.	7.2	More Details
CVE-2024-50825	A SQL Injection vulnerability was found in /admin/school_year.php in kashipara E-learning Management System Project 1.0 via the school_year parameter.	7.2	More Details
CVE-2024-50835	A SQL Injection vulnerability was found in /admin/edit_student.php in KASHIPARA E-learning Management System Project 1.0 via the cys, un, ln, fn, and id parameters.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10793	The WP Activity Log plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the user_id parameter in all versions up to, and including, 5.2.1 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 an administrative user accesses an injected page.	7.2	More Details
CVE-2024-50826	A SQL Injection vulnerability was found in /admin/add_content.php in kashipara E-learning Management System Project 1.0 via the title and content parameters.	7.2	More Details
CVE-2024-50827	A SQL Injection vulnerability was found in /admin/add_subject.php in kashipara E-learning Management System Project 1.0 via the subject_code parameter.	7.2	More Details
CVE-2024-50829	A SQL Injection vulnerability was found in /admin/edit_subject.php in kashipara E-learning Management System Project 1.0 via the unit parameter.	7.2	More Details
CVE-2024-50830	A SQL Injection vulnerability was found in /admin/calendar_of_events.php in kashipara E-learning Management System Project 1.0 via the date_start, date_end, and title parameters.	7.2	More Details
CVE-2024-10388	The WordPress GDPR plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'gdpr_firstname' and 'gdpr_lastname' parameters in all versions up to, and including, 2.0.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2024-50831	A SQL Injection was found in /admin/admin_user.php in kashipara E-learning Management System Project 1.0 via the username and password parameters.	7.2	More Details
CVE-2024-10260	The Tripetto plugin for WordPress is vulnerable to Stored Cross-Site Scripting via File uploads in all versions up to, and including, 8.0.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses the file.	7.2	More Details
CVE-2024-9887	The Login using WordPress Users (WP as SAML IDP) plugin for WordPress is vulnerable to time-based SQL Injection via the ‘id’ parameter in all versions up to, and including, 1.15.6 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.2	More Details
CVE-2024-21820	Incorrect default permissions in some Intel(R) Xeon(R) processor memory controller configurations when using Intel(R) SGX may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	More Details
CVE-2024-9500	A maliciously crafted DLL file when placed in temporary files and folders that are leveraged by the Autodesk Installer could lead to escalation of privileges to NT AUTHORITY/SYSTEM due to insecure privilege management.	7.2	More Details
CVE-2024-32844	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-22185	Time-of-check Time-of-use Race Condition in some Intel(R) processors with Intel(R) ACTM may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	More Details
CVE-2024-24985	Exposure of resource to wrong sphere in some Intel(R) processors with Intel(R) ACTM may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	More Details
CVE-2024-50834	A SQL Injection was found in /admin/teachers.php in KASHIPARA E-learning Management System Project 1.0 via the firstname and lastname parameters.	7.2	More Details
CVE-2024-50972	A SQL injection vulnerability in printtool.php of Itsourcecode Construction Management System 1.0 allows remote attackers to execute arbitrary SQL commands via the borrow_id parameter.	7.2	More Details
CVE-2024-52293	Craft is a content management system (CMS). Prior to 4.12.2 and 5.4.3, Craft is missing normalizePath in the function FileHelper::absolutePath could lead to Remote Code Execution on the server via twig SSTI. This is a sequel to CVE-2023-40035. This vulnerability is fixed in 4.12.2 and 5.4.3.	7.2	More Details
CVE-2024-50971	A SQL injection vulnerability in print.php of Itsourcecode Construction Management System 1.0 allows remote attackers to execute arbitrary SQL commands via the map_id parameter.	7.2	More Details
CVE-2024-9474	A privilege escalation vulnerability in Palo Alto Networks PAN-OS software allows a PAN-OS administrator with access to the management web interface to perform actions on the firewall with root privileges. Cloud NGFW and Prisma Access are not impacted by this vulnerability.	7.2	More Details
CVE-2024-50832	A SQL Injection vulnerability was found in /admin/edit_class.php in kashipara E-learning Management System Project 1.0 via the class_name parameter.	7.2	More Details
CVE-2024-52388	Cross-Site Request Forgery (CSRF) vulnerability in Mike “Mikeage” Miller Hebrew Date allows Stored XSS.This issue affects Hebrew Date: from n/a through 2.1.0.	7.1	More Details
CVE-2024-51641	Cross-Site Request Forgery (CSRF) vulnerability in jcmlmorav Advanced PDF Generator allows Stored XSS.This issue affects Advanced PDF Generator: from n/a through 0.4.0.	7.1	More Details
CVE-2024-51642	Cross-Site Request Forgery (CSRF) vulnerability in webhostri Seo Free allows Stored XSS.This issue affects Seo Free: from n/a through 1.4.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51643	Cross-Site Request Forgery (CSRF) vulnerability in Rajan Agaskar Amazon Associate Filter allows Stored XSS.This issue affects Amazon Associate Filter: from n/a through 0.4.	7.1	More Details
CVE-2024-52417	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BoldThemes ReConstruction allows Reflected XSS.This issue affects ReConstruction: from n/a through 1.4.7.	7.1	More Details
CVE-2024-51640	Cross-Site Request Forgery (CSRF) vulnerability in Matt Rude MDR Webmaster Tools allows Stored XSS.This issue affects MDR Webmaster Tools: from n/a through 1.1.	7.1	More Details
CVE-2024-41974	A low privileged remote attacker may modify the BACNet service properties due to incorrect permission assignment for critical resources which may lead to a DoS limited to BACNet communication.	7.1	More Details
CVE-2024-52418	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CactusThemes Gameplan allows Reflected XSS.This issue affects Gameplan: from n/a through 1.5.10.	7.1	More Details
CVE-2024-53062	In the Linux kernel, the following vulnerability has been resolved: media: mgb4: protect driver against spectre Frequency range is set from sysfs via frequency_range_store(), being vulnerable to spectre, as reported by smatch: drivers/media/pci/mgb4/mgb4_cmt.c:231 mgb4_cmt_set_vin_freq_range() warn: potential spectre issue 'cmt_vals_in' [r] drivers/media/pci/mgb4/mgb4_cmt.c:238 mgb4_cmt_set_vin_freq_range() warn: possible spectre second half. 'reg_set' Fix it.	7.1	More Details
CVE-2024-51645	Cross-Site Request Forgery (CSRF) vulnerability in Themefuse ThemeFuse Maintenance Mode allows Stored XSS.This issue affects ThemeFuse Maintenance Mode: from n/a through 1.1.3.	7.1	More Details
CVE-2024-51639	Cross-Site Request Forgery (CSRF) vulnerability in Hints Naver Blog allows Stored XSS.This issue affects Naver Blog: from n/a through 1.0.	7.1	More Details
CVE-2024-51648	Cross-Site Request Forgery (CSRF) vulnerability in Hands, Inc e-shops allows Reflected XSS.This issue affects e-shops: from n/a through 1.0.3.	7.1	More Details
CVE-2024-50268	In the Linux kernel, the following vulnerability has been resolved: usb: typec: fix potential out of bounds in ucsi_ccg_update_set_new_cam_cmd() The "*cmd" variable can be controlled by the user via debugfs. That means "new_cam" can be as high as 255 while the size of the uc->updated[] array is UCSI_MAX_ALTMODES (30). The call tree is: ucsi_cmd() // val comes from simple_attr_write_xsigned() -> ucsi_send_command() -> ucsi_send_command_common() -> ucsi_run_command() // calls ucsi->ops->sync_control() -> ucsi_ccg_sync_control()	7.1	More Details
CVE-2024-50278	In the Linux kernel, the following vulnerability has been resolved: dm cache: fix potential out-of-bounds access on the first resume Out-of-bounds access occurs if the fast device is expanded unexpectedly before the first-time resume of the cache table. This happens because expanding the fast device requires reloading the cache table for cache_create to allocate new in-core data structures that fit the new size, and the check in cache_preresume is not performed during the first resume, leading to the issue. Reproduce steps: 1. prepare component devices: dmsetup create cmeta --table "0 8192 linear /dev/sdc 0" dmsetup create cdata --table "0 65536 linear /dev/sdc 8192" dmsetup create corig --table "0 524288 linear /dev/sdc 262144" dd if=/dev/zero of=/dev/mapper/cmeta bs=4k count=1 oflag=direct 2. load a cache table of 512 cache blocks, and deliberately expand the fast device before resuming the cache, making the in-core data structures inadequate. dmsetup create cache --notable dmsetup reload cache --table "0 524288 cache /dev/mapper/cmeta \ /dev/mapper/cdata /dev/mapper/corig 128 2 metadata2 writethrough smq 0" dmsetup reload cdata --table "0 131072 linear /dev/sdc 8192" dmsetup resume cdata dmsetup resume cache 3. suspend the cache to write out the in-core dirty bitset and hint array, leading to out-of-bounds access to the dirty bitset at offset 0x40: dmsetup suspend cache KASAN reports: BUG: KASAN: vmalloc-out-of-bounds in is_dirty_callback+0x2b/0x80 Read of size 8 at addr ffffc90000085040 by task dmsetup/90 (...snip...) The buggy address belongs to the virtual mapping at [ffffc90000085000, ffffc90000087000) created by: cache_ctr+0x176a/0x35f0 (...snip...) Memory state around the buggy address: ffffc90000084f00: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ffffc90000084f80: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 >ffffc90000085000: 00 00 00 00 00 00 00 00 f8 f8 f8 f8 f8 f8 f8 f8 ^ ffffc90000085080: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ffffc90000085100: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 Fix by checking the size change on the first resume.	7.1	More Details
CVE-2024-50279	In the Linux kernel, the following vulnerability has been resolved: dm cache: fix out-of-bounds access to the dirty bitset when resizing dm-cache checks the dirty bits of the cache blocks to be dropped when shrinking the fast device, but an index bug in bitset iteration causes out-of-bounds access. Reproduce steps: 1. create a cache device of 1024 cache blocks (128 bytes dirty bitset) dmsetup create cmeta --table "0 8192 linear /dev/sdc 0" dmsetup create cdata --table "0 131072 linear /dev/sdc 8192" dmsetup create corig --table "0 524288 linear /dev/sdc 262144" dd if=/dev/zero of=/dev/mapper/cmeta bs=4k count=1 oflag=direct dmsetup create cache --table "0 524288 cache /dev/mapper/cmeta \ /dev/mapper/cdata /dev/mapper/corig 128 2 metadata2 writethrough smq 0" 2. shrink the fast device to 512 cache blocks, triggering out-of-bounds access to the dirty bitset (offset 0x80) dmsetup suspend cache dmsetup reload cdata --table "0 65536 linear /dev/sdc 8192" dmsetup resume cdata dmsetup resume cache KASAN reports: BUG: KASAN: vmalloc-out-of-bounds in cache_preresume+0x269/0x7b0 Read of size 8 at addr ffffc900000f3080 by task dmsetup/131 (...snip...) The buggy address belongs to the virtual mapping at [ffffc900000f3000, ffffc900000f5000) created by: cache_ctr+0x176a/0x35f0 (...snip...) Memory state around the buggy address: ffffc900000f2f80: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ffffc900000f3000: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 >ffffc900000f3080: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ^ ffffc900000f3100: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 ffffc900000f3180: f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 f8 Fix by making the index post-incremented.	7.1	More Details
CVE-2024-51679	Cross-Site Request Forgery (CSRF) vulnerability in GentleSource Appointmind allows Stored XSS.This issue affects Appointmind: from n/a through 4.0.0.	7.1	More Details
CVE-2024-50522	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Redy Ru WeChat Subscribers Lite allows Reflected XSS.This issue affects WeChat Subscribers Lite : from n/a through 1.6.6.	7.1	More Details
CVE-2024-50534	Cross-Site Request Forgery (CSRF) vulnerability in Syed Umair Hussain Shah World Prayer Time allows Stored XSS.This issue affects World Prayer Time: from n/a through 2.0.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50533	Cross-Site Request Forgery (CSRF) vulnerability in David Garcia Domain Sharding allows Stored XSS.This issue affects Domain Sharding: from n/a through 1.2.1.	7.1	More Details
CVE-2024-50532	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jerin K Alexander Events Manager Pro – extended allows Reflected XSS.This issue affects Events Manager Pro – extended: from n/a through 0.1.	7.1	More Details
CVE-2024-51657	Cross-Site Request Forgery (CSRF) vulnerability in Woopy Plugins SmartLink Dynamic URLs allows Stored XSS.This issue affects SmartLink Dynamic URLs: from n/a through 1.1.0.	7.1	More Details
CVE-2024-51656	Cross-Site Request Forgery (CSRF) vulnerability in litefeel Flash Show And Hide Box allows Stored XSS.This issue affects Flash Show And Hide Box: from n/a through 1.6.	7.1	More Details
CVE-2024-51655	Cross-Site Request Forgery (CSRF) vulnerability in Microkid Custom Author URL allows Stored XSS.This issue affects Custom Author URL: from n/a through 2.0.1.	7.1	More Details
CVE-2024-51654	Cross-Site Request Forgery (CSRF) vulnerability in APK.Support APK Downloader allows Stored XSS.This issue affects APK Downloader: from n/a through 1.0.0.	7.1	More Details
CVE-2024-51649	Cross-Site Request Forgery (CSRF) vulnerability in Patrick Lumumba Mobilize allows Stored XSS.This issue affects Mobilize: from n/a through 3.0.7.	7.1	More Details
CVE-2024-51653	Cross-Site Request Forgery (CSRF) vulnerability in Mario Spinaci UPDATE NOTIFICATIONS allows Stored XSS.This issue affects UPDATE NOTIFICATIONS: from n/a through 0.3.4.	7.1	More Details
CVE-2024-51652	Cross-Site Request Forgery (CSRF) vulnerability in Prem Nawaz Khan, Victor Tsaran, Ron Feathers, and Marc Kocher Skip To allows Stored XSS.This issue affects Skip To: from n/a through 2.0.0.	7.1	More Details
CVE-2024-50301	In the Linux kernel, the following vulnerability has been resolved: security/keys: fix slab-out-of-bounds in key_task_permission KASAN reports an out of bounds read: BUG: KASAN: slab-out-of-bounds in __kuid_val include/linux/uidgid.h:36 BUG: KASAN: slab-out-of-bounds in uid_eq include/linux/uidgid.h:63 [inline] BUG: KASAN: slab-out-of-bounds in key_task_permission+0x394/0x410 security/keys/permission.c:54 Read of size 4 at addr ffff88813c3ab618 by task stress-ng/4362 CPU: 2 PID: 4362 Comm: stress-ng Not tainted 5.10.0-14930-gafbffd6c3ede #15 Call Trace: __dump_stack lib/dump_stack.c:82 [inline] dump_stack+0x107/0x167 lib/dump_stack.c:123 print_address_description.constprop.0+0x19/0x170 mm/kasan/report.c:400 __kasan_report.cold+0x6c/0x84 mm/kasan/report.c:560 kasan_report+0x3a/0x50 mm/kasan/report.c:585 __kuid_val include/linux/uidgid.h:36 [inline] uid_eq include/linux/uidgid.h:63 [inline] key_task_permission+0x394/0x410 security/keys/permission.c:54 search_nested_keyrings+0x90e/0xe90 security/keys/keyring.c:793 This issue was also reported by syzbot. It can be reproduced by following these steps(more details [1]): 1. Obtain more than 32 inputs that have similar hashes, which ends with the pattern '0xxxxxxxe6'. 2. Reboot and add the keys obtained in step 1. The reproducer demonstrates how this issue happened: 1. In the search_nested_keyrings function, when it iterates through the slots in a node(below tag ascend_to_node), if the slot pointer is meta and node->back_pointer != NULL(it means a root), it will proceed to descend_to_node. However, there is an exception. If node is the root, and one of the slots points to a shortcut, it will be treated as a keyring. 2. Whether the ptr is keyring decided by keyring_ptr_is_keyring function. However, KEYRING_PTR_SUBTYPE is 0x2UL, the same as ASSOC_ARRAY_PTR_SUBTYPE_MASK. 3. When 32 keys with the similar hashes are added to the tree, the ROOT has keys with hashes that are not similar (e.g. slot 0) and it splits NODE A without using a shortcut. When NODE A is filled with keys that all hashes are xxe6, the keys are similar, NODE A will split with a shortcut. Finally, it forms the tree as shown below, where slot 6 points to a shortcut. NODE A +------>+---+ ROOT I I 0 I xxe6 +---+ I +---+ xxxx I 0 I shortcut : : xxe6 +---+ I +---+ xxe6 : : I I I xxe6 +---+ I +---+ I 6 I---+ : : xxe6 +---+ +---+ xxe6 : : I f I xxe6 +---+ +---+ xxe6 I f I +---+ 4. As mentioned above, If a slot(slot 6) of the root points to a shortcut, it may be mistakenly transferred to a key*, leading to a read out-of-bounds read. To fix this issue, one should jump to descend_to_node if the ptr is a shortcut, regardless of whether the node is root or not. [1] https://lore.kernel.org/linux-kernel/1cfa878e-8c7b-4570-8606-21daf5e13ce7@huaweicloud.com/ [jarkko: tweaked the commit message a bit to have an appropriate closes tag.]	7.1	More Details
CVE-2024-52424	Cross-Site Request Forgery (CSRF) vulnerability in Suresh Kumar wp-login customizer allows Stored XSS.This issue affects wp-login customizer: from n/a through 1.0.	7.1	More Details
CVE-2024-51650	Cross-Site Request Forgery (CSRF) vulnerability in Scott @ MyDollarPlan.com Random Featured Post allows Stored XSS.This issue affects Random Featured Post: from n/a through 1.1.3.	7.1	More Details
CVE-2024-50519	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Visser Labs Jigoshop – Store Exporter allows Reflected XSS.This issue affects Jigoshop – Store Exporter: from n/a through 1.5.8.	7.1	More Details
CVE-2024-52421	Cross-Site Request Forgery (CSRF) vulnerability in wp-buy WP Popup Window Maker allows Stored XSS.This issue affects WP Popup Window Maker: from n/a through 2.0.	7.1	More Details
CVE-2024-51644	Cross-Site Request Forgery (CSRF) vulnerability in Sam Wilson Addressbook allows Stored XSS.This issue affects Addressbook: from n/a through 1.1.3.	7.1	More Details
CVE-2024-51659	Cross-Site Request Forgery (CSRF) vulnerability in GeekRMX Twitter @Anywhere Plus allows Stored XSS.This issue affects Twitter @Anywhere Plus: from n/a through 2.0.	7.1	More Details
CVE-2024-51684	Cross-Site Request Forgery (CSRF) vulnerability in Ciprian Popescu W3P SEO allows Stored XSS.This issue affects W3P SEO: from n/a before 1.8.6.	7.1	More Details
CVE-2024-53082	In the Linux kernel, the following vulnerability has been resolved: virtio_net: Add hash_key_length check Add hash_key_length check in virtnet_probe() to avoid possible out of bound errors when setting/reading the hash key.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21799	Path traversal for some Intel(R) Extension for Transformers software before version 1.5 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.1	More Details
CVE-2024-51634	Cross-Site Request Forgery (CSRF) vulnerability in Webriti WordPress Themes & Plugins Shop Webriti Custom Login allows Reflected XSS.This issue affects Webriti Custom Login: from n/a through 0.3.	7.1	More Details
CVE-2024-51633	Cross-Site Request Forgery (CSRF) vulnerability in IvyCat Web Services Simple Page Specific Sidebars allows Stored XSS.This issue affects Simple Page Specific Sidebars: from n/a through 2.14.1.	7.1	More Details
CVE-2024-51635	Cross-Site Request Forgery (CSRF) vulnerability in Garmur While Loading allows Stored XSS.This issue affects While Loading: from n/a through 3.0.	7.1	More Details
CVE-2024-51636	Cross-Site Request Forgery (CSRF) vulnerability in Z.com by GMO GMO Social Connection allows Cross-Site Scripting (XSS). This issue affects GMO Social Connection: from n/a through 1.2.	7.1	More Details
CVE-2024-51637	Cross-Site Request Forgery (CSRF) vulnerability in Scott E. Royalty Admin SMS Alert allows Stored XSS.This issue affects Admin SMS Alert: from n/a through 1.1.0.	7.1	More Details
CVE-2024-51638	Cross-Site Request Forgery (CSRF) vulnerability in Sanjeev Mohindra Awesome Shortcodes For Genesis allows Stored XSS.This issue affects Awesome Shortcodes For Genesis: from n/a through .8.	7.1	More Details
CVE-2024-51688	Cross-Site Request Forgery (CSRF) vulnerability in FraudLabs Pro FraudLabs Pro SMS Verification allows Stored XSS.This issue affects FraudLabs Pro SMS Verification: from n/a through 1.10.1.	7.1	More Details
CVE-2024-7295	In Progress® Telerik® Report Server versions prior to 2024 Q4 (10.3.24.1112), the encryption of local asset data used an older algorithm which may allow a sophisticated actor to decrypt this information.	7.1	More Details
CVE-2024-51687	Cross-Site Request Forgery (CSRF) vulnerability in Platform.Ly Platform.Ly Official allows Stored XSS.This issue affects Platform.Ly Official: from n/a through 1.1.3.	7.1	More Details
CVE-2024-51631	Cross-Site Request Forgery (CSRF) vulnerability in Eftakhairul Islam Sticky Social Bar allows Cross Site Request Forgery.This issue affects Sticky Social Bar: from n/a through 2.0.	7.1	More Details
CVE-2024-51632	Cross-Site Request Forgery (CSRF) vulnerability in Sam Hoe SH Slideshow allows Stored XSS.This issue affects SH Slideshow: from n/a through 4.3.	7.1	More Details
CVE-2024-51658	Cross-Site Request Forgery (CSRF) vulnerability in Henrik Hoff WP Course Manager allows Stored XSS.This issue affects WP Course Manager: from n/a through 1.3.	7.1	More Details
CVE-2024-39766	Improper neutralization of special elements used in SQL command in some Intel(R) Neural Compressor software before version v3.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	7.0	More Details
CVE-2024-50286	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix slab-use-after-free in ksmbd_smb2_session_create There is a race condition between ksmbd_smb2_session_create and ksmbd_expire_session. This patch add missing sessions_table_lock while adding/deleting session from global session table.	7.0	More Details
CVE-2024-50275	In the Linux kernel, the following vulnerability has been resolved: arm64/sve: Discard stale CPU state when handling SVE traps The logic for handling SVE traps manipulates saved FPSIMD/SVE state incorrectly, and a race with preemption can result in a task having TIF_SVE set and TIF_FOREIGN_FPSTATE clear even though the live CPU state is stale (e.g. with SVE traps enabled). This has been observed to result in warnings from do_sve_acc() where SVE traps are not expected while TIF_SVE is set: l if (test_and_set_thread_flag(TIF_SVE)) l WARN_ON(1); /* SVE access shouldn't have trapped */ Warnings of this form have been reported intermittently, e.g. https://lore.kernel.org/linux-arm-kernel/CA+G9fYtEGe_DhY2Ms7+L7NKsLYUomGsgqpdBj+QwDLeSg=JhGg@mail.gmail.com/ https://lore.kernel.org/linux-arm-kernel/000000000000511e9a060ce5a45c@google.com/ The race can occur when the SVE trap handler is preempted before and after manipulating the saved FPSIMD/SVE state, starting and ending on the same CPU, e.g. l void do_sve_acc(unsigned long esr, struct pt_regs *regs) l { l // Trap on CPU 0 with TIF_SVE clear, SVE traps enabled l // task->fpsimd_cpu is 0. l // per_cpu_ptr(&fpsimd_last_state, 0) is task. l l ... l l // Preempted; migrated from CPU 0 to CPU 1. l // TIF_FOREIGN_FPSTATE is set. l l get_cpu_fpsimd_context(); l l if (test_and_set_thread_flag(TIF_SVE)) l WARN_ON(1); /* SVE access shouldn't have trapped */ l l sve_init_regs() { l if (!test_thread_flag(TIF_FOREIGN_FPSTATE)) { l ... l } else { l fpsimd_to_sve(current); l current->thread.fp_type = FP_STATE_SVE; l } l } l l put_cpu_fpsimd_context(); l l // Preempted; migrated from CPU 1 to CPU 0. l // task->fpsimd_cpu is still 0 l // If per_cpu_ptr(&fpsimd_last_state, 0) is still task then: l // - Stale HW state is reused (with SVE traps enabled) l // - TIF_FOREIGN_FPSTATE is cleared l // - A return to userspace skips HW state restore l } Fix the case where the state is not live and TIF_FOREIGN_FPSTATE is set by calling fpsimd_flush_task_state() to detach from the saved CPU state. This ensures that a subsequent context switch will not reuse the stale CPU state, and will instead set TIF_FOREIGN_FPSTATE, forcing the new state to be reloaded from memory prior to a return to userspace.	7.0	More Details
CVE-2021-1440	A vulnerability in the implementation of the Resource Public Key Infrastructure (RPKI) feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause the Border Gateway Protocol (BGP) process to crash, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of a specific RPKI to Router (RTR) Protocol packet header. An attacker could exploit this vulnerability by compromising the RPKI validator server and sending a specifically crafted RTR packet to an affected device. Alternatively, the attacker could use man-in-the-middle techniques to impersonate the RPKI validator server and send a specifically crafted RTR response packet over the established RTR TCP connection to the affected device. A successful exploit could allow the attacker to cause a DoS condition because the BGP process could constantly restart and BGP routing could become unstable.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.This advisory is part of the September 2021 release of the Cisco IOS XR Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see .	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-22067	ZTE NH8091 product has an improper permission control vulnerability. Due to improper permission control of the Web module interface, an authenticated attacker may exploit the vulnerability to execute arbitrary commands.	6.8	More Details
CVE-2024-32044	Improper access control for some Intel(R) Arc(TM) Pro Graphics for Windows drivers before version 31.0.101.5319 may allow an authenticated user to potentially enable escalation of privilege via adjacent access.	6.8	More Details
CVE-2024-10921	An authorized user may trigger crashes or receive the contents of buffer over-reads of Server memory by issuing specially crafted requests that construct malformed BSON in the MongoDB Server. This issue affects MongoDB Server v5.0 versions prior to 5.0.30 , MongoDB Server v6.0 versions prior to 6.0.19, MongoDB Server v7.0 versions prior to 7.0.15 and MongoDB Server v8.0 versions prior to and including 8.0.2.	6.8	More Details
CVE-2024-29079	Insufficient control flow management in some Intel(R) VROC software before version 8.6.0.3001 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.8	More Details
CVE-2024-7404	An issue was discovered in GitLab CE/EE affecting all versions starting from 17.2 prior to 17.3.7, starting from 17.4 prior to 17.4.4 and starting from 17.5 prior to 17.5.2, which could have allowed an attacker gaining full API access as the victim via the Device OAuth flow.	6.8	More Details
CVE-2021-3740	A Session Fixation vulnerability exists in chatwoot/chatwoot versions prior to 2.4.0. The application does not invalidate existing sessions on other devices when a user changes their password, allowing old sessions to persist. This can lead to unauthorized access if an attacker has obtained a session token.	6.8	More Details
CVE-2022-20793	A vulnerability in pairing process of Cisco TelePresence CE Software and RoomOS Software for Cisco Touch 10 Devices could allow an unauthenticated, remote attacker to impersonate a legitimate device and pair with an affected device. This vulnerability is due to insufficient identity verification. An attacker could exploit this vulnerability by impersonating a legitimate device and responding to the pairing broadcast from an affected device. A successful exploit could allow the attacker to access the affected device while impersonating a legitimate device.There are no workarounds that address this vulnerability.	6.8	More Details
CVE-2024-34167	Uncontrolled search path for the Intel(R) Server Board S2600ST Family BIOS and Firmware Update software all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-36294	Insecure inherited permissions for some Intel(R) DSA software before version 24.3.26.8 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-34049	The Salt-SSH pre-flight option copies the script to the target at a predictable path, which allows an attacker to force Salt-SSH to run their script. If an attacker has access to the target VM and knows the path to the pre-flight script before it runs they can ensure Salt-SSH runs their script with the privileges of the user running Salt-SSH. Do not make the copy path on the target predictable and ensure we check return codes of the scp command if the copy fails.	6.7	More Details
CVE-2023-20090	A vulnerability in Cisco TelePresence CE and RoomOS could allow an authenticated, local attacker to elevate privileges to root on an affected device. This vulnerability is due to improper access control on certain CLI commands. An attacker could exploit this vulnerability by running a series of crafted commands. A successful exploit could allow the attacker to elevate privileges to root. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.7	More Details
CVE-2024-36253	Uncontrolled search path in the Intel(R) SDP Tool for Windows software all version may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-34028	Uncontrolled search path in some Intel(R) Graphics Offline Compiler for OpenCL(TM) Code software for Windows before version 2024.1.0.142, graphics driver 31.0.101.5445 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-34165	Uncontrolled search path in some Intel(R) oneAPI DPC++/C++ Compiler before version 2024.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-34164	Uncontrolled search path element in some Intel(R) MAS software before version 2.5 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-38668	Uncontrolled search path for some Intel(R) Quartus(R) Prime Standard Edition software for Windows before version 23.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-36245	Uncontrolled search path element in some Intel(R) VTune(TM) Profiler software before version 2024.2.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-49592	Trial installer for McAfee Total Protection (legacy trial installer software) 16.0.53 allows local privilege escalation because of an Uncontrolled Search Path Element. The attacker could be "an adversary or knowledgeable user" and the type of attack could be called "DLL-squatting." The issue only affects execution of this installer, and does not leave McAfee Total Protection in a vulnerable state after installation is completed. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	6.7	More Details
CVE-2024-31407	Uncontrolled search path in some Intel(R) High Level Synthesis Compiler software for Intel(R) Quartus(R) Prime Pro Edition Software before version 24.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-37024	Uncontrolled search path for some ACAT software maintained by Intel(R) for Windows before version 3.11.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2017-13311	In the read() function of ProcessStats.java, there is a possible read/write serialization issue leading to a permissions bypass. This could lead to local escalation of privilege where an app can start an activity with system privileges with no additional execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2024-34022	Improper Access Control in some Thunderbolt(TM) Share software before version 1.0.49.9 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-36276	Insecure inherited permissions for some Intel(R) CIP software before version 2.4.10852 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-23312	Uncontrolled search path for some Intel(R) Binary Configuration Tool software for Windows before version 3.4.5 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-25647	Incorrect default permissions for some Intel(R) Binary Configuration Tool software for Windows before version 3.4.5 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-35245	Uncontrolled search path element in some Intel(R) PROSet/Wireless WiFi software for Windows before version 23.60 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-38383	Uncontrolled search path for some Intel(R) Quartus(R) Prime Pro Edition software for Windows before version 24.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-38387	Uncontrolled search path in the Intel(R) Graphics Driver installers for versions 15.40 and 15.45 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-35201	Incorrect default permissions in the Intel(R) SDP Tool for Windows software all versions may allow an authenticated user to enable escalation of privilege via local access.	6.7	More Details
CVE-2024-37025	Incorrect execution-assigned permissions in some Intel(R) Advanced Link Analyzer Standard Edition software installer before version 23.1.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-28950	Uncontrolled search path for some Intel(R) oneAPI Math Kernel Library software for Windows before version 2024.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-28952	Uncontrolled search path for some Intel(R) IPP software for Windows before version 2021.12.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-28881	Uncontrolled search path for some Intel(R) Fortran Compiler Classic software before version 2021.13 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-29077	Improper access control in some JAM STAPL Player software before version 2.6.1 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-26017	Uncontrolled search path in some Intel(R) Rendering Toolkit software before version 2024.1.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2021-34752	A vulnerability in the CLI of Cisco FTD Software could allow an authenticated, local attacker with administrative privileges to execute arbitrary commands with root privileges on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user-supplied command arguments. An attacker could exploit this vulnerability by submitting crafted input to the affected commands. A successful exploit could allow the attacker to execute commands with root privileges on the underlying operating system. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.7	More Details
CVE-2024-29083	Incorrect default permissions in some Intel(R) Distribution for Python software before version 2024.2 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-23198	Improper input validation in firmware for some Intel(R) PROSet/Wireless Software and Intel(R) Killer(TM) Wi-Fi products before version 23.40 may allow an unauthenticated user to enable denial of service via adjacent access.	6.6	More Details
CVE-2024-34170	Improper buffer restrictions in some Intel(R) Graphics Drivers may allow an authenticated user to potentially enable denial of service via local access.	6.6	More Details
CVE-2024-9529	The Secure Custom Fields WordPress plugin before 6.3.9, Secure Custom Fields WordPress plugin before 6.3.6.3, Advanced Custom Fields Pro WordPress plugin before 6.3.9 does not prevent users from running arbitrary functions through its setting import functionalities, which could allow high privilege users such as admin to run arbitrary PHP functions.	6.6	More Details
CVE-2024-51926	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wpsoul GreenCon allows Stored XSS.This issue affects GreenCon: from n/a through 1.0.1.	6.5	More Details
CVE-2024-48071	E-cology has a directory traversal vulnerability. An attacker can exploit this vulnerability to delete the server directory, causing the server to permanently deny service.	6.5	More Details
CVE-2024-41678	GLPI is a free asset and IT management software package. An unauthenticated user can provide a malicious link to a GLPI technician in order to exploit a reflected XSS vulnerability. Upgrade to 10.0.17.	6.5	More Details
CVE-2024-41679	GLPI is a free asset and IT management software package. An authenticated user can exploit a SQL injection vulnerability from the ticket form. Upgrade to 10.0.17.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50517	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SlovenskoIT a.s. ID-SK Toolkit allows Stored XSS.This issue affects ID-SK Toolkit: from n/a through 1.7.2.	6.5	More Details
CVE-2024-51927	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Codember Rig Elements For Elementor allows DOM-Based XSS.This issue affects Rig Elements For Elementor: from n/a through 1.0.	6.5	More Details
CVE-2024-50518	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Common Ninja Pricer Ninja allows Stored XSS.This issue affects Pricer Ninja: from n/a through 2.1.0.	6.5	More Details
CVE-2024-24446	An uninitialized pointer dereference in OpenAirInterface CN5G AMF up to v2.0.0 allows attackers to cause a Denial of Service (DoS) via a crafted InitialContextSetupResponse message sent to the AMF.	6.5	More Details
CVE-2024-43417	GLPI is a free asset and IT management software package. An unauthenticated user can provide a malicious link to a GLPI technician in order to exploit a reflected XSS vulnerability located in the Software form. Upgrade to 10.0.17.	6.5	More Details
CVE-2024-10524	Applications that use Wget to access a remote resource using shorthand URLs and pass arbitrary user credentials in the URL are vulnerable. In these cases attackers can enter crafted credentials which will cause Wget to access an arbitrary host.	6.5	More Details
CVE-2024-24425	Magma v1.8.0 and OAI EPC Federation v1.20 were discovered to contain an out-of-bounds read in the amf_as_establish_req function at /tasks/amf/amf_as.cpp. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted NAS packet.	6.5	More Details
CVE-2024-50521	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in alleythemes Alley Elementor Widget allows DOM-Based XSS.This issue affects Alley Elementor Widget: from n/a through 1.0.7.	6.5	More Details
CVE-2024-51928	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jakir Hasan Blocks Post Grid allows DOM-Based XSS.This issue affects Blocks Post Grid: from n/a through 1.0.3.	6.5	More Details
CVE-2024-50520	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Peter J. Herrel Ancient World Linked Data allows DOM-Based XSS.This issue affects Ancient World Linked Data: from n/a through 0.2.1.	6.5	More Details
CVE-2024-51929	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Phil Spectrum Icon Widget allows DOM-Based XSS.This issue affects Icon Widget: from n/a through 1.1.0.	6.5	More Details
CVE-2024-24449	An uninitialized pointer dereference in the NasPdu::NasPdu component of OpenAirInterface CN5G AMF up to v2.0.0 allows attackers to cause a Denial of Service (DoS) via a crafted InitialUEMessage message sent to the AMF.	6.5	More Details
CVE-2024-51940	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in sohelwpexpert WP Responsive Video allows DOM-Based XSS.This issue affects WP Responsive Video: from n/a through 1.0.	6.5	More Details
CVE-2024-43418	GLPI is a free asset and IT management software package. An unauthenticated user can provide a malicious link to a GLPI technician in order to exploit a reflected XSS vulnerability. Upgrade to 10.0.17.	6.5	More Details
CVE-2024-24984	Improper input validation for some Intel(R) Wireless Bluetooth(R) products for Windows before version 23.40 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2024-52917	Bitcoin Core before 22.0 has a miniupnp infinite loop in which it allocates memory on the basis of random data received over the network, e.g., large M-SEARCH replies from a fake UPnP device.	6.5	More Details
CVE-2024-52918	Bitcoin-Qt in Bitcoin Core before 0.20.0 allows remote attackers to cause a denial of service (memory consumption and application crash) via a BIP21 r parameter for a URL that has a large file.	6.5	More Details
CVE-2024-52919	Bitcoin Core before 22.0 has a CAddrMan nIdCount integer overflow and resultant assertion failure (and daemon exit) via a flood of addr messages.	6.5	More Details
CVE-2024-11193	An information disclosure vulnerability exists in Yugabyte Anywhere, where the LDAP bind password is logged in plaintext within application logs. This flaw results in the unintentional exposure of sensitive information in Yugabyte Anywhere logs, potentially allowing unauthorized users with access to these logs to view the LDAP bind password. An attacker with log access could exploit this vulnerability to gain unauthorized access to the LDAP server, leading to potential exposure or compromise of LDAP-managed resources This issue affects YugabyteDB Anywhere: from 2.20.0.0 before 2.20.7.0, from 2.23.0.0 before 2.23.1.0, from 2024.1.0.0 before 2024.1.3.0.	6.5	More Details
CVE-2024-52922	In Bitcoin Core before 25.1, an attacker can cause a node to not download the latest block, because there can be minutes of delay when an announcing peer stalls instead of complying with the peer-to-peer protocol specification.	6.5	More Details
CVE-2024-52926	Delinea Privilege Manager before 12.0.2 mishandles the security of the Windows agent.	6.5	More Details
CVE-2018-9348	In SMF_ParseMetaEvent of eas_smf.c, there is a possible integer overflow. This could lead to remote denial of service due to resource exhaustion with no additional execution privileges needed. User interaction is needed for exploitation.	6.5	More Details
CVE-2024-50848	An XML External Entity (XXE) vulnerability in the Import object and Translation Memory import functionalities of WorldServer v11.8.2 to access sensitive information and execute arbitrary commands via supplying a crafted .tmx file.	6.5	More Details
CVE-2024-8049	In Progress Telerik Document Processing Libraries, versions prior to 2024 Q4 (2024.4.1106), importing a document with unsupported features can lead to excessive processing, leading to excessive use of computing resources leaving the application process unavailable.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-52305	UnoPim is an open-source Product Information Management (PIM) system built on the Laravel framework. A vulnerability exists in the Create User process, allowing the creation of a new admin account with an option to upload a profile image. An attacker can upload a malicious SVG file containing an embedded script. When the profile image is accessed, the embedded script executes, leading to the potential theft of session cookies. This vulnerability is fixed in 0.1.5.	6.5	More Details
CVE-2024-48293	Incorrect access control in QuickHeal Antivirus Pro 24.1.0.182 and earlier allows authenticated attackers with low-level privileges to arbitrarily modify antivirus settings.	6.5	More Details
CVE-2024-45422	Improper input validation in some Zoom Apps before version 6.2.0 may allow an unauthenticated user to conduct a denial of service via network access.	6.5	More Details
CVE-2024-10717	The Styler for Ninja Forms plugin for WordPress is vulnerable to unauthorized modification of data that can lead to a denial of service due to a missing capability check on the deactivate_license function in all versions up to, and including, 3.3.4. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary option values on the WordPress site. This can be leveraged to delete an option that would create an error on the site and deny service to legitimate users. Note: This issue can also be used to add arbitrary options with an empty value.	6.5	More Details
CVE-2024-41972	A low privileged remote attacker can overwrite an arbitrary file on the filesystem which may lead to an arbitrary file read with root privileges.	6.5	More Details
CVE-2024-8937	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause a potential arbitrary code execution after a successful Man-In-The Middle attack followed by sending a crafted Modbus function call to tamper with memory area involved in the authentication process.	6.5	More Details
CVE-2024-8936	CWE-20: Improper Input Validation vulnerability exists that could lead to loss of confidentiality of controller memory after a successful Man-In-The-Middle attack followed by sending a crafted Modbus function call used to tamper with memory.	6.5	More Details
CVE-2024-52426	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Linear Oy Linear linear allows DOM-Based XSS.This issue affects Linear: from n/a through 2.7.11.	6.5	More Details
CVE-2024-52425	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Urchenko Drozd – Addons for Elementor allows Stored XSS.This issue affects Drozd – Addons for Elementor: from n/a through 1.1.1.	6.5	More Details
CVE-2024-52423	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Themify Themify Builder allows Stored XSS.This issue affects Themify Builder: from n/a through 7.6.3.	6.5	More Details
CVE-2024-52422	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Terry Lin WP Githuber MD allows Stored XSS.This issue affects WP Githuber MD: from n/a through 1.16.3.	6.5	More Details
CVE-2024-52419	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Clipboard Team Copy Anything to Clipboard allows Stored XSS.This issue affects Copy Anything to Clipboard: from n/a through 4.0.3.	6.5	More Details
CVE-2024-52317	Incorrect object re-cycling and re-use vulnerability in Apache Tomcat. Incorrect recycling of the request and response used by HTTP/2 requests could lead to request and/or response mix-up between users. This issue affects Apache Tomcat: from 11.0.0-M23 through 11.0.0-M26, from 10.1.27 through 10.1.30, from 9.0.92 through 9.0.95. Users are recommended to upgrade to version 11.0.0, 10.1.31 or 9.0.96, which fixes the issue.	6.5	More Details
CVE-2021-1379	Multiple vulnerabilities in the Cisco Discovery Protocol and Link Layer Discovery Protocol (LLDP) implementations for Cisco IP Phone Series 68xx/78xx/88xx could allow an unauthenticated, adjacent attacker to execute code remotely or cause a reload of an affected IP phone. These vulnerabilities are due to missing checks when the IP phone processes a Cisco Discovery Protocol or LLDP packet. An attacker could exploit these vulnerabilities by sending a malicious Cisco Discovery Protocol or LLDP packet to the targeted IP phone. A successful exploit could allow the attacker to execute code on the affected IP phone or cause it to reload unexpectedly, resulting in a denial of service (DoS) condition.Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit these vulnerabilities, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.	6.5	More Details
CVE-2021-1232	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to read arbitrary files on the underlying filesystem of an affected system. This vulnerability is due to insufficient access control for sensitive information that is written to an affected system. An attacker could exploit this vulnerability by accessing sensitive information that they are not authorized to access on an affected system. A successful exploit could allow the attacker to gain access to devices and other network management systems that they should not have access to.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.5	More Details
CVE-2024-37155	OpenCTI is an open source platform allowing organizations to manage their cyber threat intelligence knowledge and observables. Prior to version 6.1.9, the regex validation used to prevent Introspection queries can be bypassed by removing the extra whitespace, carriage return, and line feed characters from the query. GraphQL Queries in OpenCTI can be validated using the `secureIntrospectionPlugin`. The regex check in the plkugin can be bypassed by removing the carriage return and line feed characters (`\r\n`). Running a curl command against a local instance of OpenCTI will result in a limited error message. By running the same Introspection query without the `\r\n` characters, the unauthenticated user is able to successfully run a full Introspection query. Bypassing this restriction allows the attacker to gather a wealth of information about the GraphQL endpoint functionality that can be used to perform actions and/or read data without authorization. These queries can also be weaponized to conduct a Denial of Service (DoS) attack if sent repeatedly. Users should upgrade to version 6.1.9 to receive a patch for the issue.	6.5	More Details
CVE-2024-30424	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WPZOOM Beaver Builder Addons by WPZOOM allows Stored XSS.This issue affects Beaver Builder Addons by WPZOOM: from n/a through 1.3.4.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-9440	In parse of M3UParser.cpp there is a possible resource exhaustion due to improper input validation. This could lead to denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	6.5	More Details
CVE-2024-52341	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Offshorent Solutions Pvt Ltd.	Jinesh.P.V OS Our Team allows Stored XSS.This issue affects OS Our Team: from n/a through 1.7.	6.5	More Details
CVE-2024-52342	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Offshorent Solutions Pvt Ltd.	Jinesh.P.V OS BXSlider allows Stored XSS.This issue affects OS BXSlider: from n/a through 2.6.	6.5	More Details
CVE-2024-45608	GLPI is a free asset and IT management software package. An authenticated user can perfom a SQL injection by changing its preferences. Upgrade to 10.0.17.	6.5	More Details
CVE-2024-52343	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Offshorent Softwares Pvt. Ltd.	Jinesh.P.V OS Pricing Tables allows Stored XSS.This issue affects OS Pricing Tables: from n/a through 1.2.	6.5	More Details
CVE-2024-31141	Files or Directories Accessible to External Parties, Improper Privilege Management vulnerability in Apache Kafka Clients. Apache Kafka Clients accept configuration data for customizing behavior, and includes ConfigProvider plugins in order to manipulate these configurations. Apache Kafka also provides FileConfigProvider, DirectoryConfigProvider, and EnvVarConfigProvider implementations which include the ability to read from disk or environment variables. In applications where Apache Kafka Clients configurations can be specified by an untrusted party, attackers may use these ConfigProviders to read arbitrary contents of the disk and environment variables. In particular, this flaw may be used in Apache Kafka Connect to escalate from REST API access to filesystem/environment access, which may be undesirable in certain environments, including SaaS products. This issue affects Apache Kafka Clients: from 2.3.0 through 3.5.2, 3.6.2, 3.7.0. Users with affected applications are recommended to upgrade kafka-clients to version >=3.8.0, and set the JVM system property "org.apache.kafka.automatic.config.providers=none". Users of Kafka Connect with one of the listed ConfigProvider implementations specified in their worker config are also recommended to add appropriate "allowlist.pattern" and "allowed.paths" to restrict their operation to appropriate bounds. For users of Kafka Clients or Kafka Connect in environments that trust users with disk and environment variable access, it is not recommended to set the system property. For users of the Kafka Broker, Kafka MirrorMaker 2.0, Kafka Streams, and Kafka command-line tools, it is not recommended to set the system property.	6.5	More Details
CVE-2024-11069	The WordPress GDPR plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the 'WordPress_GDPR_Data_Delete::check_action' function in all versions up to, and including, 2.0.2. This makes it possible for unauthenticated attackers to delete arbitrary users.	6.5	More Details
CVE-2024-51930	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jie Wang Custom URL Shortener allows Stored XSS.This issue affects Custom URL Shortener: from n/a through 0.3.6.	6.5	More Details
CVE-2024-51931	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Marketever AzonBox allows DOM-Based XSS.This issue affects AzonBox: from n/a through 1.1.2.	6.5	More Details
CVE-2024-51932	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saif Bin-Alam Kings Tab Slider allows DOM-Based XSS.This issue affects Kings Tab Slider: from n/a through 1.0.	6.5	More Details
CVE-2024-51933	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Christian Ladewig Cookie Nonsense for YT allows DOM-Based XSS.This issue affects Cookie Nonsense for YT: from n/a through 1.2.0.	6.5	More Details
CVE-2024-51934	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Uri Lazcano (Urielink) Ekiline Block Collection allows DOM-Based XSS.This issue affects Ekiline Block Collection: from n/a through 1.0.5.	6.5	More Details
CVE-2024-45609	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. An unauthenticated user can provide a malicious link to a GLPI technician in order to exploit a reflected XSS vulnerability located in the reports pages. Upgrade to 10.0.17.	6.5	More Details
CVE-2024-32048	Improper input validation in the Intel(R) Distribution of OpenVINO(TM) Model Server software before version 2024.0 may allow an unauthenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2024-45610	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. An unauthenticated user can provide a malicious link to a GLPI technician in order to exploit a reflected XSS vulnerability located in the Cable form. Upgrade to 10.0.17.	6.5	More Details
CVE-2017-13313	In ElementaryStreamQueue::dequeueAccessUnitMPEG4Video of ESQueue.cpp, there is a possible infinite loop leading to resource exhaustion due to an incorrect bounds check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	6.5	More Details
CVE-2024-51935	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sam Perrow Fast Video and Image Display allows DOM-Based XSS.This issue affects Fast Video and Image Display: from n/a through 2.5.2.	6.5	More Details
CVE-2024-51936	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Henry ESB Testimonials allows Stored XSS.This issue affects ESB Testimonials: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51937	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Information Analytics IA Map Analytics Basic allows DOM-Based XSS.This issue affects IA Map Analytics Basic: from n/a through 20170413.	6.5	More Details
CVE-2024-51938	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NicheAddons Charity Addon for Elementor allows DOM-Based XSS.This issue affects Charity Addon for Elementor: from n/a through 1.3.2.	6.5	More Details
CVE-2024-52340	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Marty Thornley Photographer Connections allows Stored XSS.This issue affects Photographer Connections: from n/a through 1.3.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-52339	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mage Cast Mage Front End Forms allows Stored XSS.This issue affects Mage Front End Forms: from n/a through 1.1.4.	6.5	More Details
CVE-2024-50536	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Intuitive Design GDReseller allows DOM-Based XSS.This issue affects GDReseller: from n/a through 1.6.	6.5	More Details
CVE-2024-51939	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Santhosh veer Stylish Internal Links allows DOM-Based XSS.This issue affects Stylish Internal Links: from n/a through 1.9.	6.5	More Details
CVE-2024-52394	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in nopea.Media Print PDF Generator and Publisher allows Stored XSS.This issue affects Print PDF Generator and Publisher: from n/a through 1.1.6.	6.5	More Details
CVE-2024-52389	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Job Portal allows Stored XSS.This issue affects WP Job Portal: from n/a through 2.2.0.	6.5	More Details
CVE-2024-52349	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Md. Shiddikur Rahman Awesome Tool Tip allows DOM-Based XSS.This issue affects Awesome Tool Tip: from n/a through 1.0.	6.5	More Details
CVE-2024-52348	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in aaextention AA Audio Player allows DOM-Based XSS.This issue affects AA Audio Player: from n/a through 1.0.	6.5	More Details
CVE-2024-52347	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP website creator Website remote Install vor Gravity, WPForms, Formidable, Ninja, Caldera allows Stored XSS.This issue affects Website remote Install vor Gravity, WPForms, Formidable, Ninja, Caldera: from n/a through 4.0.	6.5	More Details
CVE-2024-52346	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Javier Méndez Veira SimpleGMaps allows Stored XSS.This issue affects SimpleGMaps: from n/a through 1.0.	6.5	More Details
CVE-2024-52345	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Roberto Alicata ra_qrcode allows Stored XSS.This issue affects ra_qrcode: from n/a through 2.1.0.	6.5	More Details
CVE-2024-52344	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Muhammad Junaid Provide Forex Signals allows Stored XSS.This issue affects Provide Forex Signals: from n/a through 1.0.	6.5	More Details
CVE-2024-50535	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kyle M. Brown Step by Step allows Stored XSS.This issue affects Step by Step: from n/a through 0.4.5.	6.5	More Details
CVE-2024-51908	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Gonzalo Geraldo Adventure Bucket List allows DOM-Based XSS.This issue affects Adventure Bucket List: from n/a through 1.0.9.	6.5	More Details
CVE-2024-50537	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Stefano Marra Smart Mockups allows Stored XSS.This issue affects Smart Mockups: from n/a through 1.2.0.	6.5	More Details
CVE-2024-51918	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Freshlight Lab Pay With Stripe allows DOM-Based XSS.This issue affects Pay With Stripe: from n/a through 1.2.1.	6.5	More Details
CVE-2024-51857	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Olympus Themes Olympus Shortcodes allows DOM-Based XSS.This issue affects Olympus Shortcodes: from n/a through 1.0.4.	6.5	More Details
CVE-2024-51858	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Umar Social Locker allows Stored XSS.This issue affects Social Locker: from n/a through 1.1.	6.5	More Details
CVE-2024-51859	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bamboo Mcr Bamboo Enquiries allows Stored XSS.This issue affects Bamboo Enquiries: from n/a through 1.9.3.	6.5	More Details
CVE-2024-51860	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DuoGeek Custom Dashboard Widget allows Stored XSS.This issue affects Custom Dashboard Widget: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51921	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in midori scrollup allows DOM-Based XSS.This issue affects scrollup: from n/a through 1.1.	6.5	More Details
CVE-2024-51861	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in duogeek EventPress allows Stored XSS.This issue affects EventPress: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51862	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Baptiste Wicht Google Visualization Charts allows Stored XSS.This issue affects Google Visualization Charts: from n/a through 0.1.	6.5	More Details
CVE-2024-51920	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in JDev Map Store Locator allows DOM-Based XSS.This issue affects Map Store Locator: from n/a through 1.2.1.	6.5	More Details
CVE-2024-51917	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Huy Le Multiple Votes in one page allows Stored XSS.This issue affects Multiple Votes in one page: from n/a through 1.0.4.	6.5	More Details
CVE-2024-51855	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Productineer Redirecter allows DOM-Based XSS.This issue affects Redirecter: from n/a through 1.0.	6.5	More Details
CVE-2024-51863	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Team Profit-Funnels PF Timer allows Stored XSS.This issue affects PF Timer: from n/a through 1.0.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50956	A buffer overflow in the RecvSocketData function of Inovance HCPLC_AM401-CPU1608TPTN 21.38.0.0, HCPLC_AM402-CPU1608TPTN 41.38.0.0, and HCPLC_AM403-CPU1608TN 81.38.0.0 allows attackers to cause a Denial of Service (DoS) or execute arbitrary code via a crafted Modbus message.	6.5	More Details
CVE-2024-51864	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Agnel Waghela Shortcode Collection allows Stored XSS.This issue affects Shortcode Collection: from n/a through 1.4.	6.5	More Details
CVE-2024-51027	Ruijie NBR800G gateway NBR_RGOS_11.1(6)B4P9 is vulnerable to command execution in /itbox_pi/networksafe.php via the province parameter.	6.5	More Details
CVE-2024-51865	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in N.O.U.S. Open Useful and Simple Simple Social Share Block allows Stored XSS.This issue affects Simple Social Share Block: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51866	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mr. Riponshah Social button allows Stored XSS.This issue affects Social button: from n/a through 1.3.	6.5	More Details
CVE-2024-51867	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alexander Conroy Simpul Events by Esotech allows Stored XSS.This issue affects Simpul Events by Esotech: from n/a through 1.8.5.	6.5	More Details
CVE-2024-51868	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DuoGeek DuoGeek Blocks allows Stored XSS.This issue affects DuoGeek Blocks: from n/a through .1.	6.5	More Details
CVE-2024-51856	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Moose Moose Elementor Kit allows DOM-Based XSS.This issue affects Moose Elementor Kit: from n/a through 1.0.0.	6.5	More Details
CVE-2024-45877	baltic-it TOPqw Webportal v1.35.283.2 is vulnerable to Incorrect Access Control in the User Management function in /Apps/TOPqw/BenutzerManagement.aspx. This allows a low privileged user to access all modules in the web portal, view and manipulate information and permissions of other users, lock other user or unlock the own account, change the password of other users, create new users or delete existing users and view, manipulate and delete reference data.	6.5	More Details
CVE-2024-51836	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Teconce Wezido allows DOM-Based XSS.This issue affects Wezido: from n/a through 1.2.	6.5	More Details
CVE-2024-51849	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Marco Piarulli My Restaurant Menu allows Stored XSS.This issue affects My Restaurant Menu: from n/a through 0.2.0.	6.5	More Details
CVE-2024-51839	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Meini Utech Spinning Earth allows DOM-Based XSS.This issue affects Utech Spinning Earth: from n/a through 1.2.	6.5	More Details
CVE-2024-51840	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rezaul haque Wd-image-magnifier-xoss allows DOM-Based XSS.This issue affects Wd-image-magnifier-xoss: from n/a through 1.0.	6.5	More Details
CVE-2024-51841	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeNcode File Select Control For Elementor allows DOM-Based XSS.This issue affects File Select Control For Elementor: from n/a through 1.3.	6.5	More Details
CVE-2024-51842	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sazzad Hu Image Carousel Shortcode allows DOM-Based XSS.This issue affects Image Carousel Shortcode: from n/a through 1.2.	6.5	More Details
CVE-2024-51844	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Kiran Patil Location Click Map allows Stored XSS.This issue affects Location Click Map: from n/a through 1.0.	6.5	More Details
CVE-2024-51846	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michael Simpson Community Yard Sale allows Stored XSS.This issue affects Community Yard Sale: from n/a through 1.1.11.	6.5	More Details
CVE-2024-50538	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Irfan Ardiansah Show Visitor IP Address allows Stored XSS.This issue affects Show Visitor IP Address: from n/a through 0.2.	6.5	More Details
CVE-2024-51848	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Digital Zoom Studio Parallaxer allows Stored XSS.This issue affects Parallaxer: from n/a through 1.00.	6.5	More Details
CVE-2024-51850	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bchristopeit WoW Guild Armory Roster allows Stored XSS.This issue affects WoW Guild Armory Roster: from n/a through 0.5.5.	6.5	More Details
CVE-2024-51854	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hola Networks Hola Free Video Player allows DOM-Based XSS.This issue affects Hola Free Video Player: from n/a through 1.3.9.	6.5	More Details
CVE-2024-51922	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Maruf Arafat VP Sitemap allows Stored XSS.This issue affects VP Sitemap: from n/a through 1.0.	6.5	More Details
CVE-2024-45876	The login form of baltic-it TOPqw Webportal v1.35.283.2 (fixed in version 1.35.283.4) at /Apps/TOPqw/Login.aspx is vulnerable to SQL injection. The vulnerability exists in the POST parameter txtUsername, which allows for manipulation of SQL queries.	6.5	More Details
CVE-2024-51851	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in saleh attari best bootstrap widgets for elementor allows DOM-Based XSS.This issue affects best bootstrap widgets for elementor: from n/a through 1.0.	6.5	More Details
CVE-2024-49776	A negative-size-param in tsMuxer version nightly-2024-04-05-01-53-02 allows attackers to cause Denial of Service (DoS) via a crafted TS video file.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41217	A heap-based buffer overflow in tsMuxer version nightly-2024-05-10-02-00-45 allows attackers to cause Denial of Service (DoS) via a crafted MKV video file.	6.5	More Details
CVE-2024-51852	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DynamicWebLab Dynamic Post Grid Elementor Addon allows DOM-Based XSS.This issue affects Dynamic Post Grid Elementor Addon: from n/a through 1.0.6.	6.5	More Details
CVE-2024-41206	A stack-based buffer over-read in tsMuxer version nightly-2024-03-14-01-51-12 allows attackers to cause Information Disclosure via a crafted TS video file.	6.5	More Details
CVE-2024-51853	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alberuni Azad Faltu Testimonial Rotator allows DOM-Based XSS.This issue affects Faltu Testimonial Rotator: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51869	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Best WP Developer Gutenium Blocks allows Stored XSS.This issue affects Gutenium Blocks: from n/a through 1.1.5.	6.5	More Details
CVE-2024-51870	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in aniketji007 Ultimate Flipbox Addon for Elementor allows Stored XSS.This issue affects Ultimate Flipbox Addon for Elementor: from n/a through .4.	6.5	More Details
CVE-2024-51871	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Luzuk Luzuk Team allows Stored XSS.This issue affects Luzuk Team: from n/a through 0.1.0.	6.5	More Details
CVE-2024-51901	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wojciech Borowicz Smooth Maps allows Stored XSS.This issue affects Smooth Maps: from n/a through 1.1.	6.5	More Details
CVE-2024-51894	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Reyzua Topbar ID for Elementor allows DOM-Based XSS.This issue affects Topbar ID for Elementor: from n/a through 1.0.1.	6.5	More Details
CVE-2024-51895	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Minical Minical Hotel Booking Plugin allows Stored XSS.This issue affects Minical Hotel Booking Plugin: from n/a through 1.0.2.	6.5	More Details
CVE-2024-51896	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in webvitaly Magic Slider allows Stored XSS.This issue affects Magic Slider: from n/a through 1.3.	6.5	More Details
CVE-2024-51897	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Erik Saulnier News Articles allows Stored XSS.This issue affects News Articles: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51898	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sachin Jadhav Semantic Shortcode allows Stored XSS.This issue affects Semantic Shortcode: from n/a through 1.0.1.	6.5	More Details
CVE-2024-51914	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Gopi Ramasamy drop in image slideshow gallery allows DOM-Based XSS.This issue affects drop in image slideshow gallery: from n/a through 12.0.	6.5	More Details
CVE-2024-51913	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mapme Mapme allows Stored XSS.This issue affects Mapme: from n/a through 1.3.2.	6.5	More Details
CVE-2024-51899	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SEO Themes Simple Pricing Table allows Stored XSS.This issue affects Simple Pricing Table: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51902	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Oliver Schaal TinyCode allows Stored XSS.This issue affects TinyCode: from n/a through 1.2.1.	6.5	More Details
CVE-2024-51872	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Luzuk Luzuk Testimonials allows Stored XSS.This issue affects Luzuk Testimonials: from n/a through 0.0.1.	6.5	More Details
CVE-2024-51903	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in imFORZA WP Listings Pro allows Stored XSS.This issue affects WP Listings Pro: from n/a through 3.0.14.	6.5	More Details
CVE-2024-51904	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Joan Boluda Embed documents shortcode allows Stored XSS.This issue affects Embed documents shortcode: from n/a through 1.5.	6.5	More Details
CVE-2024-51905	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ravi & Suma RSV PDF Preview allows Stored XSS.This issue affects RSV PDF Preview: from n/a through 1.0.	6.5	More Details
CVE-2024-51906	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rapid Sort RSV 360 View allows DOM-Based XSS.This issue affects RSV 360 View: from n/a through 1.0.	6.5	More Details
CVE-2024-51912	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Lilaea Media IntelliWidget Elements allows DOM-Based XSS.This issue affects IntelliWidget Elements: from n/a through 2.2.7.	6.5	More Details
CVE-2024-51911	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ketan Patel Featured product by category name allows DOM-Based XSS.This issue affects Featured product by category name: from n/a through 1.1.	6.5	More Details
CVE-2024-51907	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in codemenschen WP Virtual Room Configurator allows Stored XSS.This issue affects WP Virtual Room Configurator: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51910	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mauro Cordioli Assist24 Help Desk allows DOM-Based XSS.This issue affects Assist24 Help Desk: from n/a through 20150401.2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51893	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeAtelier Postify: Post Layout For Elementor allows DOM-Based XSS.This issue affects Postify: Post Layout For Elementor: from n/a through 1.0.1.	6.5	More Details
CVE-2024-51892	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in naa986 Sell Media File with Stripe allows Stored XSS.This issue affects Sell Media File with Stripe: from n/a through 1.0.6.	6.5	More Details
CVE-2024-51891	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 4B Systems sp. z o.o Official SalesWizard CRM Plugin allows Stored XSS.This issue affects Official SalesWizard CRM Plugin: from n/a through 1.0.2.	6.5	More Details
CVE-2024-51890	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in geoWP Geoportail Shortcode allows Stored XSS.This issue affects Geoportail Shortcode: from n/a through 2.4.4.	6.5	More Details
CVE-2024-51873	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in matorel Multi-day Booking Calendar allows DOM-Based XSS.This issue affects Multi-day Booking Calendar: from n/a through 1.0.1.	6.5	More Details
CVE-2024-51874	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ParOne, Inc. ParOne Feeds allows DOM-Based XSS.This issue affects ParOne Feeds: from n/a through 1.17.1.	6.5	More Details
CVE-2024-51875	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nazmul Ahsan MDC YouTube Downloader allows DOM-Based XSS.This issue affects MDC YouTube Downloader: from n/a through 3.0.0.	6.5	More Details
CVE-2024-51876	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Codstack Team wp_automatic_widget allows DOM-Based XSS.This issue affects wp_automatic_widget: from n/a through 1.0.1.	6.5	More Details
CVE-2024-51877	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in straightvisions GmbH SV Forms allows DOM-Based XSS.This issue affects SV Forms: from n/a through 2.0.05.	6.5	More Details
CVE-2024-51916	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Creative Brahma Multifox Plus allows DOM-Based XSS.This issue affects Multifox Plus: from n/a through 1.1.6.	6.5	More Details
CVE-2024-51878	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Joey Straile AchillesTheme-shortcodes allows DOM-Based XSS.This issue affects AchillesTheme-shortcodes: from n/a through 0.1.	6.5	More Details
CVE-2024-51879	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Arash Heidari Text Advertisements allows Stored XSS.This issue affects Text Advertisements: from n/a through 2.1.	6.5	More Details
CVE-2024-51880	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BeBetter Hotels BeBetter Social Icons allows DOM-Based XSS.This issue affects BeBetter Social Icons: from n/a through 2.7.	6.5	More Details
CVE-2024-51881	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Beautimour Be Shortcodes allows DOM-Based XSS.This issue affects Be Shortcodes: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51883	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Micha I Plant A Tree allows Stored XSS.This issue affects I Plant A Tree: from n/a through 1.7.3.	6.5	More Details
CVE-2024-51884	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Takashi Matsuyama Posts Search allows Stored XSS.This issue affects Posts Search: from n/a through 1.2.2.	6.5	More Details
CVE-2024-11215	Absolute path traversal (incorrect restriction of a path to a restricted directory) vulnerability in the EasyPHP web server, affecting version 14.1. This vulnerability could allow remote users to bypass SecurityManager restrictions and retrieve any file stored on the server by setting only consecutive strings '/...%5c'.	6.5	More Details
CVE-2024-51885	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Takashi Matsuyama Browsing History allows Stored XSS.This issue affects Browsing History: from n/a through 1.3.1.	6.5	More Details
CVE-2024-51886	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Takashi Matsuyama Posts Filter allows Stored XSS.This issue affects Posts Filter: from n/a through 1.3.1.	6.5	More Details
CVE-2024-51887	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ryan Sutana NV Slider allows Stored XSS.This issue affects NV Slider: from n/a through 1.6.	6.5	More Details
CVE-2024-51889	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GeroNikolov Fancy User List allows Stored XSS.This issue affects Fancy User List: from n/a through 3.1.	6.5	More Details
CVE-2024-51838	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jon Smajda Pull This allows DOM-Based XSS.This issue affects Pull This: from n/a through 1.1.	6.5	More Details
CVE-2024-51847	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in giovanebribeiro WP PagSeguro Payments allows Stored XSS.This issue affects WP PagSeguro Payments: from n/a through 1.0.	6.5	More Details
CVE-2024-51796	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPManageNinja Trendy Restaurant Menu allows DOM-Based XSS.This issue affects Trendy Restaurant Menu: from n/a through 1.0.0.	6.5	More Details
CVE-2024-50552	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jason Pancake Hover Video Preview allows Stored XSS.This issue affects Hover Video Preview: from n/a through 1.0.2.	6.5	More Details
CVE-2024-51812	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wasim Pro Addons For Elementor allows Stored XSS.This issue affects Pro Addons For Elementor: from n/a through 1.5.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51811	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hussam Hussien Popup Image allows Stored XSS.This issue affects Popup Image: from n/a through 1.0.1.	6.5	More Details
CVE-2024-51810	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in George Lewe Lewe Bootstrap Visuals allows Stored XSS.This issue affects Lewe Bootstrap Visuals: from n/a through 2.2.2.	6.5	More Details
CVE-2024-51809	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in George Rood Keymaster Chord Notation Free allows Stored XSS.This issue affects Keymaster Chord Notation Free: from n/a through 1.0.2.	6.5	More Details
CVE-2024-51808	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pat O'Brien codeSnips allows Stored XSS.This issue affects codeSnips: from n/a through 1.2.	6.5	More Details
CVE-2024-51807	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Black and White Digital Ltd AgendaPress – Easily Publish Meeting Agendas and Programs on WordPress allows Stored XSS.This issue affects AgendaPress – Easily Publish Meeting Agendas and Programs on WordPress: from n/a through 1.0.8.	6.5	More Details
CVE-2024-51806	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Shingo Suzumura at Fitness Website Formula Awesome Fitness Testimonials allows Stored XSS.This issue affects Awesome Fitness Testimonials: from n/a through 1.0.1.	6.5	More Details
CVE-2024-51805	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Yonatan Reinberg yPHPlista allows Stored XSS.This issue affects yPHPlista: from n/a through 1.1.1.	6.5	More Details
CVE-2024-51804	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bob Matsuoka Moka Get Posts Shortcode allows DOM-Based XSS.This issue affects Moka Get Posts Shortcode: from n/a through 1.0.	6.5	More Details
CVE-2022-20652	A vulnerability in the web-based management interface and in the API subsystem of Cisco Tetration could allow an authenticated, remote attacker to inject arbitrary commands to be executed with root-level privileges on the underlying operating system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by submitting a crafted HTTP message to the affected system. A successful exploit could allow the attacker to execute commands with root-level privileges. To exploit this vulnerability, an attacker would need valid administrator-level credentials.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.5	More Details
CVE-2024-51803	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Magnetic Creative Inline Click To Tweet allows DOM-Based XSS.This issue affects Inline Click To Tweet: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51802	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bread & Butter IO Inc. Bread & Butter allows DOM-Based XSS.This issue affects Bread & Butter: from n/a through 7.4.857.	6.5	More Details
CVE-2022-20656	A vulnerability in the web-based management interface of Cisco PI and Cisco EPNM could allow an authenticated, remote attacker to conduct a path traversal attack on an affected device. To exploit this vulnerability, the attacker must have valid credentials on the system. This vulnerability is due to insufficient input validation of the HTTPS URL by the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request that contains directory traversal character sequences to an affected device. A successful exploit could allow the attacker to write arbitrary files to the host system. Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.	6.5	More Details
CVE-2024-51801	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jake Brown Brand my Footer allows DOM-Based XSS.This issue affects Brand my Footer: from n/a through 1.1.	6.5	More Details
CVE-2024-51799	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in VBog Bg Patriarchia BU allows DOM-Based XSS.This issue affects Bg Patriarchia BU: from n/a through 2.2.3.	6.5	More Details
CVE-2021-1484	A vulnerability in the web UI of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to inject arbitrary commands on an affected system and cause a denial of service (DoS) condition. This vulnerability is due to improper input validation of user-supplied input to the device template configuration. An attacker could exploit this vulnerability by submitting crafted input to the device template configuration. A successful exploit could allow the attacker to cause a DoS condition on the affected system.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.5	More Details
CVE-2024-51924	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alexandre Magno WP Agenda allows Stored XSS.This issue affects WP Agenda: from n/a through 2.0.	6.5	More Details
CVE-2024-51798	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Surbma Surbma	Font Awesome allows DOM-Based XSS.This issue affects Surbma	Font Awesome: from n/a through 3.0.	6.5	More Details
CVE-2024-51797	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Md. Shiddikur Rahman Ultimate Accordion allows DOM-Based XSS.This issue affects Ultimate Accordion: from n/a through 1.0.	6.5	More Details
CVE-2024-51795	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ByteLabX Pdf Embedder Fay allows DOM-Based XSS.This issue affects Pdf Embedder Fay: from n/a through 1.10.1.	6.5	More Details
CVE-2024-51909	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Monarkie Digital Content Solutions audioCase allows DOM-Based XSS.This issue affects audioCase: from n/a through 1.2.1.	6.5	More Details
CVE-2024-50553	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Classy Addons Classy Addons for Elementor allows DOM-Based XSS.This issue affects Classy Addons for Elementor: from n/a through 1.2.7.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20931	A vulnerability in the version control of Cisco TelePresence CE Software for Cisco Touch 10 Devices could allow an unauthenticated, adjacent attacker to install an older version of the software on an affected device. This vulnerability is due to insufficient version control. An attacker could exploit this vulnerability by installing an older version of Cisco TelePresence CE Software on an affected device. A successful exploit could allow the attacker to take advantage of vulnerabilities in older versions of the software.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.5	More Details
CVE-2024-51794	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NotFound Storely allows Stored XSS.This issue affects Storely: from n/a through 14.7.	6.5	More Details
CVE-2024-50554	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sided Sided allows DOM-Based XSS.This issue affects Sided: from n/a through 1.4.2.	6.5	More Details
CVE-2024-50556	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in MD. Mamunur Roshid WM Zoom allows DOM-Based XSS.This issue affects WM Zoom: from n/a through 1.0.	6.5	More Details
CVE-2024-51617	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Rami Yushuvaev Clyp allows Stored XSS.This issue affects Clyp: from n/a through 1.3.	6.5	More Details
CVE-2024-50651	java_shop 1.0 is vulnerable to Incorrect Access Control, which allows attackers to obtain sensitive information of users with different IDs by modifying the ID parameter.	6.5	More Details
CVE-2024-51925	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sazzad Hu Testimonial Slider Shortcode allows Stored XSS.This issue affects Testimonial Slider Shortcode: from n/a through 1.1.9.	6.5	More Details
CVE-2024-51813	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Anantaddons, Anantsites Anant Addons for Elementor allows DOM-Based XSS.This issue affects Anant Addons for Elementor: from n/a through 1.0.5.	6.5	More Details
CVE-2024-51814	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in 野人 活动链接推广插件 allows DOM-Based XSS.This issue affects 活动链接推广插件: from n/a through 1.2.0.	6.5	More Details
CVE-2024-51831	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aboutorab Pourhaghani Persian Nested Show/Hide Text allows Stored XSS.This issue affects Persian Nested Show/Hide Text: from n/a through 1.5.	6.5	More Details
CVE-2024-50551	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Alessandro Staniscia EndomondoWP allows Stored XSS.This issue affects EndomondoWP: from n/a through 0.1.1.	6.5	More Details
CVE-2024-50543	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Amazing Team amazing neo icon font for elementor allows DOM-Based XSS.This issue affects amazing neo icon font for elementor: from n/a through 2.0.1.	6.5	More Details
CVE-2024-50545	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Auburnforest DataMentor allows DOM-Based XSS.This issue affects DataMentor: from n/a through 1.7.	6.5	More Details
CVE-2024-50546	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Print Reach, Inc. MyOrderDesk allows DOM-Based XSS.This issue affects MyOrderDesk: from n/a through 3.2.6.	6.5	More Details
CVE-2024-51835	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Ajinkya N OpenCart Product Display allows Stored XSS.This issue affects OpenCart Product Display: from n/a through 1.0.	6.5	More Details
CVE-2024-50547	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themedy Themedy Toolbox allows DOM-Based XSS.This issue affects Themedy Toolbox: from n/a through 1.0.16.	6.5	More Details
CVE-2024-51834	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Luzuk Luzuk Slider allows Stored XSS.This issue affects Luzuk Slider: from n/a through 0.1.5.	6.5	More Details
CVE-2024-51833	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Noman Akhtar Easy Social Sharebar allows Stored XSS.This issue affects Easy Social Sharebar: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51832	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Plenigo Plenigo allows Stored XSS.This issue affects Plenigo: from n/a through 1.12.0.	6.5	More Details
CVE-2024-50548	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Abdullah Nahian Awesome Progress Bar allows DOM-Based XSS.This issue affects Awesome Progress Bar: from n/a through 1.0.1.	6.5	More Details
CVE-2024-50549	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Bonway Services Bonway Static Block Editor allows DOM-Based XSS.This issue affects Bonway Static Block Editor: from n/a through 1.1.0.	6.5	More Details
CVE-2024-51923	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Websand Websand Subscription Form allows Stored XSS.This issue affects Websand Subscription Form: from n/a through 1.0.3.	6.5	More Details
CVE-2024-51830	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Fazilatunnesa News Ticker allows Stored XSS.This issue affects News Ticker: from n/a through 1.0.	6.5	More Details
CVE-2024-51829	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Figoli Quinn & Associates Mobile Kiosk allows Stored XSS.This issue affects Mobile Kiosk: from n/a through 1.3.0.	6.5	More Details
CVE-2023-0737	wallabag version 2.5.2 contains a Cross-Site Request Forgery (CSRF) vulnerability that allows attackers to arbitrarily delete user accounts via the /account/delete endpoint. This issue is fixed in version 2.5.4.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51828	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Daniel J Griffiths Beacon For Help Scout allows DOM-Based XSS.This issue affects Beacon For Help Scout: from n/a through 1.3.0.	6.5	More Details
CVE-2024-51827	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Boombox Boombox Shortcode allows DOM-Based XSS.This issue affects Boombox Shortcode: from n/a through 1.0.0.	6.5	More Details
CVE-2024-51826	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in James Turner Bitcoin Payments allows DOM-Based XSS.This issue affects Bitcoin Payments: from n/a through 1.4.2.	6.5	More Details
CVE-2024-51825	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cristopher Ocaña Alert Me! allows DOM-Based XSS.This issue affects Alert Me!: from n/a through 0.4.0.	6.5	More Details
CVE-2024-51824	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in sony7596, mrseankumar25, miraclewebssoft Advanced Video Player with Analytics allows DOM-Based XSS.This issue affects Advanced Video Player with Analytics: from n/a through 1.	6.5	More Details
CVE-2024-51823	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Sherwin Calims Add Ribbon Shortcode allows DOM-Based XSS.This issue affects Add Ribbon Shortcode: from n/a through 1.0.1.	6.5	More Details
CVE-2024-51822	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Keon Themes Creative Blocks allows Stored XSS.This issue affects Creative Blocks: from n/a through 1.0.1.	6.5	More Details
CVE-2024-51821	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in wordpresteem WE – Client Logo Carousel allows Stored XSS.This issue affects WE – Client Logo Carousel: from n/a through 1.4.	6.5	More Details
CVE-2024-11238	A vulnerability, which was classified as critical, was found in Landray EKP up to 16.0. This affects the function delPreviewFile of the file /sys/ui/sys_ui_component/sysUiComponent.do?method=delPreviewFile. The manipulation of the argument directoryPath leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.5	More Details
CVE-2024-51819	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Tigris – Flexplatform Tigris Flexplatform allows Stored XSS.This issue affects Tigris Flexplatform: from n/a through .0.2.	6.5	More Details
CVE-2024-51816	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saul Morales Pacheco Banner System allows Stored XSS.This issue affects Banner System: from n/a through 1.0.0.	6.5	More Details
CVE-2024-50541	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Enea Overclokk Advanced Control Manager for WordPress by ItalyStrap allows Stored XSS.This issue affects Advanced Control Manager for WordPress by ItalyStrap: from n/a through 2.16.0.	6.5	More Details
CVE-2024-50540	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DemixPress (dp) AddThis allows Stored XSS.This issue affects (dp) AddThis: from n/a through 1.0.2.	6.5	More Details
CVE-2024-50542	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zach Silberstein RLM Elementor Widgets Pack allows DOM-Based XSS.This issue affects RLM Elementor Widgets Pack: from n/a through 1.3.1.	6.5	More Details
CVE-2024-9668	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown widget in all versions up to, and including, 1.7.1001 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9682	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Form Builder widget in all versions up to, and including, 1.7.1001 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2022-31669	Harbor fails to validate the user permissions when updating tag immutability policies. By sending a request to update a tag immutability policy with an id that belongs to a project that the currently authenticated user doesn't have access to, the attacker could modify tag immutability policies configured in other projects.	6.4	More Details
CVE-2024-9059	The Royal Elementor Addons and Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Google Maps widget in all versions up to, and including, 1.7.1001 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-2021-1483	A vulnerability in the web UI of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to gain read and write access to information that is stored on an affected system. This vulnerability is due to improper handling of XML External Entity (XXE) entries when the affected software parses certain XML files. An attacker could exploit this vulnerability by persuading a user to import a crafted XML file with malicious entries. A successful exploit could allow the attacker to read and write files within the affected application.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.4	More Details
CVE-2022-31667	Harbor fails to validate the user permissions when updating a robot account that belongs to a project that the authenticated user doesn't have access to. By sending a request that attempts to update a robot account, and specifying a robot account id and robot account name that belongs to a different project that the user doesn't have access to, it was possible to revoke the robot account permissions.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9426	The Aqua SVG Sprite plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 3.0.14 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2018-9371	In the Mediatek Preloader, there are out of bounds reads and writes due to an exposed interface that allows arbitrary peripheral memory mapping with insufficient blacklisting/whitelisting. This could lead to local elevation of privilege, given physical access to the device with no additional execution privileges needed. User interaction is needed for exploitation.	6.4	More Details
CVE-2021-1482	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization checking and gain access to sensitive information on an affected system. This vulnerability is due to insufficient authorization checks. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to bypass authorization checking and gain access to sensitive information on the affected system.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.4	More Details
CVE-2024-10268	The MP3 Audio Player – Music Player, Podcast Player & Radio by Sonaar plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's sonaar_audioplayer shortcode in all versions up to, and including, 5.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8961	The Essential Addons for Elementor – Best Elementor Addon, Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘nomore_items_text’ parameter in all versions up to, and including, 6.0.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8985	The Social Proof (Testimonial) Slider plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's spslider-block shortcode in all versions up to, and including, 2.2.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9850	The SVG Case Study plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-9386	The Exclusive Divi – Divi Preloader, Modules for Divi & Extra Theme plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-10147	The Steel plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's btn shortcode in all versions up to, and including, 1.3.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-10015	The ConvertCalculator for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' and 'type' parameters in all versions up to, and including, 1.1.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-11195	The Email Subscription Popup plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's print_email_subscribe_form shortcode in all versions up to, and including, 1.2.22 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-10592	The Mapster WP Maps plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the popup class parameter in all versions up to, and including, 1.6.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-10017	The PJW Mime Config plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-11198	The GD Rating System plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘extra_class’ parameter in all versions up to, and including, 3.6.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-11224	The Parallax Image plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘position’ parameter in all versions up to, and including, 1.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-11092	The SVGPlus plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REST API SVG File uploads in all versions up to, and including, 1.1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-10390	The Elfsight Telegram Chat CC plugin for WordPress is vulnerable to unauthorized modification of data to a missing capability check on the 'updatePreferences' function in all versions up to, and including, 1.1.0. 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-2024-10887	The NiceJob plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of the plugin's shortcodes (nicejob-lead, nicejob-review, nicejob-engage, nicejob-badge, nicejob-stories) in all versions up to, and including, 3.6.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-40885	Use after free in the UEFI firmware of some Intel(R) Server M20NTP BIOS may allow a privileged user to potentially enable escalation of privilege via local access.	6.4	More Details
CVE-2024-10113	The WP AdCenter – Ad Manager & Adsense Ads plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpadcenter_ad shortcode in all versions up to, and including, 2.5.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2020-3539	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to view, modify, and delete data without proper authorization. The vulnerability is due to a failure to limit access to resources that are intended for users with Administrator privileges. An attacker could exploit this vulnerability by convincing a user to click a malicious URL. A successful exploit could allow a low-privileged attacker to list, view, create, edit, and delete templates in the same manner as a user with Administrator privileges.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.3	More Details
CVE-2024-11250	A vulnerability was found in code-projects Inventory Management up to 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /model/editProduct.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-11251	A vulnerability was found in erzhongxmu Jeewms up to 20241108. It has been rated as critical. This issue affects some unknown processing of the file cgReportController.do of the component AuthInterceptor. The manipulation of the argument begin_date leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. This product does not use versioning. This is why information about affected and unaffected releases are unavailable. Other parameters might be affected as well.	6.3	More Details
CVE-2024-52392	Cross-Site Request Forgery (CSRF) vulnerability in W3speedster W3SPEEDSTER.This issue affects W3SPEEDSTER: from n/a through 7.25.	6.3	More Details
CVE-2024-39811	Improper input validation in firmware for some Intel(R) Server M20NTP Family UEFI may allow a privileged user to potentially enable escalation of privilege via local access.	6.3	More Details
CVE-2024-10262	The The Drop Shadow Boxes plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.7.14. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for authenticated attackers, with Subscriber-level access and above, to execute arbitrary shortcodes.	6.3	More Details
CVE-2024-11305	A vulnerability classified as critical was found in Altenergy Power Control Software up to 20241108. This vulnerability affects the function get_status_zigbee of the file /index.php/display/status_zigbee. The manipulation of the argument date leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-11212	A vulnerability, which was classified as critical, has been found in SourceCodester Best Employee Management System 1.0. Affected by this issue is some unknown functionality of the file /admin/fetch_product_details.php. The manipulation of the argument barcode leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2022-20871	A vulnerability in the web management interface of Cisco AsyncOS for Cisco Secure Web Appliance, formerly Cisco Web Security Appliance (WSA), could allow an authenticated, remote attacker to perform a command injection and elevate privileges to root. This vulnerability is due to insufficient validation of user-supplied input for the web interface. An attacker could exploit this vulnerability by authenticating to the system and sending a crafted HTTP packet to the affected device. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system and elevate privileges to root. To successfully exploit this vulnerability, an attacker would need at least read-only credentials.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.Attention: Simplifying the Cisco portfolio includes the renaming of security products under one brand: Cisco Secure. For more information, see .	6.3	More Details
CVE-2024-11244	A vulnerability classified as critical was found in code-projects Farmacia 1.0. This vulnerability affects unknown code of the file /editar-cliente.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-11245	A vulnerability, which was classified as critical, has been found in code-projects Farmacia 1.0. This issue affects some unknown processing of the file /editar-produto.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-11209	A vulnerability was found in Apereo CAS 6.6. It has been classified as critical. This affects an unknown part of the file /login?service of the component 2FA. The manipulation leads to improper authentication. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-52511	Nextcloud Tables allows users to to create tables with individual columns. By directly specifying the ID of a table or view, a malicious user could blindly insert new rows into tables they have no access to. It is recommended that the Nextcloud Tables is upgraded to 0.8.0.	6.3	More Details
CVE-2024-52555	In JetBrains WebStorm before 2024.3 code execution in Untrusted Project mode was possible via type definitions installer script	6.3	More Details
CVE-2024-11308	The DVC from TRCore encrypts files using a hardcoded key. Attackers can use this key to decrypt the files and restore the original content.	6.2	More Details
CVE-2021-1444	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web services interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive, browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.This advisory is part of the October 2021 release of the Cisco ASA, FTD, and FMC Security Advisory Bundled publication. For a complete list of the advisories and links to them, see .	6.1	More Details
CVE-2024-10850	The Razorpay Payment Button Elementor Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.2.5. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9830	The Bard theme for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.216. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2020-3431	A vulnerability in the web-based management interface of Cisco Small Business RV042 Dual WAN VPN Routers and Cisco Small Business RV042G Dual Gigabit WAN VPN Routers could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.1	More Details
CVE-2024-10851	The Razorpay Payment Button Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.4.6. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-11400	The HUSKY – Products Filter Professional for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the really_curr_tax parameter in all versions up to, and including, 1.3.6.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-10103	In the process of testing the MailPoet WordPress plugin before 5.3.2, a vulnerability was found that allows you to implement Stored XSS on behalf of the editor by embedding malicious script, which entails account takeover backdoor	6.1	More Details
CVE-2024-9777	The Ashe theme for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.243. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-10038	The WP-Strava plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.12.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	6.1	More Details
CVE-2024-10884	The SimpleForm Contact Form Submissions plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.1.0. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20654	A vulnerability in the web-based interface of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web-based interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based interface of Cisco Webex Meetings. An attacker could exploit this vulnerability by persuading a user of the interface to click a maliciously crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.1	More Details
CVE-2024-8874	The AJAX Login and Registration modal popup + inline form plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.24. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2022-20849	A vulnerability in the Broadband Network Gateway PPP over Ethernet (PPPoE) feature of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause the PPPoE process to continually crash. This vulnerability exists because the PPPoE feature does not properly handle an error condition within a specific crafted packet sequence. An attacker could exploit this vulnerability by sending a sequence of specific PPPoE packets from controlled customer premises equipment (CPE). A successful exploit could allow the attacker to cause the PPPoE process to continually restart, resulting in a denial of service condition (DoS).Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.This advisory is part of the September 2022 release of the Cisco IOS XR Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see .	6.1	More Details
CVE-2024-9356	The Yotpo: Product & Photo Reviews for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'yotpo_user_email' and 'yotpo_user_name' parameters in all versions up to, and including, 1.7.8 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2022-20632	A vulnerability in the web-based management interface of Cisco ECE could allow an unauthenticated, remote attacker to conduct an XSS attack against a user of the interface of an affected device. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.1	More Details
CVE-2024-11182	An XSS issue was discovered in MDaemon Email Server before version 24.5.1c. An attacker can send an HTML e-mail message with JavaScript in an img tag. This could allow a remote attacker to load arbitrary JavaScript code in the context of a webmail user's browser window.	6.1	More Details
CVE-2024-9938	The Bounce Handler MailPoet 3 plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'page' parameter in all versions up to, and including, 1.3.21 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2022-20631	A vulnerability in the web-based management interface of Cisco ECE could allow an unauthenticated, remote attacker to conduct an XSS attack against a user of the interface of an affected device. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious script code in a chat window. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or allow the attacker to access sensitive browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.1	More Details
CVE-2024-10825	The Hide My WP Ghost – Security & Firewall plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the URL in all versions up to, and including, 5.3.01 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick an administrative user into performing an action such as clicking on a link.	6.1	More Details
CVE-2021-3988	A Cross-site Scripting (XSS) vulnerability exists in janeczku/calibre-web, specifically in the file `edit_books.js`. The vulnerability occurs when editing book properties, such as uploading a cover or a format. The affected code directly inserts user input into the DOM without proper sanitization, allowing attackers to execute arbitrary JavaScript code. This can lead to various attacks, including stealing cookies. The issue is present in the code handling the `#btn-upload-cover` change event.	6.1	More Details
CVE-2024-8873	The PeproDev WooCommerce Receipt Uploader plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.6.9. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-37027	Improper Input validation in some Intel(R) VTune(TM) Profiler software before version 2024.2.0 may allow an authenticated user to potentially enable denial of service via local access.	6.1	More Details
CVE-2024-10577	The 胖鼠采集(Fat Rat Collect) 微信知乎简书腾讯新闻列表分页采集, 还有自动采集、自动发布、自动标签、等多项功能。开源插件 plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to missing escaping on a URL in all versions up to, and including, 2.7.3. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-1240	An open redirection vulnerability exists in pyload/pyload version 0.5.0. The vulnerability is due to improper handling of the 'next' parameter in the login functionality. An attacker can exploit this vulnerability to redirect users to malicious sites, which can be used for phishing or other malicious activities. The issue is fixed in pyload-ng 0.5.0b3.dev79.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9615	The BulkPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 0.3.5. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-48068	A cross-site scripting (XSS) vulnerability in Shenzhen Landray Software Co.,LTD Landray EKP v16 and earlier allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2024-50969	A Reflected cross-site scripting (XSS) vulnerability in browse.php of Code-projects Jonnys Liquor 1.0 allows remote attackers to inject arbitrary web scripts or HTML via the search parameter.	6.1	More Details
CVE-2024-9477	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AirTies Air4443 Firmware allows Cross-Site Scripting (XSS).This issue affects Air4443 Firmware: through 14102024. NOTE: The vendor was contacted and it was learned that the product classified as End-of-Life and End-of-Support.	6.1	More Details
CVE-2024-10877	The AFI – The Easiest Integration Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.92.0. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-52318	Incorrect object recycling and reuse vulnerability in Apache Tomcat. This issue affects Apache Tomcat: 11.0.0, 10.1.31, 9.0.96. Users are recommended to upgrade to version 11.0.1, 10.1.32 or 9.0.97, which fixes the issue.	6.1	More Details
CVE-2024-10684	The Kognetiks Chatbot for WordPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'dir' parameter in all versions up to, and including, 2.1.7 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-10882	The Product Delivery Date for WooCommerce – Lite plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.8.0. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-41785	IBM Concert Software 1.0.0 through 1.0.1 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.1	More Details
CVE-2024-10875	The Gallery Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of remove_Query_Arg without appropriate escaping on the URL in all versions up to, and including, 1.6.58. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9614	The Constant Contact Forms by MailMunch plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.1.2. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-8648	An issue has been discovered in GitLab CE/EE affecting all versions from 16 before 17.3.7, 17.4 before 17.4.4, and 17.5 before 17.5.2. The vulnerability could allow an attacker to inject malicious JavaScript code in Analytics Dashboards through a specially crafted URL.	6.1	More Details
CVE-2024-10883	The SimpleForm – Contact form made simple plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.2.0. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-36275	NULL pointer dereference in some Intel(R) Optane(TM) PMem Management software versions before CR_MGMT_02.00.00.4040, CR_MGMT_03.00.00.0499 may allow a authenticated user to potentially enable denial of service via local access.	6.1	More Details
CVE-2023-20060	A vulnerability in the web-based management interface of Cisco Prime Collaboration Deployment could allow an unauthenticated, remote attacker to conduct a cross-site scripting attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco plans to release software updates that address this vulnerability. There are no workarounds that address this vulnerability.	6.1	More Details
CVE-2024-9609	The LearnPress Export Import – WordPress extension for LearnPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'learnpress_import_form_server' parameter in all versions up to, and including, 4.0.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20663	A vulnerability in the web-based management interface of Cisco Secure Network Analytics, formerly Stealthwatch Enterprise, could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.Attention: Simplifying the Cisco portfolio includes the renaming of security products under one brand: Cisco Secure. For more information, see .	6.1	More Details
CVE-2022-20657	A vulnerability in the web-based management interface of Cisco PI and Cisco EPNM could allow an unauthenticated, remote attacker to conduct an XSS attack against a user of the interface of an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.	6.1	More Details
CVE-2024-39610	Cross-site scripting vulnerability exists in FitNesse releases prior to 20241026. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the user who is using the product.	6.1	More Details
CVE-2024-49505	A Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in openSUSE Tumbleweed MirrorCache allows the execution of arbitrary JS via reflected XSS in the REGEX and P parameters. This issue affects MirrorCache before 1.083.	6.1	More Details
CVE-2024-3447	A heap-based buffer overflow was found in the SDHCI device emulation of QEMU. The bug is triggered when both `s->data_count` and the size of `s->fifo_buffer` are set to 0x200, leading to an out-of-bound access. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition.	6.0	More Details
CVE-2022-20845	A vulnerability in the TL1 function of Cisco Network Convergence System (NCS) 4000 Series could allow an authenticated, local attacker to cause a memory leak in the TL1 process. This vulnerability is due to TL1 not freeing memory under some conditions. An attacker could exploit this vulnerability by connecting to the device and issuing TL1 commands after being authenticated. A successful exploit could allow the attacker to cause the TL1 process to consume large amounts of memory. When the memory reaches a threshold, the Resource Monitor (Resmon) process will begin to restart or shutdown the top five consumers of memory, resulting in a denial of service (DoS).Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.This advisory is part of the September 2022 release of the Cisco IOS XR Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see .	6.0	More Details
CVE-2024-21850	Sensitive information in resource not removed before reuse in some Intel(R) TDX Seamldr module software before version 1.5.02.00 may allow a privileged user to potentially enable escalation of privilege via local access.	6.0	More Details
CVE-2024-50515	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saturday Drive Ninja Forms allows Stored XSS.This issue affects Ninja Forms: from n/a through 3.8.16.	5.9	More Details
CVE-2024-31074	Observable timing discrepancy in some Intel(R) QAT Engine for OpenSSL software before version v1.6.1 may allow information disclosure via network access.	5.9	More Details
CVE-2024-43189	IBM Concert Software 1.0.0 through 1.0.1 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.	5.9	More Details
CVE-2024-50514	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Saturday Drive Ninja Forms allows Stored XSS.This issue affects Ninja Forms: from n/a through 3.8.16.	5.9	More Details
CVE-2024-50513	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Post Grid Team by WPXPO PostX allows Stored XSS.This issue affects PostX: from n/a through 4.1.15.	5.9	More Details
CVE-2023-1419	A script injection vulnerability was found in the Debezium database connector, where it does not properly sanitize some parameters. This flaw allows an attacker to send a malicious request to inject a parameter that may allow the viewing of unauthorized data.	5.9	More Details
CVE-2024-28885	Observable discrepancy in some Intel(R) QAT Engine for OpenSSL software before version v1.6.1 may allow information disclosure via network access.	5.9	More Details
CVE-2024-0787	phpIPAM version 1.5.1 contains a vulnerability where an attacker can bypass the IP block mechanism to brute force passwords for users by using the 'X-Forwarded-For' header. The issue lies in the 'get_user_ip()' function in 'class.Common.php' at lines 1044 and 1045, where the presence of the 'X-Forwarded-For' header is checked and used instead of 'REMOTE_ADDR'. This vulnerability allows attackers to perform brute force attacks on user accounts, including the admin account. The issue is fixed in version 1.7.0.	5.9	More Details
CVE-2024-33617	Insufficient control flow management in some Intel(R) QAT Engine for OpenSSL software before version v1.6.1 may allow information disclosure via network access.	5.9	More Details
CVE-2024-50516	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Adam Skaat Countdown & Clock allows Stored XSS.This issue affects Countdown & Clock: from n/a through 2.8.0.9.	5.9	More Details
CVE-2024-10104	The Jobs for WordPress plugin before 2.7.8 does not sanitise and escape some of its Job settings, which could allow high privilege users such as contributor to perform Stored Cross-Site Scripting attacks	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50430	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in The Beaver Builder Team Beaver Builder allows Stored XSS.This issue affects Beaver Builder: from n/a through 2.8.3.7.	5.9	More Details
CVE-2023-27609	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in NetTantra WP Roles at Registration allows Stored XSS.This issue affects WP Roles at Registration: from n/a through 0.23.	5.9	More Details
CVE-2023-39176	A flaw was found within the parsing of SMB2 requests that have a transform header in the kernel ksmbd module. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this to disclose sensitive information on affected installations of Linux. Only systems with ksmbd enabled are vulnerable to this CVE.	5.8	More Details
CVE-2021-1494	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of specific HTTP header parameters. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass a configured file policy for HTTP packets and deliver a malicious payload.	5.8	More Details
CVE-2021-34753	A vulnerability in the payload inspection for Ethernet Industrial Protocol (ENIP) traffic for Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to bypass configured rules for ENIP traffic. This vulnerability is due to incomplete processing during deep packet inspection for ENIP packets. An attacker could exploit this vulnerability by sending a crafted ENIP packet to the targeted interface. A successful exploit could allow the attacker to bypass configured access control and intrusion policies that should trigger and drop for the ENIP packet.	5.8	More Details
CVE-2024-28049	Improper input validation in firmware for some Intel(R) PROSet/Wireless Software and Intel(R) Killer(TM) Wi-Fi wireless products before version 23.40 may allow an unauthenticated user to enable denial of service via adjacent access.	5.7	More Details
CVE-2024-52520	Nextcloud Server is a self hosted personal cloud system. Due to a pre-flighted HEAD request, the link reference provider could be tricked into downloading bigger websites than intended, to find open-graph data. It is recommended that the Nextcloud Server is upgraded to 28.0.10 or 29.0.7 and Nextcloud Enterprise Server is upgraded to 27.1.11.8, 28.0.10 or 29.0.7.	5.7	More Details
CVE-2024-52515	Nextcloud Server is a self hosted personal cloud system. After an admin enables the default-disabled SVG preview provider, a malicious user could upload a manipulated SVG file referencing paths. If the file would exist the preview of the SVG would preview the other file instead. It is recommended that the Nextcloud Server is upgraded to 27.1.10, 28.0.6 or 29.0.1 and Nextcloud Enterprise Server is upgraded to 24.0.12.15, 25.0.13.10, 26.0.13.4, 27.1.10, 28.0.6 or 29.0.1.	5.7	More Details
CVE-2024-47820	MarkUs, a web application for the submission and grading of student assignments, is vulnerable to path traversal in versions prior to 2.4.8. Authenticated instructors may download any file on the web server MarkUs is running on, depending on the file permissions. MarkUs v2.4.8 has addressed this issue. No known workarounds are available at the application level aside from upgrading.	5.7	More Details
CVE-2024-52711	DI-8100 v16.07.26A1 is vulnerable to Buffer Overflow In the ip_position_asp function via the ip parameter.	5.7	More Details
CVE-2024-41970	A low privileged remote attacker may gain access to forbidden diagnostic data due to incorrect permission assignment for critical resources.	5.7	More Details
CVE-2024-45611	GLPI is an open-source asset and IT management software package that provides ITIL Service Desk features, licenses tracking and software auditing. An authenticated user can bypass the access control policy to create a private RSS feed attached to another user account and use a malicious payload to triggger a stored XSS. Upgrade to 10.0.17.	5.7	More Details
CVE-2024-8978	The Essential Addons for Elementor – Best Elementor Addon, Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 6.0.9 via the 'init_content_register_user_email_controls' function. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive data including usernames and passwords of any users who register via the Login I Register Form widget, as long as that user opens the email notification for successful registration.	5.7	More Details
CVE-2024-45670	IBM Security SOAR 51.0.1.0 and earlier contains a mechanism for users to recover or change their passwords without knowing the original password, but the user account must be compromised prior to the weak recovery mechanism.	5.6	More Details
CVE-2024-29076	Uncaught exception for some Intel(R) CST software before version 8.7.10803 may allow an authenticated user to potentially enable denial of service via local access.	5.5	More Details
CVE-2024-49536	Audition versions 23.6.9, 24.4.6 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-36284	Improper input validation in some Intel(R) Neural Compressor software before version v3.0 may allow an authenticated user to potentially enable escalation of privilege via adjacent access.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50303	In the Linux kernel, the following vulnerability has been resolved: resource,kexec: walk_system_ram_res_rev must retain resource flags walk_system_ram_res_rev() erroneously discards resource flags when passing the information to the callback. This causes systems with IORESOURCE_SYSRAM_DRIVER_MANAGED memory to have these resources selected during kexec to store kexec buffers if that memory happens to be at placed above normal system ram. This leads to undefined behavior after reboot. If the kexec buffer is never touched, nothing happens. If the kexec buffer is touched, it could lead to a crash (like below) or undefined behavior. Tested on a system with CXL memory expanders with driver managed memory, TPM enabled, and CONFIG_IMA_KEXEC=y. Adding printk's showed the flags were being discarded and as a result the check for IORESOURCE_SYSRAM_DRIVER_MANAGED passes. find_next_iomem_res: name(System RAM (kmem)) start(10000000000) end(1034fffffff) flags(83000200) locate_mem_hole_top_down: start(10000000000) end(1034fffffff) flags(0) [.] BUG: unable to handle page fault for address: ffff89834ffff000 [.] #PF: supervisor read access in kernel mode [.] #PF: error_code(0x0000) - not-present page [.] PGD c04c8bf067 P4D c04c8bf067 PUD c04c8be067 PMD 0 [.] Oops: 0000 [#1] SMP [.] RIP: 0010:ima_restore_measurement_list+0x95/0x4b0 [.] RSP: 0018:ffffc900000d3a80 EFLAGS: 00010286 [.] RAX: 0000000000001000 RBX: 0000000000000000 RCX: ffff89834ffff000 [.] RDX: 0000000000000018 RSI: ffff89834ffff000 RDI: ffff89834ffff018 [.] RBP: ffffc900000d3ba0 R08: 0000000000000020 R09: ffff888132b8a900 [.] R10: 4000000000000000 R11: 000000003a616d69 R12: 0000000000000000 [.] R13: ffffffff8404ac28 R14: 0000000000000000 R15: ffff89834ffff000 [.] FS: 0000000000000000(0000) GS:ffff893d44640000(0000) knlGS:0000000000000000 [.] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [.] ata5: SATA link down (SStatus 0 SControl 300) [.] CR2: ffff89834ffff000 CR3: 000001034d00f001 CR4: 0000000000770ef0 [.] PKRU: 55555554 [.] Call Trace: [.] <TASK> [.] ? __die+0x78/0xc0 [.] ? page_fault_oops+0x2a8/0x3a0 [.] ? exc_page_fault+0x84/0x130 [.] ? asm_exc_page_fault+0x22/0x30 [.] ? ima_restore_measurement_list+0x95/0x4b0 [.] ? template_desc_init_fields+0x317/0x410 [.] ? crypto_alloc_tfm_node+0x9c/0xc0 [.] ? init_ima_lsm+0x30/0x30 [.] ima_load_kexec_buffer+0x72/0xa0 [.] ima_init+0x44/0xa0 [.] __initstub__kmod_ima__373_1201_init_ima7+0x1e/0xb0 [.] ? init_ima_lsm+0x30/0x30 [.] do_one_initcall+0xad/0x200 [.] ? idr_alloc_cyclic+0xaa/0x110 [.] ? new_slab+0x12c/0x420 [.] ? new_slab+0x12c/0x420 [.] ? number+0x12a/0x430 [.] ? sysvec_apic_timer_interrupt+0xa/0x80 [.] ? asm_sysvec_apic_timer_interrupt+0x16/0x20 [.] ? parse_args+0xd4/0x380 [.] ? parse_args+0x14b/0x380 [.] kernel_init_freeable+0x1c1/0x2b0 [.] ? rest_init+0xb0/0xb0 [.] kernel_init+0x16/0x1a0 [.] ret_from_fork+0x2f/0x40 [.] ? rest_init+0xb0/0xb0 [.] ret_from_fork_asm+0x11/0x20 [.] </TASK>	5.5	More Details
CVE-2024-11098	The SVG Block plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REST API SVG File uploads in all versions up to, and including, 1.1.24 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Administrator-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	5.5	More Details
CVE-2024-50304	In the Linux kernel, the following vulnerability has been resolved: ipv4: ip_tunnel: Fix suspicious RCU usage warning in ip_tunnel_find() The per-netns IP tunnel hash table is protected by the RTNL mutex and ip_tunnel_find() is only called from the control path where the mutex is taken. Add a lockdep expression to hlist_for_each_entry_rcu() in ip_tunnel_find() in order to validate that the mutex is held and to silence the suspicious RCU usage warning [1]. [1] WARNING: suspicious RCU usage 6.12.0-rc3-custom-gd95d9a31aceb #139 Not tainted ----------------------------- net/ipv4/ip_tunnel.c:221 RCU-list traversed in non-reader section!! other info that might help us debug this: rcu_scheduler_active = 2, debug_locks = 1 1 lock held by ip/362: #0: ffffffff86fc7cb0 (rtnl_mutex){+.+.}-{3:3}, at: rtnetlink_rcv_msg+0x377/0xf60 stack backtrace: CPU: 12 UID: 0 PID: 362 Comm: ip Not tainted 6.12.0-rc3-custom-gd95d9a31aceb #139 Hardware name: Bochs Bochs, BIOS Bochs 01/01/2011 Call Trace: <TASK> dump_stack_lvl+0xba/0x110 lockdep_rcu_suspicious.cold+0x4f/0xd6 ip_tunnel_find+0x435/0x4d0 ip_tunnel_newlink+0x517/0x7a0 ipgre_newlink+0x14c/0x170 __rtnl_newlink+0x1173/0x19c0 rtnl_newlink+0x6c/0xa0 rtnetlink_rcv_msg+0x3cc/0xf60 netlink_rcv_skb+0x171/0x450 netlink_unicast+0x539/0x7f0 netlink_sendmsg+0x8c1/0xd80 ____sys_sendmsg+0x8f9/0xc20 ___sys_sendmsg+0x197/0x1e0 __sys_sendmsg+0x122/0x1f0 do_syscall_64+0xbb/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f	5.5	More Details
CVE-2024-53042	In the Linux kernel, the following vulnerability has been resolved: ipv4: ip_tunnel: Fix suspicious RCU usage warning in ip_tunnel_init_flow() There are code paths from which the function is called without holding the RCU read lock, resulting in a suspicious RCU usage warning [1]. Fix by using l3mdev_master_upper_ifindex_by_index() which will acquire the RCU read lock before calling l3mdev_master_upper_ifindex_by_index_rcu(). [1] WARNING: suspicious RCU usage 6.12.0-rc3-custom-gac8f72681cf2 #141 Not tainted ----------------------------- net/core/dev.c:876 RCU-list traversed in non-reader section!! other info that might help us debug this: rcu_scheduler_active = 2, debug_locks = 1 1 lock held by ip/361: #0: ffffffff86fc7cb0 (rtnl_mutex){+.+.}-{3:3}, at: rtnetlink_rcv_msg+0x377/0xf60 stack backtrace: CPU: 3 UID: 0 PID: 361 Comm: ip Not tainted 6.12.0-rc3-custom-gac8f72681cf2 #141 Hardware name: Bochs Bochs, BIOS Bochs 01/01/2011 Call Trace: <TASK> dump_stack_lvl+0xba/0x110 lockdep_rcu_suspicious.cold+0x4f/0xd6 dev_get_by_index_rcu+0x1d3/0x210 l3mdev_master_upper_ifindex_by_index_rcu+0x2b/0xf0 ip_tunnel_bind_dev+0x72f/0xa00 ip_tunnel_newlink+0x368/0x7a0 ipgre_newlink+0x14c/0x170 __rtnl_newlink+0x1173/0x19c0 rtnl_newlink+0x6c/0xa0 rtnetlink_rcv_msg+0x3cc/0xf60 netlink_rcv_skb+0x171/0x450 netlink_unicast+0x539/0x7f0 netlink_sendmsg+0x8c1/0xd80 ____sys_sendmsg+0x8f9/0xc20 ___sys_sendmsg+0x197/0x1e0 __sys_sendmsg+0x122/0x1f0 do_syscall_64+0xbb/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f	5.5	More Details
CVE-2023-4134	A use-after-free vulnerability was found in the cyttsp4_core driver in the Linux kernel. This issue occurs in the device cleanup routine due to a possible rearming of the watchdog_timer from the workqueue. This could allow a local user to crash the system, causing a denial of service.	5.5	More Details
CVE-2024-50273	In the Linux kernel, the following vulnerability has been resolved: btrfs: reinitialize delayed ref list after deleting it from the list At insert_delayed_ref() if we need to update the action of an existing ref to BTRFS_DROP_DELAYED_REF, we delete the ref from its ref head's ref_add_list using list_del(), which leaves the ref's add_list member not reinitialized, as list_del() sets the next and prev members of the list to LIST_POISON1 and LIST_POISON2, respectively. If later we end up calling drop_delayed_ref() against the ref, which can happen during merging or when destroying delayed refs due to a transaction abort, we can trigger a crash since at drop_delayed_ref() we call list_empty() against the ref's add_list, which returns false since the list was not reinitialized after the list_del() and as a consequence we call list_del() again at drop_delayed_ref(). This results in an invalid list access since the next and prev members are set to poison pointers, resulting in a splat if CONFIG_LIST_HARDENED and CONFIG_DEBUG_LIST are set or invalid poison pointer dereferences otherwise. So fix this by deleting from the list with list_del_init() instead.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50272	In the Linux kernel, the following vulnerability has been resolved: filemap: Fix bounds checking in filemap_read() If the caller supplies an iocb->ki_pos value that is close to the filesystem upper limit, and an iterator with a count that causes us to overflow that limit, then filemap_read() enters an infinite loop. This behaviour was discovered when testing xfstests generic/525 with the "localio" optimisation for loopback NFS mounts.	5.5	More Details
CVE-2017-13227	In the autofill service, the package name that is provided by the app process is trusted inappropriately. This could lead to information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2017-13309	In readEncryptedData of ConscryptEngine.java, there is a possible plaintext leak due to improperly used crypto. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-51765	A security vulnerability has been identified in HPE Cray Data Virtualization Service (DVS). Depending on configuration, this vulnerability may lead to local/cluster unauthorized access.	5.5	More Details
CVE-2024-50296	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix kernel crash when uninstalling driver When the driver is uninstalled and the VF is disabled concurrently, a kernel crash occurs. The reason is that the two actions call function pci_disable_sriov(). The num_VFs is checked to determine whether to release the corresponding resources. During the second calling, num_VFs is not 0 and the resource release function is called. However, the corresponding resource has been released during the first invoking. Therefore, the problem occurs: [15277.839633][T50670] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000020 ... [15278.131557][T50670] Call trace: [15278.134686][T50670] klist_put+0x28/0x12c [15278.138682][T50670] klist_del+0x14/0x20 [15278.142592][T50670] device_del+0xbc/0x3c0 [15278.146676][T50670] pci_remove_bus_device+0x84/0x120 [15278.151714][T50670] pci_stop_and_remove_bus_device+0x6c/0x80 [15278.157447][T50670] pci_iov_remove_virtfn+0xb4/0x12c [15278.162485][T50670] sriov_disable+0x50/0x11c [15278.166829][T50670] pci_disable_sriov+0x24/0x30 [15278.171433][T50670] hnae3_unregister_ae_algo_prepare+0x60/0x90 [hnae3] [15278.178039][T50670] hclge_exit+0x28/0xd0 [hclge] [15278.182730][T50670] __se_sys_delete_module.isra.0+0x164/0x230 [15278.188550][T50670] __arm64_sys_delete_module+0x1c/0x30 [15278.193848][T50670] invoke_syscall+0x50/0x11c [15278.198278][T50670] el0_svc_common.constprop.0+0x158/0x164 [15278.203837][T50670] do_el0_svc+0x34/0xcc [15278.207834][T50670] el0_svc+0x20/0x30 For details, see the following figure. rmmod hclge disable VFs ---------- hclge_exit() sriov_numvfs_store() ... device_lock() pci_disable_sriov() hns3_pci_sriov_configure() pci_disable_sriov() sriov_disable() sriov_disable() if !num_VFs : if !num_VFs : return; return; sriov_del_vfs() sriov_del_vfs() ... ... klist_put() klist_put() ... ... num_VFs = 0; num_VFs = 0; device_unlock(); In this patch, when driver is removing, we get the device_lock() to protect num_VFs, just like sriov_numvfs_store().	5.5	More Details
CVE-2024-51764	A security vulnerability has been identified in HPE Data Management Framework (DMF) Suite (CXFS). Depending on configuration, this vulnerability may lead to local/cluster unauthorized access.	5.5	More Details
CVE-2024-50281	In the Linux kernel, the following vulnerability has been resolved: KEYS: trusted: dcp: fix NULL dereference in AEAD crypto operation When sealing or unsealing a key blob we currently do not wait for the AEAD cipher operation to finish and simply return after submitting the request. If there is some load on the system we can exit before the cipher operation is done and the buffer we read from/write to is already removed from the stack. This will e.g. result in NULL pointer dereference errors in the DCP driver during blob creation. Fix this by waiting for the AEAD cipher operation to finish before resuming the seal and unseal calls.	5.5	More Details
CVE-2024-50302	In the Linux kernel, the following vulnerability has been resolved: HID: core: zero-initialize the report buffer Since the report buffer is used by all kinds of drivers in various ways, let's zero-initialize it during allocation to make sure that it can't be ever used to leak kernel memory via specially-crafted report.	5.5	More Details
CVE-2023-4679	A use after free vulnerability exists in GPAC version 2.3-DEV-revrelease, specifically in the gf_filterpacket_del function in filter_core/filter.c at line 38. This vulnerability can lead to a double-free condition, which may cause the application to crash.	5.5	More Details
CVE-2024-50284	In the Linux kernel, the following vulnerability has been resolved: ksmbd: Fix the missing xa_store error check xa_store() can fail, it return xa_err(-EINVAL) if the entry cannot be stored in an XArray, or xa_err(-ENOMEM) if memory allocation failed, so check error for xa_store() to fix it.	5.5	More Details
CVE-2024-50285	In the Linux kernel, the following vulnerability has been resolved: ksmbd: check outstanding simultaneous SMB operations If Client send simultaneous SMB operations to ksmbd, It exhausts too much memory through the "ksmbd_work_cache". It will cause OOM issue. ksmbd has a credit mechanism but it can't handle this problem. This patch add the check if it exceeds max credits to prevent this problem by assuming that one smb request consumes at least one credit.	5.5	More Details
CVE-2024-50270	In the Linux kernel, the following vulnerability has been resolved: mm/damon/core: avoid overflow in damon_feed_loop_next_input() damon_feed_loop_next_input() is inefficient and fragile to overflows. Specifically, 'score_goal_diff_bp' calculation can overflow when 'score' is high. The calculation is actually unnecessary at all because 'goal' is a constant of value 10,000. Calculation of 'compensation' is again fragile to overflow. Final calculation of return value for under-achiving case is again fragile to overflow when the current score is under-achieving the target. Add two corner cases handling at the beginning of the function to make the body easier to read, and rewrite the body of the function to avoid overflows and the unnecessary bp value calcuation.	5.5	More Details
CVE-2024-50287	In the Linux kernel, the following vulnerability has been resolved: media: v4l2-tpg: prevent the risk of a division by zero As reported by Coverity, the logic at tpg_precalculate_line() blindly rescales the buffer even when scaled_witdh is equal to zero. If this ever happens, this will cause a division by zero. Instead, add a WARN_ON_ONCE() to trigger such cases and return without doing any precalculation.	5.5	More Details
CVE-2024-50300	In the Linux kernel, the following vulnerability has been resolved: regulator: rtq2208: Fix uninitialized use of regulator_config Fix rtq2208 driver uninitialized use to cause kernel error.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50288	In the Linux kernel, the following vulnerability has been resolved: media: vivid: fix buffer overwrite when using > 32 buffers The maximum number of buffers that can be requested was increased to 64 for the video capture queue. But video capture used a must_blank array that was still sized for 32 (VIDEO_MAX_FRAME). This caused an out-of-bounds write when using buffer indices >= 32. Create a new define MAX_VID_CAP_BUFFERS that is used to access the must_blank array and set max_num_buffers for the video capture queue. This solves a crash reported by: https://bugzilla.kernel.org/show_bug.cgi?id=219258	5.5	More Details
CVE-2024-50299	In the Linux kernel, the following vulnerability has been resolved: sctp: properly validate chunk size in sctp_sf_ootb() A size validation fix similar to that in Commit 50619dbf8db7 ("sctp: add size validation when walking chunks") is also required in sctp_sf_ootb() to address a crash reported by syzbot: BUG: KMSAN: uninit-value in sctp_sf_ootb+0x7f5/0xce0 net/sctp/sm_statefuns.c:3712 sctp_sf_ootb+0x7f5/0xce0 net/sctp/sm_statefuns.c:3712 sctp_do_sm+0x181/0x93d0 net/sctp/sm_sideeffect.c:1166 sctp_endpoint_bh_rcv+0xc38/0xf90 net/sctp/endpointola.c:407 sctp_inq_push+0x2ef/0x380 net/sctp/inqueue.c:88 sctp_rcv+0x3831/0x3b20 net/sctp/input.c:243 sctp4_rcv+0x42/0x50 net/sctp/protocol.c:1159 ip_protocol_deliver_rcu+0xb51/0x13d0 net/ipv4/ip_input.c:205 ip_local_deliver_finish+0x336/0x500 net/ipv4/ip_input.c:233	5.5	More Details
CVE-2024-50298	In the Linux kernel, the following vulnerability has been resolved: net: enetc: allocate vf_state during PF probes In the previous implementation, vf_state is allocated memory only when VF is enabled. However, net_device_ops::ndo_set_vf_mac() may be called before VF is enabled to configure the MAC address of VF. If this is the case, enetc_pf_set_vf_mac() will access vf_state, resulting in access to a null pointer. The simplified error log is as follows. root@ls1028ardb:~# ip link set eno0 vf 1 mac 00:0c:e7:66:77:89 [173.543315] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000004 [173.637254] pc : enetc_pf_set_vf_mac+0x3c/0x80 Message from sy [173.641973] lr : do_setlink+0x4a8/0xec8 [173.732292] Call trace: [173.734740] enetc_pf_set_vf_mac+0x3c/0x80 [173.738847] __rtnl_newlink+0x530/0x89c [173.742692] rtnl_newlink+0x50/0x7c [173.746189] rtnetlink_rcv_msg+0x128/0x390 [173.750298] netlink_rcv_skb+0x60/0x130 [173.754145] rtnetlink_rcv+0x18/0x24 [173.757731] netlink_unicast+0x318/0x380 [173.761665] netlink_sendmsg+0x17c/0x3c8	5.5	More Details
CVE-2024-50291	In the Linux kernel, the following vulnerability has been resolved: media: dvb-core: add missing buffer index check dvb_vb2_expbuf() didn't check if the given buffer index was for a valid buffer. Add this check.	5.5	More Details
CVE-2024-29085	Improper access control for some BigDL software maintained by Intel(R) before version 2.5.0 may allow an authenticated user to potentially enable escalation of privilege via adjacent access.	5.5	More Details
CVE-2024-50271	In the Linux kernel, the following vulnerability has been resolved: signal: restore the override_rlimit logic Prior to commit d64696905554 ("Reimplement RLIMIT_SIGPENDING on top of ucounts") UCOUNT_RLIMIT_SIGPENDING rlimit was not enforced for a class of signals. However now it's enforced unconditionally, even if override_rlimit is set. This behavior change caused production issues. For example, if the limit is reached and a process receives a SIGSEGV signal, sigqueue_alloc fails to allocate the necessary resources for the signal delivery, preventing the signal from being delivered with siginfo. This prevents the process from correctly identifying the fault address and handling the error. From the user-space perspective, applications are unaware that the limit has been reached and that the siginfo is effectively 'corrupted'. This can lead to unpredictable behavior and crashes, as we observed with java applications. Fix this by passing override_rlimit into inc_rlimit_get_ucounts() and skip the comparison to max there if override_rlimit is set. This effectively restores the old behavior.	5.5	More Details
CVE-2024-53048	In the Linux kernel, the following vulnerability has been resolved: ice: fix crash on probe for DPLL enabled E810 LOM The E810 Lan On Motherboard (LOM) design is vendor specific. Intel provides the reference design, but it is up to vendor on the final product design. For some cases, like Linux DPLL support, the static values defined in the driver does not reflect the actual LOM design. Current implementation of dpll pins is causing the crash on probe of the ice driver for such DPLL enabled E810 LOM designs: WARNING: (...) at drivers/dpll/dpll_core.c:495 dpll_pin_get+0x2c4/0x330 ... Call Trace: <TASK> ? __warn+0x83/0x130 ? dpll_pin_get+0x2c4/0x330 ? report_bug+0x1b7/0x1d0 ? handle_bug+0x42/0x70 ? exc_invalid_op+0x18/0x70 ? asm_exc_invalid_op+0x1a/0x20 ? dpll_pin_get+0x117/0x330 ? dpll_pin_get+0x2c4/0x330 ? dpll_pin_get+0x117/0x330 ice_dpll_get_pins.isra.0+0x52/0xe0 [ice] ... The number of dpll pins enabled by LOM vendor is greater than expected and defined in the driver for Intel designed NICs, which causes the crash. Prevent the crash and allow generic pin initialization within Linux DPLL subsystem for DPLL enabled E810 LOM designs. Newly designed solution for described issue will be based on "per HW design" pin initialization. It requires pin information dynamically acquired from the firmware and is already in progress, planned for next-tree only.	5.5	More Details
CVE-2024-53043	In the Linux kernel, the following vulnerability has been resolved: mctp i2c: handle NULL header address daddr can be NULL if there is no neighbour table entry present, in that case the tx packet should be dropped. saddr will usually be set by MCTP core, but check for NULL in case a packet is transmitted by a different protocol.	5.5	More Details
CVE-2024-50266	In the Linux kernel, the following vulnerability has been resolved: clk: qcom: videocc-sm8350: use HW_CTRL_TRIGGER for vcodec GDSCs A recent change in the venus driver results in a stuck clock on the Lenovo ThinkPad X13s, for example, when streaming video in firefox: video_cc_mvs0_clk status stuck at 'off' WARNING: CPU: 6 PID: 2885 at drivers/clk/qcom/clk-branch.c:87 clk_branch_wait+0x144/0x15c ... Call trace: clk_branch_wait+0x144/0x15c clk_branch2_enable+0x30/0x40 clk_core_enable+0xd8/0x29c clk_enable+0x2c/0x4c vcodec_clks_enable.isra.0+0x94/0xd8 [venus_core] coreid_power_v4+0x464/0x628 [venus_core] vdec_start_streaming+0xc4/0x510 [venus_dec] vb2_start_streaming+0x6c/0x180 [videobuf2_common] vb2_core_streamon+0x120/0x1dc [videobuf2_common] vb2_streamon+0x1c/0x6c [videobuf2_v4l2] v4l2_m2m_ioctl_streamon+0x30/0x80 [v4l2_mem2mem] v4l_streamon+0x24/0x30 [videodev] using the out-of-tree sm8350/sc8280xp venus support. [1] Update also the sm8350/sc8280xp GDSC definitions so that the hw control mode can be changed at runtime as the venus driver now requires.	5.5	More Details
CVE-2024-53075	In the Linux kernel, the following vulnerability has been resolved: riscv: Prevent a bad reference count on CPU nodes When populating cache leaves we previously fetched the CPU device node at the very beginning. But when ACPI is enabled we go through a specific branch which returns early and does not call 'of_node_put' for the node that was acquired. Since we are not using a CPU device node for the ACPI code anyways, we can simply move the initialization of it just passed the ACPI block, and we are guaranteed to have an 'of_node_put' call for the acquired node. This prevents a bad reference count of the CPU device node. Moreover, the previous function did not check for errors when acquiring the device node, so a return -ENOENT has been added for that case.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-53076	In the Linux kernel, the following vulnerability has been resolved: iio: gts-helper: Fix memory leaks for the error path of iio_gts_build_avail_scale_table() If per_time_scales[i] or per_time_gains[i] kcalloc fails in the for loop of iio_gts_build_avail_scale_table(), the err_free_out will fail to call kfree() each time when i is reduced to 0, so all the per_time_scales[0] and per_time_gains[0] will not be freed, which will cause memory leaks. Fix it by checking if i >= 0.	5.5	More Details
CVE-2024-53077	In the Linux kernel, the following vulnerability has been resolved: rpcrdma: Always release the rpcrdma_device's xa_array Dai pointed out that the xa_init_flags() in rpcrdma_add_one() needs to have a matching xa_destroy() in rpcrdma_remove_one() to release underlying memory that the xarray might have accrued during operation.	5.5	More Details
CVE-2022-20626	A vulnerability in the web-based management interface of Cisco Prime Access Registrar Appliance could allow an authenticated, remote attacker to conduct a cross-site scripting attack against a user of the interface. The attacker would require valid credentials for the device. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	5.5	More Details
CVE-2024-53078	In the Linux kernel, the following vulnerability has been resolved: drm/tegra: Fix NULL vs IS_ERR() check in probe() The iommu_paging_domain_alloc() function doesn't return NULL pointers, it returns error pointers. Update the check to match.	5.5	More Details
CVE-2024-53079	In the Linux kernel, the following vulnerability has been resolved: mm/thp: fix deferred split unqueue naming and locking Recent changes are putting more pressure on THP deferred split queues: under load revealing long-standing races, causing list_del corruptions, "Bad page state"s and worse (I keep BUGs in both of those, so usually don't get to see how badly they end up without). The relevant recent changes being 6.8's mTHP, 6.10's mTHP swapout, and 6.12's mTHP swapin, improved swap allocation, and underused THP splitting. Before fixing locking: rename misleading folio_undo_large_rmappable(), which does not undo large_rmappable, to folio_unqueue_deferred_split(), which is what it does. But that and its out-of-line __callee are mm internals of very limited usability: add comment and WARN_ON_ONCEs to check usage; and return a bool to say if a deferred split was unqueued, which can then be used in WARN_ON_ONCEs around safety checks (sparing callers the arcane conditionals in __folio_unqueue_deferred_split()). Just omit the folio_unqueue_deferred_split() from free_unref_folios(), all of whose callers now call it beforehand (and if any forget then bad_page() will tell) - except for its caller put_pages_list(), which itself no longer has any callers (and will be deleted separately). Swapout: mem_cgroup_swapout() has been resetting folio->memcg_data 0 without checking and unqueueing a THP folio from deferred split list; which is unfortunate, since the split_queue_lock depends on the memcg (when memcg is enabled); so swapout has been unqueueing such THPs later, when freeing the folio, using the pgdat's lock instead: potentially corrupting the memcg's list. __remove_mapping() has frozen refcount to 0 here, so no problem with calling folio_unqueue_deferred_split() before resetting memcg_data. That goes back to 5.4 commit 87eaceb3faa5 ("mm: thp: make deferred split shrinker memcg aware"): which included a check on swapcache before adding to deferred queue, but no check on deferred queue before adding THP to swapcache. That worked fine with the usual sequence of events in reclaim (though there were a couple of rare ways in which a THP on deferred queue could have been swapped out), but 6.12 commit dafff3f4c850 ("mm: split underused THPs") avoids splitting underused THPs in reclaim, which makes swapcache THPs on deferred queue commonplace. Keep the check on swapcache before adding to deferred queue? Yes: it is no longer essential, but preserves the existing behaviour, and is likely to be a worthwhile optimization (vmstat showed much more traffic on the queue under swapping load if the check was removed); update its comment. Memcg-v1 move (deprecated): mem_cgroup_move_account() has been changing folio->memcg_data without checking and unqueueing a THP folio from the deferred list, sometimes corrupting "from" memcg's list, like swapout. Refcount is non-zero here, so folio_unqueue_deferred_split() can only be used in a WARN_ON_ONCE to validate the fix, which must be done earlier: mem_cgroup_move_charge_pte_range() first try to split the THP (splitting of course unqueues), or skip it if that fails. Not ideal, but moving charge has been requested, and khugepaged should repair the THP later: nobody wants new custom unqueueing code just for this deprecated case. The 87eaceb3faa5 commit did have the code to move from one deferred list to another (but was not conscious of its unsafety while refcount non-0); but that was removed by 5.6 commit fac0516b5534 ("mm: thp: don't need care deferred split queue in memcg charge move path"), which argued that the existence of a PMD mapping guarantees that the THP cannot be on a deferred list. As above, false in rare cases, and now commonly false. Backport to 6.11 should be straightforward. Earlier backports must take care that other _deferred_list fixes and dependencies are included. There is not a strong case for backports, but they can fix cornercases.	5.5	More Details
CVE-2024-53080	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Lock XArray when getting entries for the VM Similar to commit cac075706f29 ("drm/panthor: Fix race when converting group handle to group object") we need to use the XArray's internal locking when retrieving a vm pointer from there. v2: Removed part of the patch that was trying to protect fetching the heap pointer from XArray, as that operation is protected by the @pool->lock.	5.5	More Details
CVE-2024-53081	In the Linux kernel, the following vulnerability has been resolved: media: ar0521: don't overflow when checking PLL values The PLL checks are comparing 64 bit integers with 32 bit ones, as reported by Coverity. Depending on the values of the variables, this may underflow. Fix it ensuring that both sides of the expression are u64.	5.5	More Details
CVE-2024-53083	In the Linux kernel, the following vulnerability has been resolved: usb: typec: qcom-pmic: init value of hdr_len/txbuf_len earlier If the read of USB_PDPHY_RX_ACKNOWLEDGE_REG failed, then hdr_len and txbuf_len are uninitialized. This commit stops to print uninitialized value and misleading/false data.	5.5	More Details
CVE-2024-53084	In the Linux kernel, the following vulnerability has been resolved: drm/imagination: Break an object reference loop When remaining resources are being cleaned up on driver close, outstanding VM mappings may result in resources being leaked, due to an object reference loop, as shown below, with each object (or set of objects) referencing the object below it: PVR GEM Object GPU scheduler "finished" fence GPU scheduler “scheduled” fence PVR driver “done” fence PVR Context PVR VM Context PVR VM Mappings PVR GEM Object The reference that the PVR VM Context has on the VM mappings is a soft one, in the sense that the freeing of outstanding VM mappings is done as part of VM context destruction; no reference counts are involved, as is the case for all the other references in the loop. To break the reference loop during cleanup, free the outstanding VM mappings before destroying the PVR Context associated with the VM context.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-53085	In the Linux kernel, the following vulnerability has been resolved: tpm: Lock TPM chip in tpm_pm_suspend() first Setting TPM_CHIP_FLAG_SUSPENDED in the end of tpm_pm_suspend() can be racy according, as this leaves window for tpm_hwrng_read() to be called while the operation is in progress. The recent bug report gives also evidence of this behaviour. Aadress this by locking the TPM chip before checking any chip->flags both in tpm_pm_suspend() and tpm_hwrng_read(). Move TPM_CHIP_FLAG_SUSPENDED check inside tpm_get_random() so that it will be always checked only when the lock is reserved.	5.5	More Details
CVE-2024-53086	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Drop VM dma-resv lock on xe_sync_in_fence_get failure in exec IOCTL Upon failure all locks need to be dropped before returning to the user. (cherry picked from commit 7d1a4258e602ffdce529f56686925034c1b3b095)	5.5	More Details
CVE-2024-53087	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix possible exec queue leak in exec IOCTL In a couple of places after an exec queue is looked up the exec IOCTL returns on input errors without dropping the exec queue ref. Fix this ensuring the exec queue ref is dropped on input error. (cherry picked from commit 07064a200b40ac2195cb6b7b779897d9377e5e6f)	5.5	More Details
CVE-2018-9340	In ResStringPool::setTo of ResourceTypes.cpp, it's possible for an attacker to control the value of mStringPoolSize to be out of bounds, causing information disclosure.	5.5	More Details
CVE-2024-43086	In validateAccountsInternal of AccountManagerService.java, there is a possible way to leak account credentials to a third party app due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-43084	In visitUris of multiple files, there is a possible information disclosure due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2018-9345	In BnAudioPolicyService::onTransact of AudioPolicyService.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2018-9346	In BnAudioPolicyService::onTransact of AudioPolicyService.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-43083	In validate of WifiConfigurationUtil.java , there is a possible persistent denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2024-43082	In onActivityResult of EditUserPhotoController.java, there is a possible cross-user media read due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2018-9410	In analyzeAxes of FontUtils.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2018-9412	In removeUnsynchronization of ID3.cpp there is a possible resource exhaustion due to improper input validation. This could lead to denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	5.5	More Details
CVE-2018-9420	In BnCameraService::onTransact of CameraService.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2018-9421	In writeInplace of Parcel.cpp, there is a possible information leak across processes, using Binder, due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-20039	A vulnerability in Cisco IND could allow an authenticated, local attacker to read application data. This vulnerability is due to insufficient default file permissions that are applied to the application data directory. An attacker could exploit this vulnerability by accessing files in the application data directory. A successful exploit could allow the attacker to view sensitive information. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	5.5	More Details
CVE-2024-53074	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: don't leak a link on AP removal Release the link mapping resource in AP removal. This impacted devices that do not support the MLD API (9260 and down). On those devices, we couldn't start the AP again after the AP has been already started and stopped.	5.5	More Details
CVE-2024-53073	In the Linux kernel, the following vulnerability has been resolved: NFSD: Never decrement pending_async_copies on error The error flow in nfsd4_copy() calls cleanup_async_copy(), which already decrements nn->pending_async_copies.	5.5	More Details
CVE-2024-48294	A NULL pointer dereference in the component libPdfCore.dll of Wondershare PDF Reader v1.0.9.2544 allows attackers to cause a Denial of Service (DoS) via a crafted PDF file.	5.5	More Details
CVE-2024-53072	In the Linux kernel, the following vulnerability has been resolved: platform/x86/amd/pmc: Detect when STB is not available Loading the amd_pmc module as: amd_pmc enable_stb=1 ...can result in the following messages in the kernel ring buffer: amd_pmc AMDI0009:00: SMU cmd failed. err: 0xff ioremap on RAM at 0x0000000000000000 - 0x00000000000fffff WARNING: CPU: 10 PID: 2151 at arch/x86/mm/ioremap.c:217 __ioremap_caller+0x2cd/0x340 Further debugging reveals that this occurs when the requests for S2D_PHYS_ADDR_LOW and S2D_PHYS_ADDR_HIGH return a value of 0, indicating that the STB is inaccessible. To prevent the ioremap warning and provide clarity to the user, handle the invalid address and display an error message.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50265	In the Linux kernel, the following vulnerability has been resolved: ocfs2: remove entry once instead of null-ptr-dereference in ocfs2_xa_remove() Syzkaller is able to provoke null-ptr-dereference in ocfs2_xa_remove(): [57.319872] (a.out,1161,7):ocfs2_xa_remove:2028 ERROR: status = -12 [57.320420] (a.out,1161,7):ocfs2_xa_cleanup_value_truncate:1999 ERROR: Partial truncate while removing xattr overlay.upper. Leaking 1 clusters and removing the entry [57.321727] BUG: kernel NULL pointer dereference, address: 0000000000000004 [...] [57.325727] RIP: 0010:ocfs2_xa_block_wipe_namevalue+0x2a/0xc0 [...] [57.331328] Call Trace: [57.331477] <TASK> [...] [57.333511] ? do_user_addr_fault+0x3e5/0x740 [57.333778] ? exc_page_fault+0x70/0x170 [57.334016] ? asm_exc_page_fault+0x2b/0x30 [57.334263] ? __pfx_ocfs2_xa_block_wipe_namevalue+0x10/0x10 [57.334596] ? ocfs2_xa_block_wipe_namevalue+0x2a/0xc0 [57.334913] ocfs2_xa_remove_entry+0x23/0xc0 [57.335164] ocfs2_xa_set+0x704/0xcf0 [57.335381] ? _raw_spin_unlock+0x1a/0x40 [57.335620] ? ocfs2_inode_cache_unlock+0x16/0x20 [57.335915] ? trace_preempt_on+0x1e/0x70 [57.336153] ? start_this_handle+0x16c/0x500 [57.336410] ? preempt_count_sub+0x50/0x80 [57.336656] ? _raw_read_unlock+0x20/0x40 [57.336906] ? start_this_handle+0x16c/0x500 [57.337162] ocfs2_xattr_block_set+0xa6/0x1e0 [57.337424] __ocfs2_xattr_set_handle+0x1fd/0x5d0 [57.337706] ? ocfs2_start_trans+0x13d/0x290 [57.337971] ocfs2_xattr_set+0xb13/0xfb0 [57.338207] ? dput+0x46/0x1c0 [57.338393] ocfs2_xattr_trusted_set+0x28/0x30 [57.338665] ? ocfs2_xattr_trusted_set+0x28/0x30 [57.338948] __vfs_removexattr+0x92/0xc0 [57.339182] __vfs_removexattr_locked+0xd5/0x190 [57.339456] ? preempt_count_sub+0x50/0x80 [57.339705] vfs_removexattr+0x5f/0x100 [...] Reproducer uses faultinject facility to fail ocfs2_xa_remove() -> ocfs2_xa_value_truncate() with -ENOMEM. In this case the comment mentions that we can return 0 if ocfs2_xa_cleanup_value_truncate() is going to wipe the entry anyway. But the following 'rc' check is wrong and execution flow do 'ocfs2_xa_remove_entry(loc);' twice: * 1st: in ocfs2_xa_cleanup_value_truncate(); * 2nd: returning back to ocfs2_xa_remove() instead of going to 'out'. Fix this by skipping the 2nd removal of the same entry and making syzkaller repro happy.	5.5	More Details
CVE-2024-53044	In the Linux kernel, the following vulnerability has been resolved: net/sched: sch_api: fix xa_insert() error path in tcf_block_get_ext() This command: $ tc qdisc replace dev eth0 ingress_block 1 egress_block 1 clsact Error: block dev insert failed: -EBUSY. fails because user space requests the same block index to be set for both ingress and egress. [side note, I don't think it even failed prior to commit 913b47d3424e ("net/sched: Introduce tc block netdev tracking infra"), because this is a command from an old set of notes of mine which used to work, but alas, I did not scientifically bisect this] The problem is not that it fails, but rather, that the second time around, it fails differently (and irrecoverably): $ tc qdisc replace dev eth0 ingress_block 1 egress_block 1 clsact Error: dsa_core: Flow block cb is busy. [another note: the extack is added by me for illustration purposes. the context of the problem is that clsact_init() obtains the same &q->ingress_block pointer as &q->egress_block, and since we call tcf_block_get_ext() on both of them, "dev" will be added to the block->ports xarray twice, thus failing the operation: once through the ingress block pointer, and once again through the egress block pointer. the problem itself is that when xa_insert() fails, we have emitted a FLOW_BLOCK_BIND command through ndo_setup_tc(), but the offload never sees a corresponding FLOW_BLOCK_UNBIND.] Even correcting the bad user input, we still cannot recover: $ tc qdisc replace dev swp3 ingress_block 1 egress_block 2 clsact Error: dsa_core: Flow block cb is busy. Basically the only way to recover is to reboot the system, or unbind and rebind the net device driver. To fix the bug, we need to fill the correct error teardown path which was missed during code movement, and call tcf_block_offload_unbind() when xa_insert() fails. [last note, fundamentally I blame the label naming convention in tcf_block_get_ext() for the bug. The labels should be named after what they do, not after the error path that jumps to them. This way, it is obviously wrong that two labels pointing to the same code mean something is wrong, and checking the code correctness at the goto site is also easier]	5.5	More Details
CVE-2024-53045	In the Linux kernel, the following vulnerability has been resolved: ASoC: dapm: fix bounds checker error in dapm_widget_list_create The widgets array in the snd_soc_dapm_widget_list has a __counted_by attribute attached to it, which points to the num_widgets variable. This attribute is used in bounds checking, and if it is not set before the array is filled, then the bounds sanitizer will issue a warning or a kernel panic if CONFIG_UBSAN_TRAP is set. This patch sets the size of the widgets list calculated with list_for_each as the initial value for num_widgets as it is used for allocating memory for the array. It is updated with the actual number of added elements after the array is filled.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-53046	In the Linux kernel, the following vulnerability has been resolved: arm64: dts: imx8ulp: correct the flexspi compatible string The flexspi on imx8ulp only has 16 LUTs, and imx8mm flexspi has 32 LUTs, so correct the compatible string here, otherwise will meet below error: [1.119072] ------------[cut here]------------ [1.123926] WARNING: CPU: 0 PID: 1 at drivers/spi/spi-nxp-fspi.c:855 nxp_fspi_exec_op+0xb04/0xb64 [1.133239] Modules linked in: [1.136448] CPU: 0 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.11.0-rc6-next-20240902-00001-g131bf9439dd9 #69 [1.146821] Hardware name: NXP i.MX8ULP EVK (DT) [1.151647] pstate: 40000005 (nZcv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [1.158931] pc : nxp_fspi_exec_op+0xb04/0xb64 [1.163496] lr : nxp_fspi_exec_op+0xa34/0xb64 [1.168060] sp : ffff80008002b2a0 [1.171526] x29: ffff80008002b2d0 x28: 0000000000000000 x27: 0000000000000000 [1.179002] x26: ffff2eb645542580 x25: ffff800080610014 x24: ffff800080610000 [1.186480] x23: ffff2eb645548080 x22: 0000000000000006 x21: ffff2eb6455425e0 [1.193956] x20: 0000000000000000 x19: ffff80008002b5e0 x18: ffffffffffffffff [1.201432] x17: ffff2eb644467508 x16: 0000000000000138 x15: 0000000000000002 [1.208907] x14: 0000000000000000 x13: ffff2eb6400d8080 x12: 00000000ffffff00 [1.216378] x11: 0000000000000000 x10: ffff2eb6400d8080 x9 : ffff2eb697adca80 [1.223850] x8 : ffff2eb697ad3cc0 x7 : 0000000100000000 x6 : 0000000000000001 [1.231324] x5 : 0000000000000000 x4 : 0000000000000000 x3 : 00000000000007a6 [1.238795] x2 : 0000000000000000 x1 : 00000000000001ce x0 : 00000000ffffff92 [1.246267] Call trace: [1.248824] nxp_fspi_exec_op+0xb04/0xb64 [1.253031] spi_mem_exec_op+0x3a0/0x430 [1.257139] spi_nor_read_id+0x80/0xcc [1.261065] spi_nor_scan+0x1ec/0xf10 [1.264901] spi_nor_probe+0x108/0x2fc [1.268828] spi_mem_probe+0x6c/0xbc [1.272574] spi_probe+0x84/0xe4 [1.275958] really_probe+0xbc/0x29c [1.279713] __driver_probe_device+0x78/0x12c [1.284277] driver_probe_device+0xd8/0x15c [1.288660] __device_attach_driver+0xb8/0x134 [1.293316] bus_for_each_drv+0x88/0xe8 [1.297337] __device_attach+0xa0/0x190 [1.301353] device_initial_probe+0x14/0x20 [1.305734] bus_probe_device+0xac/0xb0 [1.309752] device_add+0x5d0/0x790 [1.313408] __spi_add_device+0x134/0x204 [1.317606] of_register_spi_device+0x3b4/0x590 [1.322348] spi_register_controller+0x47c/0x754 [1.327181] devm_spi_register_controller+0x4c/0xa4 [1.332289] nxp_fspi_probe+0x1cc/0x2b0 [1.336307] platform_probe+0x68/0xc4 [1.340145] really_probe+0xbc/0x29c [1.343893] __driver_probe_device+0x78/0x12c [1.348457] driver_probe_device+0xd8/0x15c [1.352838] __driver_attach+0x90/0x19c [1.356857] bus_for_each_dev+0x7c/0xdc [1.360877] driver_attach+0x24/0x30 [1.364624] bus_add_driver+0xe4/0x208 [1.368552] driver_register+0x5c/0x124 [1.372573] __platform_driver_register+0x28/0x34 [1.377497] nxp_fspi_driver_init+0x1c/0x28 [1.381888] do_one_initcall+0x80/0x1c8 [1.385908] kernel_init_freeable+0x1c4/0x28c [1.390472] kernel_init+0x20/0x1d8 [1.394138] ret_from_fork+0x10/0x20 [1.397885] ---[end trace 0000000000000000]--- [1.407908] ------------[cut here]------------	5.5	More Details
CVE-2024-53047	In the Linux kernel, the following vulnerability has been resolved: mptcp: init: protect sched with rcu_read_lock Enabling CONFIG_PROVE_RCU_LIST with its dependence CONFIG_RCU_EXPERT creates this splat when an MPTCP socket is created: ============================= WARNING: suspicious RCU usage 6.12.0-rc2+ #11 Not tainted ----------------------------- net/mptcp/sched.c:44 RCU-list traversed in non-reader section!! other info that might help us debug this: rcu_scheduler_active = 2, debug_locks = 1 no locks held by mptcp_connect/176. stack backtrace: CPU: 0 UID: 0 PID: 176 Comm: mptcp_connect Not tainted 6.12.0-rc2+ #11 Hardware name: Bochs Bochs, BIOS Bochs 01/01/2011 Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:123) lockdep_rcu_suspicious (kernel/locking/lockdep.c:6822) mptcp_sched_find (net/mptcp/sched.c:44 (discriminator 7)) mptcp_init_sock (net/mptcp/protocol.c:2867 (discriminator 1)) ? sock_init_data_uid (arch/x86/include/asm/atomic.h:28) inet_create.part.0.constprop.0 (net/ipv4/af_inet.c:386) ? __sock_create (include/linux/rcupdate.h:347 (discriminator 1)) __sock_create (net/socket.c:1576) __sys_socket (net/socket.c:1671) ? __pfx___sys_socket (net/socket.c:1712) ? do_user_addr_fault (arch/x86/mm/fault.c:1419 (discriminator 1)) __x64_sys_socket (net/socket.c:1728) do_syscall_64 (arch/x86/entry/common.c:52 (discriminator 1)) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) That's because when the socket is initialised, rcu_read_lock() is not used despite the explicit comment written above the declaration of mptcp_sched_find() in sched.c. Adding the missing lock/unlock avoids the warning.	5.5	More Details
CVE-2024-52613	A heap-based buffer under-read in tsMuxer version nightly-2024-05-12-02-01-18 allows attackers to cause Denial of Service (DoS) via a crafted MOV video file.	5.5	More Details
CVE-2024-53049	In the Linux kernel, the following vulnerability has been resolved: slub/kunit: fix a WARNING due to unwrapped __kmalloc_cache_noprof 'modprobe slub_kunit' will have a warning as shown below. The root cause is that __kmalloc_cache_noprof was directly used, which resulted in no alloc_tag being allocated. This caused current->alloc_tag to be null, leading to a warning in alloc_tag_add_check. Let's add an alloc_hook layer to __kmalloc_cache_noprof specifically within lib/slub_kunit.c, which is the only user of this internal slub function outside kmalloc implementation itself. [58162.947016] WARNING: CPU: 2 PID: 6210 at ./include/linux/alloc_tag.h:125 alloc_tagging_slab_alloc_hook+0x268/0x27c [58162.957721] Call trace: [58162.957919] alloc_tagging_slab_alloc_hook+0x268/0x27c [58162.958286] __kmalloc_cache_noprof+0x14c/0x344 [58162.958615] test_kmalloc_redzone_access+0x50/0x10c [slub_kunit] [58162.959045] kunit_try_run_case+0x74/0x184 [kunit] [58162.959401] kunit_generic_run_threadfn_adapter+0x2c/0x4c [kunit] [58162.959841] kthread+0x10c/0x118 [58162.960093] ret_from_fork+0x10/0x20 [58162.960363] ---[end trace 0000000000000000]---	5.5	More Details
CVE-2024-53050	In the Linux kernel, the following vulnerability has been resolved: drm/i915/hdcp: Add encoder check in hdcp2_get_capability Add encoder check in intel_hdcp2_get_capability to avoid null pointer error.	5.5	More Details
CVE-2024-53051	In the Linux kernel, the following vulnerability has been resolved: drm/i915/hdcp: Add encoder check in intel_hdcp_get_capability Sometimes during hotplug scenario or suspend/resume scenario encoder is not always initialized when intel_hdcp_get_capability add a check to avoid kernel null pointer dereference.	5.5	More Details
CVE-2024-53053	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Fix another deadlock during RTC update If ufshcd_rtc_work calls ufshcd_rpm_put_sync() and the pm's usage_count is 0, we will enter the runtime suspend callback. However, the runtime suspend callback will wait to flush ufshcd_rtc_work, causing a deadlock. Replace ufshcd_rpm_put_sync() with ufshcd_rpm_put() to avoid the deadlock.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-53055	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: fix 6 GHz scan construction If more than 255 colocated APs exist for the set of all APs found during 2.4/5 GHz scanning, then the 6 GHz scan construction will loop forever since the loop variable has type u8, which can never reach the number found when that's bigger than 255, and is stored in a u32 variable. Also move it into the loops to have a smaller scope. Using a u32 there is fine, we limit the number of APs in the scan list and each has a limit on the number of RNR entries due to the frame size. With a limit of 1000 scan results, a frame size upper bound of 4096 (really it's more like ~2300) and a TBTT entry size of at least 11, we get an upper bound for the number of ~372k, well in the bounds of a u32.	5.5	More Details
CVE-2024-53056	In the Linux kernel, the following vulnerability has been resolved: drm/mediatek: Fix potential NULL dereference in mtk_crtc_destroy() In mtk_crtc_create(), if the call to mbox_request_channel() fails then we set the "mtk_crtc->cmdq_client.chan" pointer to NULL. In that situation, we do not call cmdq_pkt_create(). During the cleanup, we need to check if the "mtk_crtc->cmdq_client.chan" is NULL first before calling cmdq_pkt_destroy(). Calling cmdq_pkt_destroy() is unnecessary if we didn't call cmdq_pkt_create() and it will result in a NULL pointer dereference.	5.5	More Details
CVE-2023-6110	A flaw was found in OpenStack. When a user tries to delete a non-existing access rule in it's scope, it deletes other existing access rules which are not associated with any application credentials.	5.5	More Details
CVE-2024-53058	In the Linux kernel, the following vulnerability has been resolved: net: stmmac: TSO: Fix unbalanced DMA map/unmap for non-paged SKB data In case the non-paged data of a SKB carries protocol header and protocol payload to be transmitted on a certain platform that the DMA AXI address width is configured to 40-bit/48-bit, or the size of the non-paged data is bigger than TSO_MAX_BUFF_SIZE on a certain platform that the DMA AXI address width is configured to 32-bit, then this SKB requires at least two DMA transmit descriptors to serve it. For example, three descriptors are allocated to split one DMA buffer mapped from one piece of non-paged data: dma_desc[N + 0], dma_desc[N + 1], dma_desc[N + 2]. Then three elements of tx_q->tx_skbuff_dma[] will be allocated to hold extra information to be reused in stmmac_tx_clean(): tx_q->tx_skbuff_dma[N + 0], tx_q->tx_skbuff_dma[N + 1], tx_q->tx_skbuff_dma[N + 2]. Now we focus on tx_q->tx_skbuff_dma[entry].buf, which is the DMA buffer address returned by DMA mapping call. stmmac_tx_clean() will try to unmap the DMA buffer _ONLY_IF_ tx_q->tx_skbuff_dma[entry].buf is a valid buffer address. The expected behavior that saves DMA buffer address of this non-paged data to tx_q->tx_skbuff_dma[entry].buf is: tx_q->tx_skbuff_dma[N + 0].buf = NULL; tx_q->tx_skbuff_dma[N + 1].buf = NULL; tx_q->tx_skbuff_dma[N + 2].buf = dma_map_single(); Unfortunately, the current code misbehaves like this: tx_q->tx_skbuff_dma[N + 0].buf = dma_map_single(); tx_q->tx_skbuff_dma[N + 1].buf = NULL; tx_q->tx_skbuff_dma[N + 2].buf = NULL; On the stmmac_tx_clean() side, when dma_desc[N + 0] is closed by the DMA engine, tx_q->tx_skbuff_dma[N + 0].buf is a valid buffer address obviously, then the DMA buffer will be unmapped immediately. There may be a rare case that the DMA engine does not finish the pending dma_desc[N + 1], dma_desc[N + 2] yet. Now things will go horribly wrong, DMA is going to access a unmapped/unreferenced memory region, corrupted data will be transmited or iommu fault will be triggered :(In contrast, the for-loop that maps SKB fragments behaves perfectly as expected, and that is how the driver should do for both non-paged data and paged frags actually. This patch corrects DMA map/unmap sequences by fixing the array index for tx_q->tx_skbuff_dma[entry].buf when assigning DMA buffer address. Tested and verified on DWXGMAC CORE 3.20a	5.5	More Details
CVE-2024-53060	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: prevent NULL pointer dereference if ATIF is not supported acpi_evaluate_object() may return AE_NOT_FOUND (failure), which would result in dereferencing buffer.pointer (obj) while being NULL. Although this case may be unrealistic for the current code, it is still better to protect against possible bugs. Bail out also when status is AE_NOT_FOUND. This fixes 1 FORWARD_NULL issue reported by Coverity Report: CID 1600951: Null pointer dereferences (FORWARD_NULL) (cherry picked from commit 91c9e221fe2553edf2db71627d8453f083de87a1)	5.5	More Details
CVE-2024-53063	In the Linux kernel, the following vulnerability has been resolved: media: dvbdev: prevent the risk of out of memory access The dvbdev contains a static variable used to store dvb minors. The behavior of it depends if CONFIG_DVB_DYNAMIC_MINORS is set or not. When not set, dvb_register_device() won't check for boundaries, as it will rely that a previous call to dvb_register_adapter() would already be enforcing it. On a similar way, dvb_device_open() uses the assumption that the register functions already did the needed checks. This can be fragile if some device ends using different calls. This also generate warnings on static check analysers like Coverity. So, add explicit guards to prevent potential risk of OOM issues.	5.5	More Details
CVE-2024-53064	In the Linux kernel, the following vulnerability has been resolved: idpf: fix idpf_vc_core_init error path In an event where the platform running the device control plane is rebooted, reset is detected on the driver. It releases all the resources and waits for the reset to complete. Once the reset is done, it tries to build the resources back. At this time if the device control plane is not yet started, then the driver timeouts on the virtchnl message and retries to establish the mailbox again. In the retry flow, mailbox is deinitialized but the mailbox workqueue is still alive and polling for the mailbox message. This results in accessing the released control queue leading to null-ptr-deref. Fix it by unrolling the work queue cancellation and mailbox deinitialization in the reverse order which they got initialized.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-53065	In the Linux kernel, the following vulnerability has been resolved: mm/slab: fix warning caused by duplicate kmem_cache creation in kmem_buckets_create Commit b035f5a6d852 ("mm: slab: reduce the kmalloc() minimum alignment if DMA bouncing possible") reduced ARCH_KMALLOC_MINALIGN to 8 on arm64. However, with KASAN_HW_TAGS enabled, arch_slab_minalign() becomes 16. This causes kmalloc_caches[*][8] to be aliased to kmalloc_caches[*][16], resulting in kmem_buckets_create() attempting to create a kmem_cache for size 16 twice. This duplication triggers warnings on boot: [2.325108] ------------[cut here]------------ [2.325135] kmem_cache of name 'memdup_user-16' already exists [2.325783] WARNING: CPU: 0 PID: 1 at mm/slab_common.c:107 __kmem_cache_create_args+0xb8/0x3b0 [2.327957] Modules linked in: [2.328550] CPU: 0 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.12.0-rc5mm-unstable-arm64+ #12 [2.328683] Hardware name: QEMU QEMU Virtual Machine, BIOS 2024.02-2 03/11/2024 [2.328790] pstate: 61000009 (nZCv daif -PAN -UAO -TCO +DIT -SSBS BTYPE=--) [2.328911] pc : __kmem_cache_create_args+0xb8/0x3b0 [2.328930] lr : __kmem_cache_create_args+0xb8/0x3b0 [2.328942] sp : ffff800083d6fc50 [2.328961] x29: ffff800083d6fc50 x28: f2ff0000c1674410 x27: ffff8000820b0598 [2.329061] x26: 000000007fffffff x25: 0000000000000010 x24: 0000000000002000 [2.329101] x23: ffff800083d6fce8 x22: ffff8000832222e8 x21: ffff800083222388 [2.329118] x20: f2ff0000c1674410 x19: f5ff0000c16364c0 x18: ffff800083d80030 [2.329135] x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 [2.329152] x14: 0000000000000000 x13: 0a73747369786520 x12: 79646165726c6120 [2.329169] x11: 656820747563205b x10: 2d2d2d2d2d2d2d2d x9 : 0000000000000000 [2.329194] x8 : 0000000000000000 x7 : 0000000000000000 x6 : 0000000000000000 [2.329210] x5 : 0000000000000000 x4 : 0000000000000000 x3 : 0000000000000000 [2.329226] x2 : 0000000000000000 x1 : 0000000000000000 x0 : 0000000000000000 [2.329291] Call trace: [2.329407] __kmem_cache_create_args+0xb8/0x3b0 [2.329499] kmem_buckets_create+0xfc/0x320 [2.329526] init_user_buckets+0x34/0x78 [2.329540] do_one_initcall+0x64/0x3c8 [2.329550] kernel_init_freeable+0x26c/0x578 [2.329562] kernel_init+0x3c/0x258 [2.329574] ret_from_fork+0x10/0x20 [2.329698] ---[end trace 0000000000000000]--- [2.403704] ------------[cut here]------------ [2.404716] kmem_cache of name 'msg_msg-16' already exists [2.404801] WARNING: CPU: 2 PID: 1 at mm/slab_common.c:107 __kmem_cache_create_args+0xb8/0x3b0 [2.404842] Modules linked in: [2.404971] CPU: 2 UID: 0 PID: 1 Comm: swapper/0 Tainted: G W 6.12.0-rc5mm-unstable-arm64+ #12 [2.405026] Tainted: [W]=WARN [2.405043] Hardware name: QEMU QEMU Virtual Machine, BIOS 2024.02-2 03/11/2024 [2.405057] pstate: 60400009 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [2.405079] pc : __kmem_cache_create_args+0xb8/0x3b0 [2.405100] lr : __kmem_cache_create_args+0xb8/0x3b0 [2.405111] sp : ffff800083d6fc50 [2.405115] x29: ffff800083d6fc50 x28: fbff0000c1674410 x27: ffff8000820b0598 [2.405135] x26: 000000000000ffd0 x25: 0000000000000010 x24: 0000000000006000 [2.405153] x23: ffff800083d6fce8 x22: ffff8000832222e8 x21: ffff800083222388 [2.405169] x20: fbff0000c1674410 x19: fdff0000c163d6c0 x18: ffff800083d80030 [2.405185] x17: 0000000000000000 x16: 0000000000000000 x15: 0000000000000000 [2.405201] x14: 0000000000000000 x13: 0a73747369786520 x12: 79646165726c6120 [2.405217] x11: 656820747563205b x10: 2d2d2d2d2d2d2d2d x9 : 0000000000000000 [2.405233] x8 : 0000000000000000 x7 : 0000000000000000 x6 : 0000000000000000 [2.405248] x5 : 0000000000000000 x4 : 0000000000000000 x3 : 0000000000000000 [2.405271] x2 : 0000000000000000 x1 : 0000000000000000 x0 : 0000000000000000 [2.405287] Call trace: [2 ---truncated---	5.5	More Details
CVE-2024-53066	In the Linux kernel, the following vulnerability has been resolved: nfs: Fix KMSAN warning in decode_getfattr_attrs() Fix the following KMSAN warning: CPU: 1 UID: 0 PID: 7651 Comm: cp Tainted: G B Tainted: [B]=BAD_PAGE Hardware name: QEMU Standard PC (Q35 + ICH9, 2009) === === BUG: KMSAN: uninit-value in decode_getfattr_attrs+0x2d6d/0x2f90 decode_getfattr_attrs+0x2d6d/0x2f90 decode_getfattr_generic+0x806/0xb00 nfs4_xdr_dec_getattr+0x1de/0x240 rpcauth_unwrap_resp_decode+0xab/0x100 rpcauth_unwrap_resp+0x95/0xc0 call_decode+0x4ff/0xb50 __rpc_execute+0x57b/0x19d0 rpc_execute+0x368/0x5e0 rpc_run_task+0xcfe/0xee0 nfs4_proc_getattr+0x5b5/0x990 __nfs_revalidate_inode+0x477/0xd00 nfs_access_get_cached+0x1021/0x1cc0 nfs_do_access+0x9f/0xae0 nfs_permission+0x1e4/0x8c0 inode_permission+0x356/0x6c0 link_path_walk+0x958/0x1330 path_lookupat+0xce/0x6b0 filename_lookup+0x23e/0x770 vfs_statx+0xe7/0x970 vfs_fstatat+0x1f2/0x2c0 __se_sys_newfstatat+0x67/0x880 __x64_sys_newfstatat+0xbd/0x120 x64_sys_call+0x1826/0x3cf0 do_syscall_64+0xd0/0x1b0 entry_SYSCALL_64_after_hwframe+0x77/0x7f The KMSAN warning is triggered in decode_getfattr_attrs(), when calling decode_attr_mdsthreshold(). It appears that fattr->mdsthreshold is not initialized. Fix the issue by initializing fattr->mdsthreshold to NULL in nfs_fattr_init().	5.5	More Details
CVE-2024-53067	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Start the RTC update work later The RTC update work involves runtime resuming the UFS controller. Hence, only start the RTC update work after runtime power management in the UFS driver has been fully initialized. This patch fixes the following kernel crash: Internal error: Oops: 0000000096000006 [#1] PREEMPT SMP Workqueue: events ufshcd_rtc_work Call trace: _raw_spin_lock_irqsave+0x34/0x8c (P) pm_runtime_get_if_active+0x24/0x9c (L) pm_runtime_get_if_active+0x24/0x9c ufshcd_rtc_work+0x138/0x1b4 process_one_work+0x148/0x288 worker_thread+0x2cc/0x3d4 kthread+0x110/0x114 ret_from_fork+0x10/0x20	5.5	More Details
CVE-2024-53069	In the Linux kernel, the following vulnerability has been resolved: firmware: qcom: scm: fix a NULL-pointer dereference Some SCM calls can be invoked with __scm being NULL (the driver may not have been and will not be probed as there's no SCM entry in device-tree). Make sure we don't dereference a NULL pointer.	5.5	More Details
CVE-2024-53070	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: fix fault at system suspend if device was already runtime suspended If the device was already runtime suspended then during system suspend we cannot access the device registers else it will crash. Also we cannot access any registers after dwc3_core_exit() on some platforms so move the dwc3_enable_susphy() call to the top.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-53071	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Be stricter about IO mapping flags The current panthor_device_mmap_io() implementation has two issues: 1. For mapping DRM_PANTHOR_USER_FLUSH_ID_MMIO_OFFSET, panthor_device_mmap_io() bails if VM_WRITE is set, but does not clear VM_MAYWRITE. That means userspace can use mprotect() to make the mapping writable later on. This is a classic Linux driver gotcha. I don't think this actually has any impact in practice: When the GPU is powered, writes to the FLUSH_ID seem to be ignored; and when the GPU is not powered, the dummy_latest_flush page provided by the driver is deliberately designed to not do any flushes, so the only thing writing to the dummy_latest_flush could achieve would be to make *more* flushes happen. 2. panthor_device_mmap_io() does not block MAP_PRIVATE mappings (which are mappings without the VM_SHARED flag). MAP_PRIVATE in combination with VM_MAYWRITE indicates that the VMA has copy-on-write semantics, which for VM_PFNMAP are semi-supported but fairly cursed. In particular, in such a mapping, the driver can only install PTEs during mmap() by calling remap_pfn_range() (because remap_pfn_range() wants to **store the physical address of the mapped physical memory into the vm_pgoff of the VMA**); installing PTEs later on with a fault handler (as panthor does) is not supported in private mappings, and so if you try to fault in such a mapping, vmf_insert_pfn_prot() splats when it hits a BUG() check. Fix it by clearing the VM_MAYWRITE flag (userspace writing to the FLUSH_ID doesn't make sense) and requiring VM_SHARED (copy-on-write semantics for the FLUSH_ID don't make sense). Reproducers for both scenarios are in the notes of my patch on the mailing list; I tested that these bugs exist on a Rock 5B machine. Note that I only compile-tested the patch, I haven't tested it; I don't have a working kernel build setup for the test machine yet. Please test it before applying it.	5.5	More Details
CVE-2024-40579	Cross Site Scripting vulnerability in Virtuozzo Hybrid Server for WHMCS Open Source v.1.7.1 allows a remote attacker to obtain sensitive information via modification of the hostname parameter.	5.4	More Details
CVE-2024-49025	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	5.4	More Details
CVE-2020-26063	A vulnerability in the API endpoints of Cisco Integrated Management Controller could allow an authenticated, remote attacker to bypass authorization and take actions on a vulnerable system without authorization. The vulnerability is due to improper authorization checks on API endpoints. An attacker could exploit this vulnerability by sending malicious requests to an API endpoint. An exploit could allow the attacker to download files from or modify limited configuration options on the affected system.There are no workarounds that address this vulnerability.	5.4	More Details
CVE-2024-1097	A stored cross-site scripting (XSS) vulnerability exists in craigk5n/webcalendar version 1.3.0. The vulnerability occurs in the 'Report Name' input field while creating a new report. An attacker can inject malicious scripts, which are then executed in the context of other users who view the report, potentially leading to the theft of user accounts and cookies.	5.4	More Details
CVE-2024-50655	emlog pro <=2.3.18 is vulnerable to Cross Site Scripting (XSS), which allows attackers to write malicious JavaScript code in published articles.	5.4	More Details
CVE-2021-3741	A stored cross-site scripting (XSS) vulnerability was discovered in chatwoot/chatwoot, affecting all versions prior to 2.6. The vulnerability occurs when a user uploads an SVG file containing a malicious XSS payload in the profile settings. When the avatar is opened in a new page, the custom JavaScript code is executed, leading to potential security risks.	5.4	More Details
CVE-2021-3841	sylius/sylius versions prior to 1.9.10, 1.10.11, and 1.11.2 are vulnerable to stored cross-site scripting (XSS) through SVG files. This vulnerability allows attackers to inject malicious scripts that can be executed in the context of the user's browser.	5.4	More Details
CVE-2021-1466	A vulnerability in the vDaemon service of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to cause a buffer overflow on an affected system, resulting in a denial of service (DoS) condition. The vulnerability is due to incomplete bounds checks for data that is provided to the vDaemon service of an affected system. An attacker could exploit this vulnerability by sending malicious data to the vDaemon listening service on the affected system. A successful exploit could allow the attacker to cause a buffer overflow condition on the affected system, which could allow the attacker to cause the vDaemon listening service to reload and result in a DoS condition.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	5.4	More Details
CVE-2023-0109	A stored cross-site scripting (XSS) vulnerability was discovered in usememos/memos version 0.9.1. This vulnerability allows an attacker to upload a JavaScript file containing a malicious script and reference it in an HTML file. When the HTML file is accessed, the malicious script is executed. This can lead to the theft of sensitive information, such as login credentials, from users visiting the affected website. The issue has been fixed in version 0.10.0.	5.4	More Details
CVE-2024-52505	matrix-appservice-irc is a Node.js IRC bridge for the Matrix messaging protocol. The provisioning API of the matrix-appservice-irc bridge up to version 3.0.2 contains a vulnerability which can lead to arbitrary IRC command execution as the bridge IRC bot. The vulnerability has been patched in matrix-appservice-irc version 3.0.3.	5.4	More Details
CVE-2024-11239	A vulnerability has been found in Landray EKP up to 16.0 and classified as critical. This vulnerability affects the function deleteFile of the file /sys/common/import.do?method=deleteFile of the component API Interface. The manipulation of the argument folder leads to path traversal. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2024-51817	Missing Authorization vulnerability in CodeZel Combo WP Rewrite Slugs allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Combo WP Rewrite Slugs: from n/a through 1.0.	5.4	More Details
CVE-2024-4311	zenml-io/zenml version 0.56.4 is vulnerable to an account takeover due to the lack of rate-limiting in the password change function. An attacker can brute-force the current password in the 'Update Password' function, allowing them to take over the user's account. This vulnerability is due to the absence of rate-limiting on the '/api/v1/current-user' endpoint, which does not restrict the number of attempts an attacker can make to guess the current password. Successful exploitation results in the attacker being able to change the password and take control of the account.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50983	FlightPath 7.5 contains a Cross Site Scripting (XSS) vulnerability, which allows authenticated remote attackers with administrative rights to inject arbitrary JavaScript in the web browser of a user by including a malicious payload into the Last Name section in the Create/Edit Faculty/Staff User or Create/Edit Student User sections.	5.4	More Details
CVE-2024-50838	A Stored Cross-Site Scripting (XSS) vulnerability was found in /admin/department.php in KASHIPARA E-learning Management System Project 1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the d and pi parameters.	5.4	More Details
CVE-2024-52942	An issue was discovered in Veritas Enterprise Vault before 15.1 UPD882911, ZDI-CAN-24696. It allows an authenticated remote attacker to inject a parameter into an HTTP request, allowing for Cross-Site Scripting (XSS) while viewing archived content. This could reflect back to an authenticated user without sanitization if executed by that user.	5.4	More Details
CVE-2024-28169	Cleartext transmission of sensitive information for some BigDL software maintained by Intel(R) before version 2.5.0 may allow an authenticated user to potentially enable denial of service via adjacent access.	5.4	More Details
CVE-2024-50837	A Stored Cross-Site Scripting (XSS) vulnerability was found in /admin/admin_user.php in KASHIPARA E-learning Management System Project 1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the firstname and username parameters.	5.4	More Details
CVE-2024-11085	The WP Log Viewer plugin for WordPress is vulnerable to unauthorized use of functionality due to a missing capability check on several AJAX actions in all versions up to, and including, 1.2.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to access logs, update plugin-related user settings and general plugin settings.	5.4	More Details
CVE-2024-33231	Cross Site Scripting vulnerability in Ferozo Email version 1.1 allows a local attacker to execute arbitrary code via a crafted payload to the PDF preview component.	5.4	More Details
CVE-2024-42834	A stored cross-site scripting (XSS) vulnerability in the Create Customer API in Incognito Service Activation Center (SAC) UI v14.11 allows authenticated attackers to execute arbitrary web scripts or HTML via injecting a crafted payload into the lastName parameter.	5.4	More Details
CVE-2024-52941	An issue was discovered in Veritas Enterprise Vault before 15.1 UPD882911, ZDI-CAN-24695. It allows an authenticated remote attacker to inject a parameter into an HTTP request, allowing for Cross-Site Scripting (XSS) while viewing archived content. This could reflect back to an authenticated user without sanitization if executed by that user.	5.4	More Details
CVE-2024-52943	An issue was discovered in Veritas Enterprise Vault before 15.1 UPD882911, ZDI-CAN-24697. It allows an authenticated remote attacker to inject a parameter into an HTTP request, allowing for Cross-Site Scripting (XSS) while viewing archived content. This could reflect back to an authenticated user without sanitization if executed by that user.	5.4	More Details
CVE-2024-45875	The create user function in baltic-it TOPqw Webportal 1.35.287.1 (fixed in version1.35.291), in /Apps/TOPqw/BenutzerManagement.aspx/SaveNewUser, is vulnerable to SQL injection. The JSON object username allows the manipulation of SQL queries.	5.4	More Details
CVE-2024-52944	An issue was discovered in Veritas Enterprise Vault before 15.1 UPD882911, ZDI-CAN-24698. It allows an authenticated remote attacker to inject a parameter into an HTTP request, allowing for Cross-Site Scripting while viewing archived content. This could reflect back to an authenticated user without sanitization if executed by that user.	5.4	More Details
CVE-2024-52947	A cross-site scripting (XSS) vulnerability in LemonLDAP::NG before 2.20.1 allows remote attackers to inject arbitrary web script or HTML via the url parameter of the upgrade session confirmation page (upgradeSession / forceUpgrade) if the "Upgrade session" plugin has been enabled by an admin	5.4	More Details
CVE-2024-41968	A low privileged remote attacker may modify the docker settings setup of the device, leading to a limited DoS.	5.4	More Details
CVE-2020-26067	A vulnerability in the web-based interface of Cisco Webex Teams could allow an authenticated, remote attacker to conduct cross-site scripting attacks. The vulnerability is due to improper validation of usernames. An attacker could exploit this vulnerability by creating an account that contains malicious HTML or script content and joining a space using the malicious account name. A successful exploit could allow the attacker to conduct cross-site scripting attacks and potentially gain access to sensitive browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	5.4	More Details
CVE-2024-52762	A cross-site scripting (XSS) vulnerability in the component /master/header.php of Ganglia-web v3.73 to v3.76 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the "tz" parameter.	5.4	More Details
CVE-2024-52763	A cross-site scripting (XSS) vulnerability in the component /graph_all_periods.php of Ganglia-web v3.73 to v3.75 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the "g" parameter.	5.4	More Details
CVE-2024-51142	Cross Site Scripting vulnerability in Chamilo LMS v.1.11.26 allows an attacker to execute arbitrary code via the svkey parameter of the storageapi.php file.	5.4	More Details
CVE-2022-47424	Cross-Site Request Forgery (CSRF) vulnerability in Repute InfoSystems ARMember, Repute InfoSystems ARMember Premium allows Cross-Site Request Forgery.This issue affects ARMember: from n/a through 4.0.5; ARMember Premium: from n/a before 6.7.1.	5.4	More Details
CVE-2024-45878	The "Stammdaten" menu of baltic-it TOPqw Webportal v1.35.283.2 (fixed in version 1.35.291), in /Apps/TOPqw/qwStammdaten.aspx, is vulnerable to persistent Cross-Site Scripting (XSS).	5.4	More Details
CVE-2024-50800	Cross Site Scripting vulnerability in M2000 Smart4Web before v.5.020241004 allows a remote attacker to execute arbitrary code via the error parameter in URL	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-11210	A vulnerability was found in EyouCMS 1.51. It has been rated as critical. This issue affects the function editFile of the file application/admin/logic/FilemanagerLogic.php. The manipulation of the argument activepath leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.4	More Details
CVE-2024-50842	A Stored Cross-Site Scripting (XSS) vulnerability was found in /admin/school_year.php in KASHIPARA E-learning Management System Project 1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the school_year parameter.	5.4	More Details
CVE-2024-50841	A Stored Cross-Site Scripting (XSS) vulnerability was found in /admin/calendar_of_events.php in KASHIPARA E-learning Management System Project 1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the date_start, date_end, and title parameters.	5.4	More Details
CVE-2024-49689	Missing Authorization vulnerability in Harmonic Design HD Quiz – Save Results Light allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects HD Quiz – Save Results Light: from n/a through 0.5.	5.4	More Details
CVE-2024-50840	A Stored Cross-Site Scripting (XSS) vulnerability was found in /admin/class.php in KASHIPARA E-learning Management System Project 1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the class_name parameter.	5.4	More Details
CVE-2024-50839	A Stored Cross-Site Scripting (XSS) vulnerability was found in /admin/add_subject.php in KASHIPARA E-learning Management System Project 1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the subject_code and title parameters.	5.4	More Details
CVE-2024-50803	The mediapool feature of the Redaxo Core CMS application v 5.17.1 is vulnerable to Cross Site Scripting(XSS) which allows a remote attacker to escalate privileges	5.4	More Details
CVE-2022-20948	A vulnerability in the web management interface of Cisco BroadWorks Hosted Thin Receptionist could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient user input validation. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	5.4	More Details
CVE-2024-8180	An issue has been discovered in GitLab CE/EE affecting all versions from 17.3 before 17.3.7, 17.4 before 17.4.4, and 17.5 before 17.5.2. Improper output encoding could lead to XSS if CSP is not enabled.	5.4	More Details
CVE-2024-45879	The file upload function in the "QWKalkulation" tool of baltic-it TOPqw Webportal v1.35.287.1 (fixed in version 1.35.291), in /Apps/TOPqw/QWKalkulation/QWKalkulation.aspx, is vulnerable to Cross-Site Scripting (XSS). To exploit the persistent XSS vulnerability, an attacker has to be authenticated to the application that uses the "TOPqw Webportal" as a software. When authenticated, the attacker can persistently place the malicious JavaScript code in the "QWKalkulation" menu.'	5.4	More Details
CVE-2024-10146	The Simple File List WordPress plugin before 6.1.13 does not sanitise and escape a generated URL before outputting it back in an attribute, leading to a Reflected Cross-Site Scripting which could be used against admins.	5.4	More Details
CVE-2024-42499	Improper limitation of a pathname to a restricted directory ('Path Traversal') issue exists in FitNesse releases prior to 20241026. If this vulnerability is exploited, an attacker may be able to know whether a file exists at a specific path, and/or obtain some part of the file contents under specific conditions.	5.3	More Details
CVE-2022-20648	A vulnerability in a debug function for Cisco RCM for Cisco StarOS Software could allow an unauthenticated, remote attacker to perform debug actions that could result in the disclosure of confidential information that should be restricted. This vulnerability exists because of a debug service that incorrectly listens to and accepts incoming connections. An attacker could exploit this vulnerability by connecting to the debug port and executing debug commands. A successful exploit could allow the attacker to view sensitive debugging information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	5.3	More Details
CVE-2024-10531	The Kognetiks Chatbot for WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the update_assistant() function in all versions up to, and including, 2.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to update GTP assistants.	5.3	More Details
CVE-2024-10802	The Hash Elements plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the hash_elements_get_posts_title_by_id() function in all versions up to, and including, 1.4.7. This makes it possible for unauthenticated attackers to retrieve draft post titles that should not be accessible to unauthenticated users.	5.3	More Details
CVE-2024-8001	A vulnerability was found in VIWIS LMS 9.11. It has been classified as critical. Affected is an unknown function of the component Print Handler. The manipulation leads to missing authorization. It is possible to launch the attack remotely. A user with the role learner can use the administrative print function with an active session before and after an exam slot to access the entire exam including solutions in the web application. It is recommended to apply a patch to fix this issue.	5.3	More Details
CVE-2022-20766	A vulnerability in the Cisco Discovery Protocol functionality of Cisco ATA 190 Series Adaptive Telephone Adapter firmware could allow an unauthenticated, remote attacker to cause a DoS condition on an affected device. This vulnerability is due to an out-of-bounds read when processing Cisco Discovery Protocol packets. An attacker could exploit this vulnerability by sending crafted Cisco Discovery Protocol packets to an affected device. A successful exploit could allow the attacker to cause a service restart.Cisco has released firmware updates that address this vulnerability. There are no workarounds that address this vulnerability.	5.3	More Details
CVE-2024-50843	A Directory listing issue was found in PHPGurukul User Registration & Login and User Management System 3.2, which allows remote attackers attacker to access sensitive files and directories via /loginsystem/assets.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9578	The Hide Links plugin for WordPress is vulnerable to unauthorized shortcode execution due to do_shortcode being hooked through the comment_text filter in all versions up to and including 1.4.2. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes available on the target site.	5.3	More Details
CVE-2024-39707	Insyde IHISI function 0x49 can restore factory defaults for certain UEFI variables without further authentication by default, which could lead to a possible roll-back attack in certain platforms. This is fixed in: kernel 5.2, version 05.29.19; kernel 5.3, version 05.38.19; kernel 5.4, version 05.46.19; kernel 5.5, version 05.54.19; kernel 5.6, version 05.61.19.	5.3	More Details
CVE-2024-45642	IBM Security ReaQta 3.12 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	5.3	More Details
CVE-2024-52395	Missing Authorization vulnerability in QunatumCloud Floating Buttons for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Floating Buttons for WooCommerce: from n/a through 2.8.8.	5.3	More Details
CVE-2024-52600	Statmatic is a Laravel and Git powered content management system (CMS). Prior to version 5.17.0, assets uploaded with appropriately crafted filenames may result in them being placed in a location different than what was configured. The issue affects front-end forms with `assets` fields and other places where assets can be uploaded, although users would need upload permissions anyway. Files can be uploaded so they would be located on the server in a different location, and potentially override existing files. Traversal outside an asset container is not possible. This path traversal vulnerability has been fixed in 5.17.0.	5.3	More Details
CVE-2024-39285	Improper access control in UEFI firmware in some Intel(R) Server M20NTP Family may allow a privileged user to potentially enable information disclosure via local access.	5.3	More Details
CVE-2020-26062	A vulnerability in Cisco Integrated Management Controller could allow an unauthenticated, remote attacker to enumerate valid usernames within the vulnerable application. The vulnerability is due to differences in authentication responses sent back from the application as part of an authentication attempt. An attacker could exploit this vulnerability by sending authentication requests to the affected application. A successful exploit could allow the attacker to confirm the names of administrative user accounts for use in further attacks.There are no workarounds that address this vulnerability.	5.3	More Details
CVE-2024-10224	Qualys discovered that if unsanitized input was used with the library Modules::ScanDeps, before version 1.36 a local attacker could possibly execute arbitrary shell commands by open()ing a "pesky pipe" (such as passing "commandsl" as a filename) or by passing arbitrary strings to eval().	5.3	More Details
CVE-2024-23919	Improper buffer restrictions in some Intel(R) Graphics software may allow an authenticated user to potentially enable escalation of privilege via local access.	5.3	More Details
CVE-2024-20373	A vulnerability in the implementation of the Simple Network Management Protocol (SNMP) IPv4 access control list (ACL) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to perform SNMP polling of an affected device, even if it is configured to deny SNMP traffic. This vulnerability exists because Cisco IOS Software and Cisco IOS XE Software do not support extended IPv4 ACLs for SNMP, but they do allow administrators to configure extended named IPv4 ACLs that are attached to the SNMP server configuration without a warning message. This can result in no ACL being applied to the SNMP listening process. An attacker could exploit this vulnerability by performing SNMP polling of an affected device. A successful exploit could allow the attacker to perform SNMP operations that should be denied. The attacker has no control of the SNMP ACL configuration and would still need a valid SNMP version 2c (SNMPv2c) community string or SNMP version 3 (SNMPv3) user credentials. SNMP with IPv6 ACL configurations is not affected. For more information, see the section of this advisory.	5.3	More Details
CVE-2024-10529	The Kognetiks Chatbot for WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the delete_assistant() function in all versions up to, and including, 2.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to delete GTP assistants.	5.3	More Details
CVE-2024-52921	In Bitcoin Core before 25.0, a peer can affect the download state of other peers by sending a mutated block.	5.3	More Details
CVE-2024-52386	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Business Directory Team by RadiusTheme Classified Listing classified-listing allows PHP Local File Inclusion.This issue affects Classified Listing: from n/a through 3.1.15.1.	5.3	More Details
CVE-2024-42387	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and force the application to read unintended heap memory space.	5.3	More Details
CVE-2024-24450	Stack-based memcpy buffer overflow in the ngap_handle_pdu_session_resource_setup_response routine in OpenAirInterface CN5G AMF <= 2.0.0 allows a remote attacker with access to the N2 interface to carry out denial of service against the AMF and potentially execute code by sending a PDU Session Resource Setup Response with a suffciently large FailedToSetupList IE.	5.3	More Details
CVE-2024-10486	The Google for WooCommerce plugin for WordPress is vulnerable to Information Disclosure in all versions up to, and including, 2.8.6. This is due to publicly accessible print_php_information.php file. This makes it possible for unauthenticated attackers to retrieve information about Webserver and PHP configuration, which can be used to aid other attacks.	5.3	More Details
CVE-2024-52913	In Bitcoin Core before 0.21.0, an attacker could prevent a node from seeing a specific unconfirmed transaction, because transaction re-requests are mishandled.	5.3	More Details
CVE-2024-38828	Spring MVC controller methods with an @RequestBody byte[] method parameter are vulnerable to a DoS attack.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-11306	A vulnerability, which was classified as critical, has been found in Altenergy Power Control Software up to 20241108. This issue affects some unknown processing of the file /index.php/display/database/. The manipulation leads to improper authorization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other endpoints might be affected as well. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2024-11094	The 404 Solution plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.35.17 via the export feature. This makes it possible for unauthenticated attackers to extract sensitive data such as redirects including GET parameters which may reveal sensitive information.	5.3	More Details
CVE-2024-42389	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and force the application to read unintended heap memory space.	5.3	More Details
CVE-2022-20633	A vulnerability in the web-based management interface of Cisco ECE could allow an unauthenticated, remote attacker to perform a username enumeration attack against an affected device. This vulnerability is due to differences in authentication responses that are sent back from the application as part of an authentication attempt. An attacker could exploit this vulnerability by sending authentication requests to an affected device. A successful exploit could allow the attacker to confirm existing user accounts, which could be used in further attacks. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	5.3	More Details
CVE-2024-11118	The 404 Error Monitor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.1. This is due to missing or incorrect nonce validation on the updatePluginSettings() function. This makes it possible for unauthenticated attackers to make changes to plugin settings and clear up all the error logs via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.3	More Details
CVE-2024-10861	The Popup Box – Create Countdown, Coupon, Video, Contact Form Popups plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the deactivate_plugin_option() function in all versions up to, and including, 4.9.7. This makes it possible for unauthenticated attackers to update the 'ays_pb_upgrade_plugin' option with arbitrary data.	5.3	More Details
CVE-2024-11262	A vulnerability has been found in SourceCodester Student Record Management System 1.0 and classified as critical. Affected by this vulnerability is the function main of the component View All Student Marks. The manipulation leads to stack-based buffer overflow. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2024-38370	GLPI is a free asset and IT management software package. Starting in 9.2.0 and prior to 11.0.0, it is possible to download a document from the API without appropriate rights. Upgrade to 10.0.16.	5.3	More Details
CVE-2024-11261	A vulnerability, which was classified as critical, was found in SourceCodester Student Record Management System 1.0. Affected is an unknown function of the file StudentRecordManagementSystem.cpp of the component Number of Students Menu. The manipulation leads to memory corruption. Attacking locally is a requirement. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2024-42388	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and force the application to read unintended heap memory space.	5.3	More Details
CVE-2024-51037	An issue in kodbox v.1.52.04 and before allows a remote attacker to obtain sensitive information via the captcha feature in the password reset function.	5.3	More Details
CVE-2021-1234	A vulnerability in the cluster management interface of Cisco SD-WAN vManage Software could allow an unauthenticated, remote attacker to view sensitive information on an affected system. To be affected by this vulnerability, the vManage software must be in cluster mode. This vulnerability is due to the absence of authentication for sensitive information in the cluster management interface. An attacker could exploit this vulnerability by sending a crafted request to the cluster management interface of an affected system. A successful exploit could allow the attacker to view sensitive information on the affected system.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	5.3	More Details
CVE-2024-24447	A buffer overflow in the ngap_amf_handle_pdu_session_resource_setup_response function of oai-cn5g-amf up to v2.0.0 allows attackers to cause a Denial of Service (DoS) via a PDU Session Resource Setup Response with an empty Response Item list.	5.3	More Details
CVE-2020-3548	A vulnerability in the Transport Layer Security (TLS) protocol implementation of Cisco AsyncOS software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to cause high CPU usage on an affected device, resulting in a denial of service (DoS) condition. The vulnerability is due to inefficient processing of incoming TLS traffic. An attacker could exploit this vulnerability by sending a series of crafted TLS packets to an affected device. A successful exploit could allow the attacker to trigger a prolonged state of high CPU utilization. The affected device would still be operative, but response time and overall performance may be degraded.There are no workarounds that address this vulnerability.	5.3	More Details
CVE-2024-11023	Firebase JavaScript SDK utilizes a "FIREBASE_DEFAULTS" cookie to store configuration data, including an "_authTokenSyncURL" field used for session synchronization. If this cookie field is preset via an attacker by any other method, the attacker can manipulate the "_authTokenSyncURL" to point to their own server and it would allow an actor to capture user session data transmitted by the SDK. We recommend upgrading Firebase JS SDK at least to 10.9.0.	5.3	More Details
CVE-2021-1132	A vulnerability in the API subsystem and in the web-management interface of Cisco Network Services Orchestrator (NSO) could allow an unauthenticated, remote attacker to access sensitive data. This vulnerability exists because the web-management interface and certain HTTP-based APIs do not properly validate user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to access sensitive files on the affected system.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1424	A vulnerability in the ipsecmgr process of Cisco ASR 5000 Series Software (StarOS) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. This vulnerability is due to insufficient validation of incoming Internet Key Exchange Version 2 (IKEv2) packets. An attacker could exploit this vulnerability by sending specifically malformed IKEv2 packets to an affected device. A successful exploit could allow the attacker to cause the ipsecmgr process to restart, which would disrupt ongoing IKE negotiations and result in a temporary DoS condition.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	5.3	More Details
CVE-2023-20091	A vulnerability in the CLI of Cisco TelePresence CE and RoomOS could allow an authenticated, local attacker to overwrite arbitrary files on the local file system of an affected device. This vulnerability is due to improper access controls on files that are on the local file system. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. To exploit this vulnerability, an attacker would need to have a remote support user account. Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	5.1	More Details
CVE-2021-1464	A vulnerability in Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization checking and gain restricted access to the configuration information of an affected system. This vulnerability exists because the affected software has insufficient input validation for certain commands. An attacker could exploit this vulnerability by sending crafted requests to the affected commands of an affected system. A successful exploit could allow the attacker to bypass authorization checking and gain restricted access to the configuration data of the affected system.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	5.0	More Details
CVE-2024-43090	In multiple locations, there is a possible cross-user image read due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation.	5.0	More Details
CVE-2021-1470	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability is due to improper input validation of SQL queries to an affected system. An attacker could exploit this vulnerability by authenticating to the application and sending malicious SQL queries to an affected system. A successful exploit could allow the attacker to modify values on or return values from the vManage database or the underlying operating system.Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.	4.9	More Details
CVE-2021-1461	A vulnerability in the Image Signature Verification feature of Cisco SD-WAN Software could allow an authenticated, remote attacker with Administrator-level credentials to install a malicious software patch on an affected device. The vulnerability is due to improper verification of digital signatures for patch images. An attacker could exploit this vulnerability by crafting an unsigned software patch to bypass signature checks and loading it on an affected device. A successful exploit could allow the attacker to boot a malicious software patch image.Cisco has released software updates that address the vulnerability described in this advisory. There are no workarounds that address this vulnerability.	4.9	More Details
CVE-2024-52390	: Path Traversal: '.../...//' vulnerability in CYAN Backup allows Path Traversal.This issue affects CYAN Backup: from n/a through 2.5.3.	4.9	More Details
CVE-2024-11217	A vulnerability was found in the OAuth-server. OAuth-server logs the OAuth2 client secret when the logLevel is Debug higher for OIDC/GitHub/GitLab/Google IDPs login options.	4.9	More Details
CVE-2024-52396	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in realmag777 WOLF allows Path Traversal.This issue affects WOLF: from n/a through 1.0.8.3.	4.9	More Details
CVE-2024-50836	A Stored Cross-Site Scripting (XSS) vulnerability was found in /admin/teachers.php in KASHIPARA E-learning Management System Project 1.0. This vulnerability allows remote attackers to execute arbitrary scripts via the firstname and lastname parameters.	4.8	More Details
CVE-2024-21783	Integer overflow for some Intel(R) VPL software before version 24.1.4 may allow an authenticated user to potentially enable escalation of privilege via local access.	4.8	More Details
CVE-2024-52268	Cross-site scripting vulnerability exists in VK All in One Expansion Unit versions prior to 9.100.1.0. If this vulnerability is exploited, an arbitrary script may be executed on the web browser of the user who is accessing the web site using the product.	4.8	More Details
CVE-2024-40410	Cybele Software Thinfinity Workspace before v7.0.2.113 was discovered to contain a hardcoded cryptographic key used for encryption.	4.8	More Details
CVE-2024-50352	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Services" section of the Device Overview page allows authenticated users to inject arbitrary JavaScript through the "name" parameter when adding a service to a device. This vulnerability could result in the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and enabling unauthorized actions. This vulnerability is fixed in 24.10.0.	4.8	More Details
CVE-2024-49758	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. User with Admin role can add Notes to a device, the application did not properly sanitize the user input, when the ExamplePlugin enable, if java script code is inside the device's Notes, its will be trigger. This vulnerability is fixed in 24.10.0.	4.8	More Details
CVE-2024-51495	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the Device Overview page allows authenticated users to inject arbitrary JavaScript through the "overwrite_ip" parameter when editing a device. This vulnerability results in the execution of malicious code when the device overview page is visited, potentially compromising the accounts of other users. This vulnerability is fixed in 24.10.0.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48284	A Reflected Cross-Site Scripting (XSS) vulnerability was found in the /search-result.php page of the PHPGurukul User Registration & Login and User Management System 3.2. This vulnerability allows remote attackers to execute arbitrary scripts via the searchkey parameter in a POST HTTP request.	4.8	More Details
CVE-2024-50355	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. User with Admin role can edit the Display Name of a device, the application did not properly sanitize the user input in the device Display Name, if java script code is inside the name of the device Display Name, its can be trigger from different sources. This vulnerability is fixed in 24.10.0.	4.8	More Details
CVE-2024-50351	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Reflected Cross-Site Scripting (XSS) vulnerability in the "section" parameter of the "logs" tab of a device allows attackers to inject arbitrary JavaScript. This vulnerability results in the execution of malicious code when a user accesses the page with a malicious "section" parameter, potentially compromising their session and enabling unauthorized actions. The issue arises from a lack of sanitization in the "report_this()" function. This vulnerability is fixed in 24.10.0.	4.8	More Details
CVE-2024-50350	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Port Settings" page allows authenticated users to inject arbitrary JavaScript through the "name" parameter when creating a new Port Group. This vulnerability results in the execution of malicious code when the "Port Settings" page is visited after the affected Port Group is added to a device, potentially compromising user sessions and allowing unauthorized actions. This vulnerability is fixed in 24.10.0.	4.8	More Details
CVE-2024-49764	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Capture Debug Information" page allows authenticated users to inject arbitrary JavaScript through the "hostname" parameter when creating a new device. This vulnerability results in the execution of malicious code when the "Capture Debug Information" page is visited, redirecting the user and sending non-httponly cookies to an attacker-controlled domain. This vulnerability is fixed in 24.10.0.	4.8	More Details
CVE-2024-51494	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Port Settings" page allows authenticated users to inject arbitrary JavaScript through the "descr" parameter when editing a device's port settings. This vulnerability can lead to the execution of malicious code when the "Port Settings" page is visited, potentially compromising the user's session and allowing unauthorized actions. This vulnerability is fixed in 24.10.0.	4.8	More Details
CVE-2024-49759	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Manage User Access" page allows authenticated users to inject arbitrary JavaScript through the "bill_name" parameter when creating a new bill. This vulnerability can lead to the execution of malicious code when visiting the "Bill Access" dropdown in the user's "Manage Access" page, potentially compromising user sessions and allowing unauthorized actions. This vulnerability is fixed in 24.10.0.	4.8	More Details
CVE-2024-51497	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Custom OID" tab of a device allows authenticated users to inject arbitrary JavaScript through the "unit" parameter when creating a new OID. This vulnerability can lead to the execution of malicious code in the context of other users' sessions, compromising their accounts and enabling unauthorized actions. This vulnerability is fixed in 24.10.0.	4.8	More Details
CVE-2024-51496	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Reflected Cross-Site Scripting (XSS) vulnerability in the "metric" parameter of the "/wireless" and "/health" endpoints allows attackers to inject arbitrary JavaScript. This vulnerability results in the execution of malicious code when a user accesses the page with a malicious "metric" parameter, potentially compromising their session and allowing unauthorized actions. This vulnerability is fixed in 24.10.0.	4.8	More Details
CVE-2024-0875	A stored cross-site scripting (XSS) vulnerability exists in openemr/openemr version 7.0.1. An attacker can inject malicious payloads into the 'inputBody' field in the Secure Messaging feature, which can then be sent to other users. When the recipient views the malicious message, the payload is executed, potentially compromising their account. This issue is fixed in version 7.0.2.1.	4.8	More Details
CVE-2024-52526	LibreNMS is an open-source, PHP/MySQL/SNMP-based network monitoring system. A Stored Cross-Site Scripting (XSS) vulnerability in the "Services" tab of the Device page allows authenticated users to inject arbitrary JavaScript through the "descr" parameter when adding a service to a device. This vulnerability could result in the execution of malicious code in the context of other users' sessions, potentially compromising their accounts and enabling unauthorized actions. This vulnerability is fixed in 24.10.0.	4.8	More Details
CVE-2024-50849	A Stored Cross-Site Scripting (XSS) vulnerability in the "Rules" functionality of WorldServer v11.8.2 allows a remote authenticated attacker to execute arbitrary JavaScript code.	4.8	More Details
CVE-2023-2332	A stored Cross-site Scripting (XSS) vulnerability exists in the Conditions tab of Pricing Rules in pimcore/pimcore versions 10.5.19. The vulnerability is present in the From and To fields of the Date Range section, allowing an attacker to inject malicious scripts. This can lead to the execution of arbitrary JavaScript code in the context of the user's browser, potentially stealing cookies or redirecting users to malicious sites. The issue is fixed in version 10.5.21.	4.8	More Details
CVE-2023-38920	Cross Site Scripting vulnerability in Cyber Cafe Management System v.1.0 allows a local attacker to execute arbitrary code via a crafted script to the adminname parameter.	4.8	More Details
CVE-2022-1226	A Cross-Site Scripting (XSS) vulnerability in phpipam/phpipam versions prior to 1.4.7 allows attackers to execute arbitrary JavaScript code in the browser of a victim. This vulnerability affects the import Data set feature via a spreadsheet file upload. The affected endpoints include import-vlan-preview.php, import-subnets-preview.php, import-vrf-preview.php, import-ipaddr-preview.php, import-devtype-preview.php, import-devices-preview.php, and import-l2dom-preview.php. The vulnerability can be exploited by uploading a specially crafted spreadsheet file containing malicious JavaScript payloads, which are then executed in the context of the victim's browser. This can lead to defacement of websites, execution of malicious JavaScript code, stealing of user cookies, and unauthorized access to user accounts.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-52582	Cachi2 is a command-line interface tool that pre-fetches a project's dependencies to aid in making the project's build process network-isolated. Prior to version 0.14.0, secrets may be shown in logs when an unhandled exception is triggered because the tool is logging locals of each function. This may uncover secrets if tool used in CI/build pipelines as it's the main use case. Version 0.14.0 contains a patch for the issue. No known workarounds are available.	4.7	More Details
CVE-2024-11211	A vulnerability classified as critical has been found in EyouCMS up to 1.6.7. Affected is an unknown function of the component Website Logo Handler. The manipulation 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 vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-11242	A vulnerability was found in ZZCMS 2023. It has been rated as critical. Affected by this issue is some unknown functionality of the file /admin/ad_list.php?action=pass of the component Keyword Filtering. The manipulation of the argument keyword leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-50297	In the Linux kernel, the following vulnerability has been resolved: net: xilinx: axienet: Enqueue Tx packets in dql before dmaengine starts Enqueue packets in dql after dma engine starts causes race condition. Tx transfer starts once dma engine is started and may execute dql dequeue in completion before it gets queued. It results in following kernel crash while running iperf stress test: kernel BUG at lib/dynamic_queue_limits.c:99! <snip> Internal error: Oops - BUG: 00000000f2000800 [#1] SMP pc : dql_completed+0x238/0x248 lr : dql_completed+0x3c/0x248 Call trace: dql_completed+0x238/0x248 axienet_dma_tx_cb+0xa0/0x170 xilinx_dma_do_tasklet+0xdc/0x290 tasklet_action_common+0xf8/0x11c tasklet_action+0x30/0x3c handle_softirqs+0xf8/0x230 <snip> Start dmaengine after enqueue in dql fixes the crash.	4.7	More Details
CVE-2024-51156	07FLYCMS V1.3.9 was discovered to contain a Cross-Site Request Forgery (CSRF) via the component 'erp.07fly.net:80/admin/SysNotifyUser/del.html?id=93'.	4.7	More Details
CVE-2024-21853	Improper finite state machines (FSMs) in the hardware logic in some 4th and 5th Generation Intel(R) Xeon(R) Processors may allow an authorized user to potentially enable denial of service via local access.	4.7	More Details
CVE-2024-50277	In the Linux kernel, the following vulnerability has been resolved: dm: fix a crash if blk_alloc_disk fails If blk_alloc_disk fails, the variable md->disk is set to an error value. cleanup_mapped_device will see that md->disk is non-NULL and it will attempt to access it, causing a crash on this statement "md->disk->private_data = NULL;".	4.7	More Details
CVE-2024-11214	A vulnerability has been found in SourceCodester Best Employee Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/profile.php. The manipulation of the argument website_image leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher disclosure contains confusing vulnerability classes.	4.7	More Details
CVE-2024-29211	A race condition in Ivanti Secure Access Client before version 22.7R4 allows a local authenticated attacker to modify sensitive configuration files.	4.7	More Details
CVE-2024-53088	In the Linux kernel, the following vulnerability has been resolved: i40e: fix race condition by adding filter's intermediate sync state Fix a race condition in the i40e driver that leads to MAC/VLAN filters becoming corrupted and leaking. Address the issue that occurs under heavy load when multiple threads are concurrently modifying MAC/VLAN filters by setting mac and port VLAN. 1. Thread T0 allocates a filter in i40e_add_filter() within i40e_ndo_set_vf_port_vlan(). 2. Thread T1 concurrently frees the filter in __i40e_del_filter() within i40e_ndo_set_vf_mac(). 3. Subsequently, i40e_service_task() calls i40e_sync_vsi_filters(), which refers to the already freed filter memory, causing corruption. Reproduction steps: 1. Spawn multiple VFs. 2. Apply a concurrent heavy load by running parallel operations to change MAC addresses on the VFs and change port VLANs on the host. 3. Observe errors in dmesg: "Error I40E_AQ_RC_ENOSPC adding RX filters on VF XX, please set promiscuous on manually for VF XX". Exact code for stable reproduction Intel can't open-source now. The fix involves implementing a new intermediate filter state, I40E_FILTER_NEW_SYNC, for the time when a filter is on a tmp_add_list. These filters cannot be deleted from the hash list directly but must be removed using the full process.	4.7	More Details
CVE-2022-20634	A vulnerability in the web-based management interface of Cisco ECE could allow an unauthenticated, remote attacker to redirect a user to an undesired web page. This vulnerability is due to improper input validation of the URL parameters in an HTTP request that is sent to an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to cause the interface to redirect the user to a specific, malicious URL. This type of vulnerability is known as an open redirect and is used in phishing attacks that get users to unknowingly visit malicious sites.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	4.7	More Details
CVE-2024-11213	A vulnerability, which was classified as critical, was found in SourceCodester Best Employee Management System 1.0. This affects an unknown part of the file /admin/edit_role.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-23169	The web interface in RSA NetWitness 11.7.2.0 allows Cross-Site Scripting (XSS) via the Where textbox on the Reports screen during new rule creation.	4.6	More Details
CVE-2024-52517	Nextcloud Server is a self hosted personal cloud system. After storing "Global credentials" on the server, the API returns them and adds them into the frontend again, allowing to read them in plain text when an attacker already has access to an active session of a user. It is recommended that the Nextcloud Server is upgraded to 28.0.11, 29.0.8 or 30.0.1 and Nextcloud Enterprise Server is upgraded to 25.0.13.13, 26.0.13.9, 27.1.11.9, 28.0.11, 29.0.8 or 30.0.1.	4.6	More Details
CVE-2024-52523	Nextcloud Server is a self hosted personal cloud system. After setting up a user or administrator defined external storage with fixed credentials, the API returns them and adds them into the frontend again, allowing to read them in plain text when an attacker already has access to an active session of a user. It is recommended that the Nextcloud Server is upgraded to 28.0.12, 29.0.9 or 30.0.2 and Nextcloud Enterprise Server is upgraded to 25.0.13.14, 26.0.13.10, 27.1.11.10, 28.0.12, 29.0.9 or 30.0.2.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-3538	A vulnerability in a certain REST API endpoint of Cisco Data Center Network Manager (DCNM) Software could allow an authenticated, remote attacker to perform a path traversal attack on an affected device. The vulnerability is due to insufficient path restriction enforcement. An attacker could exploit this vulnerability by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to overwrite or list arbitrary files on the affected device.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	4.6	More Details
CVE-2024-47914	VaeMendis - CWE-352: Cross-Site Request Forgery (CSRF)	4.5	More Details
CVE-2024-34776	Out-of-bounds write in some Intel(R) SGX SDK software may allow an authenticated user to potentially enable escalation of privilege via local access.	4.5	More Details
CVE-2023-20092	Three vulnerabilities in the CLI of Cisco TelePresence CE and RoomOS could allow an authenticated, local attacker to overwrite arbitrary files on the local file system of an affected device. These vulnerabilities are due to improper access controls on files that are on the local file system. An attacker could exploit these vulnerabilities by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. To exploit these vulnerabilities, an attacker would need to have a remote support user account. Note: CVE-2023-20092 does not affect Cisco DX70, DX80, TelePresence MX Series, or TelePresence SX Series devices. Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.	4.4	More Details
CVE-2024-27200	Improper access control in some Intel(R) Granulate(TM) software before version 4.30.1 may allow a authenticated user to potentially enable escalation of privilege via local access.	4.4	More Details
CVE-2023-20093	Three vulnerabilities in the CLI of Cisco TelePresence CE and RoomOS could allow an authenticated, local attacker to overwrite arbitrary files on the local file system of an affected device. These vulnerabilities are due to improper access controls on files that are on the local file system. An attacker could exploit these vulnerabilities by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. To exploit these vulnerabilities, an attacker would need to have a remote support user account. Note: CVE-2023-20092 does not affect Cisco DX70, DX80, TelePresence MX Series, or TelePresence SX Series devices. Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.	4.4	More Details
CVE-2023-20004	Three vulnerabilities in the CLI of Cisco TelePresence CE and RoomOS could allow an authenticated, local attacker to overwrite arbitrary files on the local file system of an affected device. These vulnerabilities are due to improper access controls on files that are on the local file system. An attacker could exploit these vulnerabilities by placing a symbolic link in a specific location on the local file system of an affected device. A successful exploit could allow the attacker to overwrite arbitrary files on the affected device. To exploit these vulnerabilities, an attacker would need to have a remote support user account. Note: CVE-2023-20092 does not affect Cisco DX70, DX80, TelePresence MX Series, or TelePresence SX Series devices. Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.	4.4	More Details
CVE-2024-51330	An issue in UltiMaker Cura v.4.41 and 5.8.1 and before allows a local attacker to execute arbitrary code via Inter-process communication (IPC) mechanism between Cura application and CuraEngine processes, localhost network stack, printing settings and G-code processing and transmission components, Ultimaker 3D Printers.	4.4	More Details
CVE-2024-53052	In the Linux kernel, the following vulnerability has been resolved: io_uring/rw: fix missing NOWAIT check for O_DIRECT start write When io_uring starts a write, it'll call kiocb_start_write() to bump the super block rwsem, preventing any freezes from happening while that write is in-flight. The freeze side will grab that rwsem for writing, excluding any new writers from happening and waiting for existing writes to finish. But io_uring unconditionally uses kiocb_start_write(), which will block if someone is currently attempting to freeze the mount point. This causes a deadlock where freeze is waiting for previous writes to complete, but the previous writes cannot complete, as the task that is supposed to complete them is blocked waiting on starting a new write. This results in the following stuck trace showing that dependency with the write blocked starting a new write: task:fio state:D stack:0 pid:886 tgid:886 ppid:876 Call trace: __switch_to+0x1d8/0x348 __schedule+0x8e8/0x2248 schedule+0x110/0x3f0 percpu_rwsem_wait+0x1e8/0x3f8 __percpu_down_read+0xe8/0x500 io_write+0xbb8/0xff8 io_issue_sqe+0x10c/0x1020 io_submit_sqes+0x614/0x2110 __arm64_sys_io_uring_enter+0x524/0x1038 invoke_syscall+0x74/0x268 el0_svc_common.constprop.0+0x160/0x238 do_el0_svc+0x44/0x60 el0_svc+0x44/0xb0 el0t_64_sync_handler+0x118/0x128 el0t_64_sync+0x168/0x170 INFO: task fsfreeze:7364 blocked for more than 15 seconds. Not tainted 6.12.0-rc5-00063-g76aaf945701c #7963 with the attempting freezer stuck trying to grab the rwsem: task:fsfreeze state:D stack:0 pid:7364 tgid:7364 ppid:995 Call trace: __switch_to+0x1d8/0x348 __schedule+0x8e8/0x2248 schedule+0x110/0x3f0 percpu_down_write+0x2b0/0x680 freeze_super+0x248/0x8a8 do_vfs_ioctl+0x149c/0x1b18 __arm64_sys_ioctl+0xd0/0x1a0 invoke_syscall+0x74/0x268 el0_svc_common.constprop.0+0x160/0x238 do_el0_svc+0x44/0x60 el0_svc+0x44/0xb0 el0t_64_sync_handler+0x118/0x128 el0t_64_sync+0x168/0x170 Fix this by having the io_uring side honor IOCB_NOWAIT, and only attempt a blocking grab of the super block rwsem if it isn't set. For normal issue where IOCB_NOWAIT would always be set, this returns -EAGAIN which will have io_uring core issue a blocking attempt of the write. That will in turn also get completions run, ensuring forward progress. Since freezing requires CAP_SYS_ADMIN in the first place, this isn't something that can be triggered by a regular user.	4.4	More Details
CVE-2024-52518	Nextcloud Server is a self hosted personal cloud system. After an attacker got access to the session of a user or administrator, the attacker would be able to create, change or delete external storages without having to confirm the password. It is recommended that the Nextcloud Server is upgraded to 28.0.12, 29.0.9 or 30.0.2.	4.4	More Details
CVE-2024-52549	Jenkins Script Security Plugin 1367.vdf2fc45f229c and earlier, except 1365.1367.va_3b_b_89f8a_95b_ and 1362.1364.v4cf2dc5d8776, does not perform a permission check in a method implementing form validation, allowing attackers with Overall/Read permission to check for the existence of files on the controller file system.	4.3	More Details
CVE-2024-50652	A file upload vulnerability in java_shop 1.0 allows attackers to upload arbitrary files by modifying the avatar function.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-11243	A vulnerability classified as problematic has been found in code-projects Online Shop Store 1.0. This affects an unknown part of the file /signup.php. The manipulation of the argument m2 with the input <svg%20onload=alert(document.cookie)> 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.	4.3	More Details
CVE-2021-3987	An improper access control vulnerability exists in janeczku/calibre-web. The affected version allows users without public shelf permissions to create public shelves. The vulnerability is due to the `create_shelf` method in `shelf.py` not verifying if the user has the necessary permissions to create a public shelf. This issue can lead to unauthorized actions being performed by users.	4.3	More Details
CVE-2024-3334	A security bypass vulnerability exists in the Removable Media Encryption (RME)component of Digital Guardian Windows Agents prior to version 8.2.0. This allows a user to circumvent encryption controls by modifying metadata on the USB device thereby compromising the confidentiality of the stored data.	4.3	More Details
CVE-2024-10854	The Buy one click WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the buy_one_click_import_options AJAX action in all versions up to, and including, 2.2.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to import plugin settings.	4.3	More Details
CVE-2024-51686	Cross-Site Request Forgery (CSRF) vulnerability in Deepak Khokhar, Surender Khokhar Manage User Columns allows Cross Site Request Forgery.This issue affects Manage User Columns: from n/a through 1.0.5.	4.3	More Details
CVE-2024-33624	Improper input validation for some Intel(R) PROSet/Wireless WiFi software for Windows before version 23.60 may allow an unauthenticated user to potentially enable denial of service via network access.	4.3	More Details
CVE-2024-42390	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and force the application to read unintended heap memory space.	4.3	More Details
CVE-2024-10853	The Buy one click WooCommerce plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the removeorder AJAX action in all versions up to, and including, 2.2.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete Buy one click WooCommerce orders.	4.3	More Details
CVE-2024-10786	The Simple Local Avatars plugin for WordPress is vulnerable to unauthorized modification of datadue to a missing capability check on the sla_clear_user_cache function in all versions up to, and including, 2.7.11. This makes it possible for authenticated attackers, with Subscriber-level access and above, to clear user caches.	4.3	More Details
CVE-2021-3991	An Improper Authorization vulnerability exists in Dolibarr versions prior to the 'develop' branch. A user with restricted permissions in the 'Reception' section is able to access specific reception details via direct URL access, bypassing the intended permission restrictions.	4.3	More Details
CVE-2024-10614	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the cancel_import() function in all versions up to, and including, 5.61.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to cancel and import or check on the status.	4.3	More Details
CVE-2024-48896	A vulnerability was found in Moodle. It is possible for users with the "send message" capability to view other users' names that they may not otherwise have access to via an error message in Messaging. Note: The name returned follows the full name format configured on the site.	4.3	More Details
CVE-2024-40443	SQL Injection vulnerability in Simple Laboratory Management System using PHP and MySQL v.1.0 allows a remote attacker to cause a denial of service via the delete_users function in the Useres.php	4.3	More Details
CVE-2021-3986	A vulnerability in janeczku/calibre-web allows unauthorized users to view the names of private shelves belonging to other users. This issue occurs in the file shelf.py at line 221, where the name of the shelf is exposed in an error message when a user attempts to remove a book from a shelf they do not own. This vulnerability discloses private information and affects all versions prior to the fix.	4.3	More Details
CVE-2021-1481	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct Cypher query language injection attacks on an affected system. This vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to the interface of an affected system. A successful exploit could allow the attacker to obtain sensitive information.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	4.3	More Details
CVE-2024-52420	Cross-Site Request Forgery (CSRF) vulnerability in Creative Motion Disable Admin Notices individually allows Cross Site Request Forgery.This issue affects Disable Admin Notices individually: from n/a through 1.3.5.	4.3	More Details
CVE-2024-10530	The Kognetiks Chatbot for WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the add_new_assistant() function in all versions up to, and including, 2.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to create new GTP assistants.	4.3	More Details
CVE-2021-34750	A vulnerability in the administrative web-based GUI configuration manager of Cisco Firepower Management Center Software could allow an authenticated, remote attacker to access sensitive configuration information. The attacker would require low privilege credentials on an affected device. This vulnerability is due to lack of proper encryption of sensitive information stored within the GUI configuration manager. An attacker could exploit this vulnerability by logging into the FMC GUI and navigating to certain sensitive configurations. A successful exploit could allow the attacker to view sensitive configuration parameters in clear text.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability. [[Publication_URL{Layout()}]]This advisory is part of the October 2021 release of the Cisco ASA, FTD, and FMC Security Advisory Bundled publication. For a complete list of the advisories and links to them, see .	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-34751	A vulnerability in the administrative web-based GUI configuration manager of Cisco Firepower Management Center (FMC) Software could allow an authenticated, remote attacker to access sensitive configuration information. The attacker would require low privilege credentials on an affected device. This vulnerability exists because of improper encryption of sensitive information stored within the GUI configuration manager. An attacker could exploit this vulnerability by logging into the GUI of Cisco FMC Software and navigating to certain sensitive configurations. A successful exploit could allow the attacker to view sensitive configuration parameters in clear text.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.[[Publication_URL{Layout()}]]This advisory is part of the October 2021 release of the Cisco ASA, FTD, and FMC Security Advisory Bundled publication. For a complete list of the advisories and links to them, see .	4.3	More Details
CVE-2024-10852	The Buy one click WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the buy_one_click_export_options AJAX action in all versions up to, and including, 2.2.9. This makes it possible for authenticated attackers, with Subscriber-level access and above, to export plugin settings.	4.3	More Details
CVE-2024-6628	The EleForms – All In One Form Integration including DB for Elementor plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.9.9.9. This is due to missing or incorrect nonce validation when deleting form submissions. This makes it possible for unauthenticated attackers to delete form submissions 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-2024-10533	The WP Chat App plugin for WordPress is vulnerable to unauthorized plugin installation due to a missing capability check on the ajax_install_plugin() function in all versions up to, and including, 3.6.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install the filebird plugin.	4.3	More Details
CVE-2024-10582	The Music Player for Elementor – Audio Player & Podcast Player plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the import_mpfe_template() function in all versions up to, and including, 2.4.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to import templates.	4.3	More Details
CVE-2024-10795	The Popularis Extra plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.2.7 via the 'elementor-template' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created via Elementor that they should not have access to.	4.3	More Details
CVE-2023-20094	A vulnerability in Cisco TelePresence CE and RoomOS could allow an unauthenticated, adjacent attacker to view sensitive information on an affected device. This vulnerability exists because the affected software performs improper bounds checks. An attacker could exploit this vulnerability by sending a crafted request to an affected device. A successful exploit could allow the attacker to cause an out-of-bounds read that discloses sensitive information. Note: This vulnerability only affects Cisco Webex Desk Hub. There are no workarounds that address this vulnerability.	4.3	More Details
CVE-2024-42391	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows an attacker to send an unexpected TLS packet and force the application to read unintended heap memory space.	4.3	More Details
CVE-2024-48897	A vulnerability was found in Moodle. Additional checks are required to ensure users can only edit or delete RSS feeds that they have permission to modify.	4.3	More Details
CVE-2024-52359	IBM Concert Software 1.0.0, 1.0.1, 1.0.2, and 1.0.2.1 could allow an authenticated user to perform unauthorized actions that should be reserved to administrator used due to improper access controls.	4.3	More Details
CVE-2021-1410	A vulnerability in the distribution list feature of Cisco Webex Meetings could allow an authenticated, remote attacker to modify a distribution list that belongs to another user of their organization. The vulnerability is due to insufficient authorization enforcement for requests to update distribution lists. An attacker could exploit this vulnerability by sending a crafted request to the Webex Meetings interface to modify an existing distribution list. A successful exploit could allow the attacker to modify a distribution list that belongs to a user other than themselves.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	4.3	More Details
CVE-2024-11207	A vulnerability has been found in Apereo CAS 6.6 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /login. The manipulation of the argument redirect_uri leads to open redirect. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-43338	Cross-Site Request Forgery (CSRF) vulnerability in Automattic, Inc. Crowdsignal Dashboard – Polls, Surveys & more allows Cross Site Request Forgery.This issue affects Crowdsignal Dashboard – Polls, Surveys & more: from n/a through 3.1.2.	4.3	More Details
CVE-2022-20846	A vulnerability in the Cisco Discovery Protocol implementation for Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause the Cisco Discovery Protocol process to reload on an affected device. This vulnerability is due to a heap buffer overflow in certain Cisco Discovery Protocol messages. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to cause a heap overflow, which could cause the Cisco Discovery Protocol process to reload on the device. The bytes that can be written in the buffer overflow are restricted, which limits remote code execution.Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent). Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.This advisory is part of the September 2022 release of the Cisco IOS XR Software Security Advisory Bundled Publication. For a complete list of the advisories and links to them, see .	4.3	More Details
CVE-2024-51660	Missing Authorization vulnerability in Zakaria Binsaifullah Easy Accordion Gutenberg Block allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Easy Accordion Gutenberg Block: from n/a through 1.2.3.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49680	Missing Authorization vulnerability in Rextheme WP VR allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP VR: from n/a through 8.5.5.	4.3	More Details
CVE-2024-49697	Missing Authorization vulnerability in WP Sunshine Sunshine Photo Cart allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sunshine Photo Cart: from n/a through 3.2.9.	4.3	More Details
CVE-2024-50417	Missing Authorization vulnerability in BoldThemes Bold Page Builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Bold Page Builder: from n/a through 5.1.3.	4.3	More Details
CVE-2022-20939	A vulnerability in the web-based management interface of Cisco Smart Software Manager On-Prem could allow an authenticated, remote attacker to elevate privileges on an affected system. This vulnerability is due to inadequate protection of sensitive user information. An attacker could exploit this vulnerability by accessing certain logs on an affected system. A successful exploit could allow the attacker to use the obtained information to elevate privileges to System Admin.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	4.3	More Details
CVE-2024-10794	The Boostify Header Footer Builder for Elementor plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.3.6 via the 'bhf' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts created via Elementor that they should not have access to.	4.3	More Details
CVE-2024-1682	An unclaimed Amazon S3 bucket, 'codeconf', is referenced in an audio file link within the .rst documentation file. This bucket has been claimed by an external party. The use of this unclaimed S3 bucket could lead to data integrity issues, data leakage, availability problems, loss of trustworthiness, and potential further attacks if the bucket is used to host malicious content or as a pivot point for further attacks.	4.3	More Details
CVE-2024-11143	The Kognetiks Chatbot for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.1.8. This is due to missing or incorrect nonce validation on the update_assistant, add_new_assistant, and delete_assistant functions. This makes it possible for unauthenticated attackers to modify assistants 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-2024-51669	Cross-Site Request Forgery (CSRF) vulnerability in Vivwebs Dynamic Widgets.This issue affects Dynamic Widgets: from n/a through 1.6.4.	4.3	More Details
CVE-2020-3525	A vulnerability in the Admin portal of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to recover service account passwords that are saved on an affected system. The vulnerability is due to the incorrect inclusion of saved passwords when loading configuration pages in the Admin portal. An attacker with read or write access to the Admin portal could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to recover passwords and expose those accounts to further attack.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	4.3	More Details
CVE-2024-10593	The WPForms – Easy Form Builder for WordPress – Contact Forms, Payment Forms, Surveys, & More plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.9.1.6. This is due to missing or incorrect nonce validation on the process_admin_ui function. This makes it possible for unauthenticated attackers to delete WPForm logs 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-2024-11159	Using remote content in OpenPGP encrypted messages can lead to the disclosure of plaintext. This vulnerability affects Thunderbird < 128.4.3 and Thunderbird < 132.0.1.	4.3	More Details
CVE-2024-10897	The Tutor LMS Elementor Addons plugin for WordPress is vulnerable to unauthorized plugin installation due to a missing capability check on the install_etlms_dependency_plugin() function in all versions up to, and including, 2.1.5. This makes it possible for authenticated attackers, with Subscriber-level access and above, to install Elementor or Tutor LMS. Please note the impact of this issue is incredibly limited due to the fact that these two plugins will likely already be installed as a dependency of the plugin.	4.3	More Details
CVE-2024-48900	A vulnerability was found in Moodle. Additional checks are required to ensure users with permission to view badge recipients can only access lists of those they are intended to have access to.	4.3	More Details
CVE-2024-48898	A vulnerability was found in Moodle. Users with access to delete audiences from reports could delete audiences from other reports that they do not have permission to delete from.	4.3	More Details
CVE-2021-1465	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct a directory traversal attack and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to an affected system. A successful exploit could allow the attacker to write arbitrary files on the affected system.	4.3	More Details
CVE-2024-48901	A vulnerability was found in Moodle. Additional checks are required to ensure users can only access the schedule of a report if they have permission to edit that report.	4.3	More Details
CVE-2021-1425	A vulnerability in the web-based management interface of Cisco AsyncOS Software for Cisco Content Security Management Appliance (SMA) could allow an authenticated, remote attacker to access sensitive information on an affected device. The vulnerability exists because confidential information is being included in HTTP requests that are exchanged between the user and the device. An attacker could exploit this vulnerability by looking at the raw HTTP requests that are sent to the interface. A successful exploit could allow the attacker to obtain some of the passwords that are configured throughout the interface.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10778	The BuddyPress Builder for Elementor – BuddyBuilder plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 1.7.4 via the 'elementor-template' shortcode due to insufficient restrictions on which posts can be included. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract data from private or draft posts crated by Elementor that they should not have access to.	4.3	More Details
CVE-2024-37070	IBM Concert Software 1.0.0, 1.0.1, 1.0.2, and 1.0.2.1 could allow an authenticated user to obtain sensitive information that could aid in further attacks against the system.	4.3	More Details
CVE-2024-45420	Uncontrolled resource consumption in some Zoom Apps before version 6.2.0 may allow an authenticated user to conduct a denial of service via network access.	4.3	More Details
CVE-2024-21808	Improper buffer restrictions in some Intel(R) VPL software before version 24.1.4 may allow an authenticated user to potentially enable escalation of privilege via local access.	4.2	More Details
CVE-2024-42383	Use of Out-of-range Pointer Offset vulnerability in Cesanta Mongoose Web Server v7.14 allows to write a NULL byte value beyond the memory space dedicated for the hostname field.	4.2	More Details
CVE-2024-10978	Incorrect privilege assignment in PostgreSQL allows a less-privileged application user to view or change different rows from those intended. An attack requires the application to use SET ROLE, SET SESSION AUTHORIZATION, or an equivalent feature. The problem arises when an application query uses parameters from the attacker or conveys query results to the attacker. If that query reacts to current_setting('role') or the current user ID, it may modify or return data as though the session had not used SET ROLE or SET SESSION AUTHORIZATION. The attacker does not control which incorrect user ID applies. Query text from less-privileged sources is not a concern here, because SET ROLE and SET SESSION AUTHORIZATION are not sandboxes for unvetted queries. Versions before PostgreSQL 17.1, 16.5, 15.9, 14.14, 13.17, and 12.21 are affected.	4.2	More Details
CVE-2024-52510	The Nextcloud Desktop Client is a tool to synchronize files from Nextcloud Server with your computer. The Desktop client did not stop with an error but allowed by-passing the signature validation, if a manipulated server sends an empty initial signature. It is recommended that the Nextcloud Desktop client is upgraded to 3.14.2 or later.	4.2	More Details
CVE-2024-10976	Incomplete tracking in PostgreSQL of tables with row security allows a reused query to view or change different rows from those intended. CVE-2023-2455 and CVE-2016-2193 fixed most interaction between row security and user ID changes. They missed cases where a subquery, WITH query, security invoker view, or SQL-language function references a table with a row-level security policy. This has the same consequences as the two earlier CVEs. That is to say, it leads to potentially incorrect policies being applied in cases where role-specific policies are used and a given query is planned under one role and then executed under other roles. This scenario can happen under security definer functions or when a common user and query is planned initially and then re-used across multiple SET ROLEs. Applying an incorrect policy may permit a user to complete otherwise-forbidden reads and modifications. This affects only databases that have used CREATE POLICY to define a row security policy. An attacker must tailor an attack to a particular application's pattern of query plan reuse, user ID changes, and role-specific row security policies. Versions before PostgreSQL 17.1, 16.5, 15.9, 14.14, 13.17, and 12.21 are affected.	4.2	More Details
CVE-2024-52514	Nextcloud Server is a self hosted personal cloud system. After a user received a share with some files inside being blocked by the files access control, the user would still be able to copy the intermediate folder inside Nextcloud allowing them to afterwards potentially access the blocked files depending on the user access control rules. It is recommended that the Nextcloud Server is upgraded to 27.1.9, 28.0.5 or 29.0.0 and Nextcloud Enterprise Server is upgraded to 21.0.9.18, 22.2.10.23, 23.0.12.18, 24.0.12.14, 25.0.13.9, 26.0.13.3, 27.1.9, 28.0.5 or 29.0.0.	4.1	More Details
CVE-2023-39180	A flaw was found within the handling of SMB2_READ commands in the kernel ksmbd module. The issue results from not releasing memory after its effective lifetime. An attacker can leverage this to create a denial-of-service condition on affected installations of Linux. Authentication is not required to exploit this vulnerability, but only systems with ksmbd enabled are vulnerable.	4.0	More Details
CVE-2023-4458	A flaw was found within the parsing of extended attributes in the kernel ksmbd module. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this to disclose sensitive information on affected installations of Linux. Only systems with ksmbd enabled are vulnerable to this CVE.	4.0	More Details
CVE-2024-42385	Improper Neutralization of Delimiters vulnerability in Cesanta Mongoose Web Server v7.14 allows to trigger an out-of-bound memory write if the PEM certificate contains unexpected characters.	4.0	More Details
CVE-2024-42392	Improper Neutralization of Delimiters vulnerability in Cesanta Mongoose Web Server v7.14 allows to trigger an infinite loop bug if the input string contains unexpected characters.	4.0	More Details
CVE-2024-32485	Improper Input Validation in some Intel(R) VROC software before version 8.6.0.2003 may allow an authenticated user to potentially enable denial of service via local access.	3.9	More Details
CVE-2024-32667	Out-of-bounds read for some OpenCL(TM) software may allow an authenticated user to potentially enable denial of service via local access.	3.9	More Details
CVE-2024-38660	Protection mechanism failure in the SPP for some Intel(R) Xeon(R) processor family (E-Core) may allow an authenticated user to potentially enable escalation of privilege via local access.	3.8	More Details
CVE-2024-5030	The CM Table Of Contents WordPress plugin before 1.2.3 does not have CSRF check in place when resetting its settings, which could allow attackers to make a logged in admin perform such action via a CSRF attack	3.8	More Details
CVE-2024-25565	Insufficient control flow management in UEFI firmware for some Intel(R) Xeon(R) Processors may allow an authenticated user to enable denial of service via local access.	3.8	More Details
CVE-2024-11319	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in django CMS Association django-cms allows Cross-Site Scripting (XSS).This issue affects django-cms: 3.11.7, 3.11.8, 4.1.2, 4.1.3.	3.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42188	HCL Connections is vulnerable to a broken access control vulnerability that may allow an unauthorized user to update data in certain scenarios.	3.7	More Details
CVE-2024-11208	A vulnerability was found in Apereo CAS 6.6 and classified as problematic. Affected by this issue is some unknown functionality of the file /login?service. The manipulation leads to session expiration. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2024-11246	A vulnerability, which was classified as problematic, was found in code-projects Farmacia 1.0. Affected is an unknown function of the file /adicionar-cliente.php. The manipulation of the argument nome/cpf/dataNascimento 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 initial researcher advisory mentions the parameter "nome" to be affected. But further inspection indicates that other parameters might be affected as well.	3.5	More Details
CVE-2024-52507	Nextcloud Tables allows users to to create tables with individual columns. The information which Table (numeric ID) is shared with which groups and users and the respective permissions was not limited to affected users. It is recommended that the Nextcloud Tables app is upgraded to 0.8.1.	3.5	More Details
CVE-2024-11259	A vulnerability, which was classified as problematic, has been found in code-projects Farmacia 1.0. This issue affects some unknown processing of the file /fornecedores.php. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-11240	A vulnerability was found in IBPhoenix ibWebAdmin up to 1.0.2 and classified as problematic. This issue affects some unknown processing of the file /database.php of the component Banco de Dados Tab. The manipulation of the argument db_login_role leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-11175	A vulnerability was found in Public CMS 5.202406.d and classified as problematic. This issue affects some unknown processing of the file /admin/cmsVote/save of the component Voting Management. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The patch is named b9530b9cc1f5cfdad4b637874f59029a6283a65c. It is recommended to apply a patch to fix this issue.	3.5	More Details
CVE-2024-52509	Nextcloud Mail is the mail app for Nextcloud, a self-hosted productivity platform. The Nextcloud mail app incorrectly allowed attaching shared files without download permissions as attachments. This allowed users to send them the files to themselves and then downloading it from their mail clients. It is recommended that the Nextcloud Mail is upgraded to 2.2.10, 3.6.2 or 3.7.2.	3.5	More Details
CVE-2024-11247	A vulnerability has been found in SourceCodester Online Eyewear Shop 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /oews/classes/Master.php?f=save_product of the component Inventory Page. The manipulation of the argument brand leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	3.5	More Details
CVE-2024-33611	Improper input validation for some Intel(R) PROSet/Wireless WiFi software for Windows before version 23.60 may allow a privileged user to potentially enable denial of service via local access.	3.4	More Details
CVE-2024-25563	Improper initialization in firmware for some Intel(R) PROSet/Wireless Software and Intel(R) Killer(TM) Wi-Fi before version 23.40 may allow a privileged user to potentially enable information disclosure via local access.	3.4	More Details
CVE-2023-0657	A flaw was found in Keycloak. This issue occurs due to improperly enforcing token types when validating signatures locally. This could allow an authenticated attacker to exchange a logout token for an access token and possibly gain access to data outside of enforced permissions.	3.4	More Details
CVE-2024-52512	user_oidc app is an OpenID Connect user backend for Nextcloud. A malicious user could send a malformed login link that would redirect the user to a provided URL after successfully authenticating. It is recommended that the Nextcloud User OIDC app is upgraded to 6.1.0.	3.3	More Details
CVE-2024-45099	IBM Security ReaQta 3.12 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	3.1	More Details
CVE-2024-10977	Client use of server error message in PostgreSQL allows a server not trusted under current SSL or GSS settings to furnish arbitrary non-NUL bytes to the libpq application. For example, a man-in-the-middle attacker could send a long error message that a human or screen-scraper user of psql mistakes for valid query results. This is probably not a concern for clients where the user interface unambiguously indicates the boundary between one error message and other text. Versions before PostgreSQL 17.1, 16.5, 15.9, 14.14, 13.17, and 12.21 are affected.	3.1	More Details
CVE-2024-9633	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.3 before 17.4.2, all versions starting from 17.5 before 17.5.4, all versions starting from 17.6 before 17.6.2. This issue allows an attacker to create a group with a name matching an existing unique Pages domain, potentially leading to domain confusion attacks.	3.1	More Details
CVE-2024-52516	Nextcloud Server is a self hosted personal cloud system. When a server is configured to only allow sharing with users that are in ones own groups, after a user was removed from a group, previously shared items were not unshared. It is recommended that the Nextcloud Server is upgraded to 22.2.11 or 23.0.11 or 24.0.6 and Nextcloud Enterprise Server is upgraded to 22.2.11 or 23.0.11 or 24.0.6.	3.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-52519	Nextcloud Server is a self hosted personal cloud system. The OAuth2 client secrets were stored in a recoverable way, so that an attacker that got access to a backup of the database and the Nextcloud config file, would be able to decrypt them. It is recommended that the Nextcloud Server is upgraded to 28.0.10 or 29.0.7 and Nextcloud Enterprise Server is upgraded to 27.1.11.8, 28.0.10 or 29.0.7.	2.7	More Details
CVE-2024-51671	Missing Authorization vulnerability in ThemeIsle Otter - Gutenberg Block allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Otter - Gutenberg Block: from n/a through 3.0.3.	2.7	More Details
CVE-2024-52513	Nextcloud Server is a self hosted personal cloud system. After receiving a "Files drop" or "Password protected" share link a malicious user was able to download attachments that are referenced in Text files without providing the password. It is recommended that the Nextcloud Server is upgraded to 28.0.11, 29.0.8 or 30.0.1 and Nextcloud Enterprise Server is upgraded to 25.0.13.13, 26.0.13.9, 27.1.11.9, 28.0.11, 29.0.8 or 30.0.1.	2.6	More Details
CVE-2024-52521	Nextcloud Server is a self hosted personal cloud system. MD5 hashes were used to check background jobs for their uniqueness. This increased the chances of a background job with arguments falsely being identified as already existing and not be queued for execution. By changing the Hash to SHA256 the probability was heavily decreased. It is recommended that the Nextcloud Server is upgraded to 28.0.10, 29.0.7 or 30.0.0.	2.6	More Details
CVE-2024-46383	Hathway Skyworth Router CM5100-511 v4.1.1.24 was discovered to store sensitive information about USB and Wifi connected devices in plaintext.	2.4	More Details
CVE-2024-28051	Out-of-bounds read in some Intel(R) VPL software before version 24.1.4 may allow an authenticated user to potentially enable information disclosure via local access.	2.2	More Details
CVE-2024-28030	NULL pointer dereference in some Intel(R) VPL software before version 24.1.4 may allow an authenticated user to potentially enable denial of service via local access.	2.2	More Details
CVE-2024-52525	Nextcloud Server is a self hosted personal cloud system. Under certain conditions the password of a user was stored unencrypted in the session data. The session data is encrypted before being saved in the session storage (Redis or disk), but it would allow a malicious process that gains access to the memory of the PHP process, to get access to the cleartext password of the user. It is recommended that the Nextcloud Server is upgraded to 28.0.12, 29.0.9 or 30.0.2.	1.8	More Details
CVE-2021-1491	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to read arbitrary files on the underlying file system of the device. This vulnerability is due to insufficient file scope limiting. An attacker could exploit this vulnerability by creating a specific file reference on the file system and then accessing it through the web-based management interface. A successful exploit could allow the attacker to read arbitrary files from the file system of the underlying operating system.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	N/A	More Details
CVE-2024-34780	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	N/A	More Details
CVE-2024-11165	An information disclosure vulnerability exists in the backup configuration process where the SAS token is not masked in the configuration response. This oversight results in sensitive information leakage within the yb_backup log files, exposing the SAS token in plaintext. The leakage occurs during the backup procedure, leading to potential unauthorized access to resources associated with the SAS token. This issue affects YugabyteDB Anywhere: from 2.20.0.0 before 2.20.7.0, from 2.23.0.0 before 2.23.1.0, from 2024.1.0.0 before 2024.1.3.0.	N/A	More Details
CVE-2024-32847	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	N/A	More Details
CVE-2024-11136	The default TCL Camera application exposes a provider vulnerable to path traversal vulnerability. Malicious application can supply malicious URI path and delete arbitrary files from user’s external storage.	N/A	More Details
CVE-2024-49504	grub2 allowed attackers with access to the grub shell to access files on the encrypted disks.	N/A	More Details
CVE-2024-9472	A null pointer dereference in Palo Alto Networks PAN-OS software on PA-800 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series hardware platforms when Decryption policy is enabled allows an unauthenticated attacker to crash PAN-OS by sending specific traffic through the data plane, resulting in a denial of service (DoS) condition. Repeated attempts to trigger this condition will result in PAN-OS entering maintenance mode. Palo Alto Networks VM-Series, Cloud NGFW, and Prisma Access are not affected. This issue only affects PA-800 Series, PA-3200 Series, PA-5200 Series, and PA-7000 Series running these specific versions of PAN-OS: * 10.2.7-h12 * 10.2.8-h10 * 10.2.9-h9 * 10.2.9-h11 * 10.2.10-h2 * 10.2.10-h3 * 10.2.11 * 10.2.11-h1 * 10.2.11-h2 * 10.2.11-h3 * 11.1.2-h9 * 11.1.2-h12 * 11.1.3-h2 * 11.1.3-h4 * 11.1.3-h6 * 11.2.2 * 11.2.2-h1	N/A	More Details
CVE-2024-5920	A cross-site scripting (XSS) vulnerability in Palo Alto Networks PAN-OS software enables an authenticated read-write Panorama administrator to push a specially crafted configuration to a PAN-OS node. This enables impersonation of a legitimate PAN-OS administrator who can perform restricted actions on the PAN-OS node after the execution of JavaScript in the legitimate PAN-OS administrator's browser.	N/A	More Details
CVE-2024-1271	Rejected reason: This CVE was previously published at https://bugzilla.redhat.com/show_bug.cgi?id=2262978 but later rejected for the following reason: The flaw requires an attacker to have superuser credentials which is a condition that already permits all impacts, hence not constituing a security vulnerability.	N/A	More Details
CVE-2024-5919	A blind XML External Entities (XXE) injection vulnerability in the Palo Alto Networks PAN-OS software enables an authenticated attacker to exfiltrate arbitrary files from firewalls to an attacker controlled server. This attack requires network access to the firewall management interface.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49506	Insecure creation of temporary files allows local users on systems with non-default configurations to cause denial of service or set the encryption key for a filesystem	N/A	More Details
CVE-2024-5918	An improper certificate validation vulnerability in Palo Alto Networks PAN-OS software enables an authorized user with a specially crafted client certificate to connect to an impacted GlobalProtect portal or GlobalProtect gateway as a different legitimate user. This attack is possible only if you "Allow Authentication with User Credentials OR Client Certificate."	N/A	More Details
CVE-2024-34787	Path traversal in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a local unauthenticated attacker to achieve code execution. User interaction is required.	N/A	More Details
CVE-2024-50289	In the Linux kernel, the following vulnerability has been resolved: media: av7110: fix a spectre vulnerability As warned by smatch: drivers/staging/media/av7110/av7110_ca.c:270 dvb_ca_ioctl() warn: potential spectre issue 'av7110->ci_slot' [w] (local cap) There is a spectre-related vulnerability at the code. Fix it.	N/A	More Details
CVE-2021-1462	A vulnerability in the CLI of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to elevate privileges on an affected system. To exploit this vulnerability, an attacker would need to have a valid Administrator account on an affected system. The vulnerability is due to incorrect privilege assignment. An attacker could exploit this vulnerability by logging in to an affected system with an Administrator account and creating a malicious file, which the system would parse at a later time. A successful exploit could allow the attacker to obtain root privileges on the affected system.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	N/A	More Details
CVE-2024-52524	Giskard is an evaluation and testing framework for AI systems. A Remote Code Execution (ReDoS) vulnerability was discovered in Giskard component by the GitHub Security Lab team. When processing datasets with specific text patterns with Giskard detectors, this vulnerability could trigger exponential regex evaluation times, potentially leading to denial of service. Giskard versions prior to 2.15.5 are affected.	N/A	More Details
CVE-2024-11303	The pathname of the root directory to a Restricted Directory ('Path Traversal') vulnerability in Korenix JetPort 5601 allows Path Traversal.This issue affects JetPort 5601: through 1.2.	N/A	More Details
CVE-2024-38649	An out-of-bounds write in IPsec of Ivanti Connect Secure before version 22.7R2.1(Not Applicable to 9.1Rx) allows a remote unauthenticated attacker to cause a denial of service.	N/A	More Details
CVE-2024-9526	There exists a stored XSS Vulnerability in Kubeflow Pipeline View web UI. The Kubeflow Web UI allows to create new pipelines. When creating a new pipeline, it is possible to add a description. The description field allows html tags, which are not filtered properly. Leading to a stored XSS. We recommend upgrading past commit 930c35f1c543998e60e8d648ce93185c9b5dbe8d	N/A	More Details
CVE-2020-3420	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of the affected software. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.There are no workarounds that address this vulnerability.	N/A	More Details
CVE-2024-7124	Improper Neutralization of Input During Web Page Generation vulnerability in DInGO dLibra software in the parameter 'filter' in the endpoint 'indexsearch' allows a Reflected Cross-Site Scripting (XSS). An attacker might trick somebody into using a crafted URL, which will cause a script to be run in user's browser. This issue affects DInGO dLibra software in versions from 6.0 before 6.3.20.	N/A	More Details
CVE-2024-11304	Missing input validation in the SEH Computertechnik utnserver Pro, SEH Computertechnik utnserver ProMAX, SEH Computertechnik INU-100 web-interface allows stored Cross-Site Scripting (XSS). This issue affects utnserver Pro, utnserver ProMAX, INU-100 version 20.1.22 and below.	N/A	More Details
CVE-2024-52528	Budget Control Gateway acts as an entry point for incoming requests and routes them to the appropriate microservices for Budget Control. Budget Control Gateway does not properly validate auth tokens, which allows attackers to bypass intended restrictions. This vulnerability is fixed in 1.5.2.	N/A	More Details
CVE-2024-52302	common-user-management is a robust Spring Boot application featuring user management services designed to control user access dynamically. There is a critical security vulnerability in the application endpoint /api/v1/customer/profile-picture. This endpoint allows file uploads without proper validation or restrictions, enabling attackers to upload malicious files that can lead to Remote Code Execution (RCE).	N/A	More Details
CVE-2024-37400	An out of bounds read in Ivanti Connect Secure before version 22.7R2.3 allows a remote unauthenticated attacker to trigger an infinite loop, causing a denial of service.	N/A	More Details
CVE-2020-3532	A vulnerability in the web-based management interface of Cisco Unified Communications Manager, Cisco Unified Communications Manager Session Management Edition, Cisco Unified Communications Manager IM & Presence Service, and Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information.There are no workarounds that address this vulnerability.	N/A	More Details
CVE-2024-21540	Rejected reason: This issue is not a vulnerability because no real attack scenario can happen.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-52295	DataEase is an open source data visualization analysis tool. Prior to 2.10.2, DataEase allows attackers to forge jwt and take over services. The JWT secret is hardcoded in the code, and the UID and OID are hardcoded. The vulnerability has been fixed in v2.10.2.	N/A	More Details
CVE-2024-47759	GLPI is a free Asset and IT management software package. An technician can upload a SVG containing a malicious script. The script will then be executed when any user will try to see the document contents. Upgrade to 10.0.17.	N/A	More Details
CVE-2024-34784	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	N/A	More Details
CVE-2024-38654	Improper bounds checking in Ivanti Secure Access Client before version 22.7R3 allows a local authenticated attacker with admin privileges to cause a denial of service.	N/A	More Details
CVE-2024-8781	Execution with Unnecessary Privileges, : Improper Protection of Alternate Path vulnerability in TR7 Application Security Platform (ASP) allows Privilege Escalation, -Privilege Abuse.This issue affects Application Security Platform (ASP): v1.4.25.188.	N/A	More Details
CVE-2024-38655	Argument injection in Ivanti Connect Secure before version 22.7R2.1 and 9.1R18.9 and Ivanti Policy Secure before version 22.7R1.1 and 9.1R18.9 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	N/A	More Details
CVE-2021-1285	Multiple Cisco products are affected by a vulnerability in the Ethernet Frame Decoder of the Snort detection engine that could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper handling of error conditions when processing Ethernet frames. An attacker could exploit this vulnerability by sending malicious Ethernet frames through an affected device. A successful exploit could allow the attacker to exhaust disk space on the affected device, which could result in administrators being unable to log in to the device or the device being unable to boot up correctly.Note: Manual intervention is required to recover from this situation. Customers are advised to contact the Cisco Technical Assistance Center (TAC) to help recover a device in this condition.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	N/A	More Details
CVE-2024-10686	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-51689. Reason: This candidate is a reservation duplicate of CVE-2024-51689. Notes: All CVE users should reference CVE-2024-51689 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-5917	A server-side request forgery in PAN-OS software enables an unauthenticated attacker to use the administrative web interface as a proxy, which enables the attacker to view internal network resources not otherwise accessible.	N/A	More Details
CVE-2024-10394	A local user can bypass the OpenAFS PAG (Process Authentication Group) throttling mechanism in Unix clients, allowing the user to create a PAG using an existing id number, effectively joining the PAG and letting the user steal the credentials in that PAG.	N/A	More Details
CVE-2024-9476	A vulnerability in Grafana Labs Grafana OSS and Enterprise allows Privilege Escalation allows users to gain access to resources from other organizations within the same Grafana instance via the Grafana Cloud Migration Assistant.This vulnerability will only affect users who utilize the Organizations feature to isolate resources on their Grafana instance.	N/A	More Details
CVE-2024-7865	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-2414. Reason: This candidate is a reservation duplicate of CVE-2023-2414. Notes: All CVE users should reference CVE-2023-2414 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-32839	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	N/A	More Details
CVE-2024-53054	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-39711	Argument injection in Ivanti Connect Secure before version 22.7R2.1 and 9.1R18.7 and Ivanti Policy Secure before version 22.7R1.1 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	N/A	More Details
CVE-2024-32841	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	N/A	More Details
CVE-2024-51499	MarkUs is a web application for the submission and grading of student assignments. In versions prior to 2.4.8, an arbitrary file write vulnerability accessible via the update_files method of the SubmissionsController allows authenticated users (e.g. students) to write arbitrary files to any location on the web server MarkUs is running on (depending on the permissions of the underlying filesystem). e.g. This can lead to a delayed remote code execution in case an attacker is able to write a Ruby file into the config/initializers/ subfolder of the Ruby on Rails application. MarkUs v2.4.8 has addressed this issue. No known workarounds are available at the application level aside from upgrading.	N/A	More Details
CVE-2024-6413	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-2414. Reason: This candidate is a reservation duplicate of CVE-2023-2414. Notes: All CVE users should reference CVE-2023-2414 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-52304	aiohttp is an asynchronous HTTP client/server framework for asyncio and Python. Prior to version 3.10.11, the Python parser parses newlines in chunk extensions incorrectly which can lead to request smuggling vulnerabilities under certain conditions. If a pure Python version of aiohttp is installed (i.e. without the usual C extensions) or `AIOHTTP_NO_EXTENSIONS` is enabled, then an attacker may be able to execute a request smuggling attack to bypass certain firewalls or proxy protections. Version 3.10.11 fixes the issue.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-52506	Graylog is a free and open log management platform. The reporting functionality in Graylog allows the creation and scheduling of reports which contain dashboard widgets displaying individual log messages or metrics aggregated from fields of multiple log messages. This functionality, as included in Graylog 6.1.0 & 6.1.1, is vulnerable to information leakage triggered by multiple concurrent report rendering requests from authorized users. When multiple report renderings are requested at the same start time, the headless browser instance used to render the PDF will be reused. Depending on the timing, either a check for the browser instance "freshness" hits, resulting in an error instead of the report being returned, or one of the concurrent report rendering requests "wins" and this report is returned for all report rendering requests that do not return an error. This might lead to one user getting the report of a different user, potentially leaking indexed log messages or aggregated data that this user normally has no access to. This problem is fixed in Graylog 6.1.2. There is no known workaround besides disabling the reporting functionality.	N/A	More Details
CVE-2024-50293	In the Linux kernel, the following vulnerability has been resolved: net/smc: do not leave a dangling sk pointer in __smc_create() Thanks to commit 4bbd360a5084 ("socket: Print pf->create() when it does not clear sock->sk on failure."), syzbot found an issue with AF_SMC: smc_create must clear sock->sk on failure, family: 43, type: 1, protocol: 0 WARNING: CPU: 0 PID: 5827 at net/socket.c:1565 __sock_create+0x96f/0xa30 net/socket.c:1563 Modules linked in: CPU: 0 UID: 0 PID: 5827 Comm: syz-executor259 Not tainted 6.12.0-rc6-next-20241106-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024 RIP: 0010:__sock_create+0x96f/0xa30 net/socket.c:1563 Code: 03 00 74 08 4c 89 e7 e8 4f 3b 85 f8 49 8b 34 24 48 c7 c7 40 89 0c 8d 8b 54 24 04 8b 4c 24 0c 44 8b 44 24 08 e8 32 78 db f7 90 <0f> 0b 90 90 e9 d3 fd ff ff 89 e9 80 e1 07 fe c1 38 c1 0f 8c ee f7 RSP: 0018:ffffc90003e4fda0 EFLAGS: 00010246 RAX: 099c6f938c7f4700 RBX: 1ffffffff1a595fd RCX: ffff888034823c00 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: 00000000fffffe9 R08: ffffffff81567052 R09: 1ffff920007c9f50 R10: dfffc0000000000 R11: fffff520007c9f51 R12: ffffffff8d2cafe8 R13: 1ffffffff1a595fe R14: ffffffff9a789c40 R15: ffff8880764298c0 FS: 000055557b518380(0000) GS:ffff8880b8600000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fa62ff43225 CR3: 0000000031628000 CR4: 00000000003526f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> sock_create net/socket.c:1616 [inline] __sys_socket_create net/socket.c:1653 [inline] __sys_socket+0x150/0x3c0 net/socket.c:1700 __do_sys_socket net/socket.c:1714 [inline] __se_sys_socket net/socket.c:1712 [inline] For reference, see commit 2d859aff775d ("Merge branch 'do-not-leave-dangling-sk-pointers-in-pf-create-functions'")	N/A	More Details
CVE-2024-50292	In the Linux kernel, the following vulnerability has been resolved: ASoC: stm32: spdifrx: fix dma channel release in stm32_spdifrx_remove In case of error when requesting ctrl_chan DMA channel, ctrl_chan is not null. So the release of the dma channel leads to the following issue: [4.879000] st,stm32-spdifrx 500d0000.audio-controller: dma_request_slave_channel error -19 [4.888975] Unable to handle kernel NULL pointer dereference at virtual address 000000000000003d [...] [5.096577] Call trace: [5.099099] dma_release_channel+0x24/0x100 [5.103235] stm32_spdifrx_remove+0x24/0x60 [snd_soc_stm32_spdifrx] [5.109494] stm32_spdifrx_probe+0x320/0x4c4 [snd_soc_stm32_spdifrx] To avoid this issue, release channel only if the pointer is valid.	N/A	More Details
CVE-2024-52584	Autolab is a course management service that enables auto-graded programming assignments. There is a vulnerability in version 3.0.1 where CAs can view or edit the grade for any submission ID, even if they are not a CA for the class that has the submission. The endpoints only check that the CAs have the authorization level of a CA in the class in the endpoint, which is not necessarily the class the submission is attached to. Version 3.0.2 contains a patch. No known workarounds are available.	N/A	More Details
CVE-2024-52585	Autolab is a course management service that enables auto-graded programming assignments. There is an HTML injection vulnerability in version 3.0.1 that can affect instructors and CAs on the grade submissions page. The issue is patched in version 3.0.2. One may apply the patch manually by editing line 589 on `gradesheet.js.erb` to take in feedback as text rather than html.	N/A	More Details
CVE-2024-34781	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	N/A	More Details
CVE-2024-50295	In the Linux kernel, the following vulnerability has been resolved: net: arc: fix the device for dma_map_single/dma_unmap_single The ndev->dev and pdev->dev aren't the same device, use ndev->dev.parent which has dma_mask, ndev->dev.parent is just pdev->dev. Or it would cause the following issue: [39.933526] ------------[cut here]------------ [39.938414] WARNING: CPU: 1 PID: 501 at kernel/dma/mapping.c:149 dma_map_page_attrs+0x90/0x1f8	N/A	More Details
CVE-2024-50294	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix missing locking causing hanging calls If a call gets aborted (e.g. because kafs saw a signal) between it being queued for connection and the I/O thread picking up the call, the abort will be prioritised over the connection and it will be removed from local->new_client_calls by rxrpc_disconnect_client_call() without a lock being held. This may cause other calls on the list to disappear if a race occurs. Fix this by taking the client_call_lock when removing a call from whatever list its ->wait_link happens to be on.	N/A	More Details
CVE-2024-37376	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	N/A	More Details
CVE-2024-44756	NUS-M9 ERP Management Software v3.0.0 was discovered to contain a SQL injection vulnerability via the usercode parameter at /UserWH/checkLogin.	N/A	More Details
CVE-2023-4348	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2020-26066	A vulnerability in the web UI of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to gain read and write access to information that is stored on an affected system. The vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by persuading a user to import a crafted XML file with malicious entries. A successful exploit could allow the attacker to read and write files within the affected application.Cisco has released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48962	Improper Control of Generation of Code ('Code Injection'), Cross-Site Request Forgery (CSRF), : Improper Neutralization of Special Elements Used in a Template Engine vulnerability in Apache OFBiz. This issue affects Apache OFBiz: before 18.12.17. Users are recommended to upgrade to version 18.12.17, which fixes the issue.	N/A	More Details
CVE-2024-2552	A command injection vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator to bypass system restrictions in the management plane and delete files on the firewall.	N/A	More Details
CVE-2024-2551	A null pointer dereference vulnerability in Palo Alto Networks PAN-OS software enables an unauthenticated attacker to stop a core system service on the firewall by sending a crafted packet through the data plane that causes a denial of service (DoS) condition. Repeated attempts to trigger this condition result in the firewall entering maintenance mode.	N/A	More Details
CVE-2024-21697	This High severity RCE (Remote Code Execution) vulnerability was introduced in versions 4.2.8 of Sourcetree for Mac and 3.4.19 for Sourcetree for Windows. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.8, allows an unauthenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Sourcetree for Mac and Sourcetree for Windows customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Sourcetree for Mac 4.2: Upgrade to a release greater than or equal to 4.2.9 Sourcetree for Windows 3.4: Upgrade to a release greater than or equal to 3.4.20 See the release notes ([https://www.sourcetreeapp.com/download-archives]). You can download the latest version of Sourcetree for Mac and Sourcetree for Windows from the download center ([https://www.sourcetreeapp.com/download-archives]). This vulnerability was reported via our Penetration Testing program.	N/A	More Details
CVE-2024-2550	A null pointer dereference vulnerability in the GlobalProtect gateway in Palo Alto Networks PAN-OS software enables an unauthenticated attacker to stop the GlobalProtect service on the firewall by sending a specially crafted packet that causes a denial of service (DoS) condition. Repeated attempts to trigger this condition result in the firewall entering maintenance mode.	N/A	More Details
CVE-2024-7787	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ITG Computer Technology vSRM Supplier Relationship Management System allows Reflected XSS, Cross-Site Scripting (XSS).This issue affects vSRM Supplier Relationship Management System: before 28.08.2024.	N/A	More Details
CVE-2024-5082	A Remote Code Execution vulnerability has been discovered in Sonatype Nexus Repository 2. This issue affects Nexus Repository 2 OSS/Pro versions up to and including 2.15.1.	N/A	More Details
CVE-2024-5083	A stored Cross-site Scripting vulnerability has been discovered in Sonatype Nexus Repository 2 This issue affects Nexus Repository 2 OSS/Pro versions up to and including 2.15.1.	N/A	More Details
CVE-2024-39712	Argument injection in Ivanti Connect Secure before version 22.7R2.1 and 9.1R18.7 and Ivanti Policy Secure before version 22.7R1.1 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	N/A	More Details
CVE-2024-10396	An authenticated user can provide a malformed ACL to the fileserver's StoreACL RPC, causing the fileserver to crash, possibly expose uninitialized memory, and possibly store garbage data in the audit log. Malformed ACLs provided in responses to client FetchACL RPCs can cause client processes to crash and possibly expose uninitialized memory into other ACLs stored on the server.	N/A	More Details
CVE-2024-10691	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-9530. Reason: This candidate is a reservation duplicate of CVE-2024-9530. Notes: All CVE users should reference CVE-2024-9530 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-50290	In the Linux kernel, the following vulnerability has been resolved: media: cx24116: prevent overflows on SNR calculus as reported by Coverity, if reading SNR registers fail, a negative number will be returned, causing an underflow when reading SNR registers. Prevent that.	N/A	More Details
CVE-2024-39710	Argument injection in Ivanti Connect Secure before version 22.7R2.1 and 9.1R18.7 and Ivanti Policy Secure before version 22.7R1.1 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	N/A	More Details
CVE-2024-52522	Rclone is a command-line program to sync files and directories to and from different cloud storage providers. Insecure handling of symlinks with --links and --metadata in rclone while copying to local disk allows unprivileged users to indirectly modify ownership and permissions on symlink target files when a superuser or privileged process performs a copy. This vulnerability could enable privilege escalation and unauthorized access to critical system files, compromising system integrity, confidentiality, and availability. This vulnerability is fixed in 1.68.2.	N/A	More Details
CVE-2024-10397	A malicious server can crash the OpenAFS cache manager and other client utilities, and possibly execute arbitrary code.	N/A	More Details
CVE-2024-49379	Umbrel is a home server OS for self-hosting. The login functionality of Umbrel before version 1.2.2 contains a reflected cross-site scripting (XSS) vulnerability in use-auth.tsx. An attacker can specify a malicious redirect query parameter to trigger the vulnerability. If a JavaScript URL is passed to the redirect parameter the attacker provided JavaScript will be executed after the user entered their password and clicked on login. This vulnerability is fixed in 1.2.2.	N/A	More Details
CVE-2024-34782	SQL injection in Ivanti Endpoint Manager before 2024 November Security Update or 2022 SU6 November Security Update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	N/A	More Details