SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 18 September 2024

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-44146	A logic issue was addressed with improved file handling. This issue is fixed in macOS Sequoia 15. An app may be able to break out of its sandbox.	10.0	More Details
CVE-2024-44148	This issue was addressed with improved validation of file attributes. This issue is fixed in macOS Sequoia 15. An app may be able to break out of its sandbox.	10.0	More Details
CVE-2024-8522	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to SQL Injection via the 'c_only_fields' parameter of the /wp-json/learnpress/v1/courses REST API endpoint in all versions up to, and including, 4.2.7 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.	10.0	More Details
CVE-2024-8529	The LearnPress – WordPress LMS Plugin plugin for WordPress is vulnerable to SQL Injection via the 'c_fields' parameter of the /wp-json/lp/v1/courses/archive-course REST API endpoint in all versions up to, and including, 4.2.7 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.	10.0	More Details
CVE-2024-6678	An issue was discovered in GitLab CE/EE affecting all versions starting from 8.14 prior to 17.1.7, starting from 17.2 prior to 17.2.5, and starting from 17.3 prior to 17.3.2, which allows an attacker to trigger a pipeline as an arbitrary user under certain circumstances.	9.9	More Details
CVE-2024-45496	A flaw was found in OpenShift. This issue occurs due to the misuse of elevated privileges in the OpenShift Container Platform's build process. During the build initialization step, the git-clone container is run with a privileged security context, allowing unrestricted access to the node. An attacker with developer-level access can provide a crafted .gitconfig file containing commands executed during the cloning process, leading to arbitrary command execution on the worker node. An attacker running code in a privileged container could escalate their permissions on the node running the container.	9.9	More Details
CVE-2024-45798	arduino-esp32 is an Arduino core for the ESP32, ESP32-S2, ESP32-S3, ESP32-C3, ESP32-C6 and ESP32-H2 microcontrollers. The `arduino-esp32` CI is vulnerable to multiple Poisoned Pipeline Execution (PPE) vulnerabilities. Code injection in `tests_results.yml` workflow (`GHSL-2024-169`) and environment Variable injection (`GHSL-2024-170`). These issue have been addressed but users are advised to verify the contents of the downloaded artifacts.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45697	Certain models of D-Link wireless routers have a hidden functionality where the telnet service is enabled when the WAN port is plugged in. Unauthorized remote attackers can log in and execute OS commands using hard-coded credentials.	9.8	More Details
CVE-2024-8277	The WooCommerce Photo Reviews Premium plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 1.3.13.2. This is due to the plugin not properly validating what user transient is being used in the login() function and not properly verifying the user's identity. This makes it possible for unauthenticated attackers to log in as user that has dismissed an admin notice in the past 30 days, which is often an administrator. Alternatively, a user can log in as any user with any transient that has a valid user_id as the value, though it would be more difficult to exploit this successfully.	9.8	More Details
CVE-2024-44430	SQL Injection vulnerability in Best Free Law Office Management Software-v1.0 allows an attacker to execute arbitrary code and obtain sensitive information via a crafted payload to the kortex_lite/control/register_case.php interface	9.8	More Details
CVE-2024-8039	Improper permission configurationDomain configuration vulnerability of the mobile application (com.afmobi.boomplayer) can lead to account takeover risks.	9.8	More Details
CVE-2024-38812	The vCenter Server contains a heap-overflow vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger this vulnerability by sending a specially crafted network packet potentially leading to remote code execution.	9.8	More Details
CVE-2024-45694	The web service of certain models of D-Link wireless routers contains a Stack-based Buffer Overflow vulnerability, which allows unauthenticated remote attackers to exploit this vulnerability to execute arbitrary code on the device.	9.8	More Details
CVE-2024-45695	The web service of certain models of D-Link wireless routers contains a Stack-based Buffer Overflow vulnerability, which allows unauthenticated remote attackers to exploit this vulnerability to execute arbitrary code on the device.	9.8	More Details
CVE-2024-45698	Certain models of D-Link wireless routers do not properly validate user input in the telnet service, allowing unauthenticated remote attackers to use hard-coded credentials to log into telnet and inject arbitrary OS commands, which can then be executed on the device.	9.8	More Details
CVE-2024-46046	Tenda FH451 v1.0.0.9 has a stack overflow vulnerability located in the RouteStatic function.	9.8	More Details
CVE-2024-22399	Deserialization of Untrusted Data vulnerability in Apache Seata. When developers disable authentication on the Seata-Server and do not use the Seata client SDK dependencies, they may construct uncontrolled serialized malicious requests by directly sending bytecode based on the Seata private protocol. This issue affects Apache Seata: 2.0.0, from 1.0.0 through 1.8.0. Users are recommended to upgrade to version 2.1.0/1.8.1, which fixes the issue.	9.8	More Details
CVE-2024-46451	TOTOLINK AC1200 T8 v4.1.5cu.861_B20230220 has a buffer overflow vulnerability in the setWiFiAclRules function via the desc parameter.	9.8	More Details
CVE-2024-46419	TOTOLINK AC1200 T8 v4.1.5cu.861_B20230220 has a buffer overflow vulnerability in the setWizardCfg function via the ssid5g parameter.	9.8	More Details
CVE-2024-6401	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in SFS Consulting InsureE GL allows SQL Injection.This issue affects InsureE GL: before 4.6.2.	9.8	More Details
CVE-2024-7098	Improper Restriction of XML External Entity Reference vulnerability in SFS Consulting ww.Winsure allows XML Injection.This issue affects ww.Winsure: before 4.6.2.	9.8	More Details
CVE-2024-7104	Improper Control of Generation of Code ('Code Injection') vulnerability in SFS Consulting ww.Winsure allows Code Injection.This issue affects ww.Winsure: before 4.6.2.	9.8	More Details
CVE-2024-44623	An issue in TuomoKu SPx-GC v.1.3.0 and before allows a remote attacker to execute arbitrary code via the child_process.js function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45414	The HTTPD binary in multiple ZTE routers has a stack-based buffer overflow vulnerability in webPrivateDecrypt function. This function is responsible for decrypting RSA encrypted ciphertext, the encrypted data is supplied base64 encoded. The decoded ciphertext is stored on the stack without checking its length. An unauthenticated attacker can get RCE as root by exploiting this vulnerability.	9.8	More Details
CVE-2024-45415	The HTTPD binary in multiple ZTE routers has a stack-based buffer overflow vulnerability in check_data_integrity function. This function is responsible for validating the checksum of data in post request. The checksum is sent encrypted in the request, the function decrypts it and stores the checksum on the stack without validating it. An unauthenticated attacker can get RCE as root by exploiting this vulnerability.	9.8	More Details
CVE-2024-46048	Tenda FH451 v1.0.0.9 has a command injection vulnerability in the formexeCommand function i	9.8	More Details
CVE-2024-46049	Tenda O6 V3.0 firmware V1.0.0.7(2054) contains a stack overflow vulnerability in the formexeCommand function.	9.8	More Details
CVE-2024-46045	Tenda CH22 V1.0.0.6(468) has a stack overflow vulnerability located in the frmL7PlotForm function.	9.8	More Details
CVE-2024-46044	CH22 V1.0.0.6(468) has a stack overflow vulnerability located in the fromqossetting function.	9.8	More Details
CVE-2024-45790	This vulnerability exists in Reedos aiM-Star version 2.0.1 due to missing restrictions for excessive failed authentication attempts on its API based login. A remote attacker could exploit this vulnerability by conducting a brute force attack against legitimate user passwords, which could lead to gain unauthorized access and compromise other user accounts.	9.8	More Details
CVE-2024-6091	A vulnerability in significant-gravitas/autogpt version 0.5.1 allows an attacker to bypass the shell commands denylist settings. The issue arises when the denylist is configured to block specific commands, such as 'whoami' and '/bin/whoami'. An attacker can circumvent this restriction by executing commands with a modified path, such as '/bin/./whoami', which is not recognized by the denylist.	9.8	More Details
CVE-2024-27112	A unauthenticated SQL Injection has been found in the SO Planning tool that occurs when the public view setting is enabled. An attacker could use this vulnerability to gain access to the underlying database. The vulnerability has been remediated in version 1.52.02.	9.8	More Details
CVE-2024-27113	An unauthenticated Insecure Direct Object Reference (IDOR) to the database has been found in the SO Planning tool that occurs when the public view setting is enabled. An attacker could use this vulnerability to gain access to the underlying database by exporting it as a CSV file. The vulnerability has been remediated in version 1.52.02.	9.8	More Details
CVE-2024-27114	A unauthenticated Remote Code Execution (RCE) vulnerability is found in the SO Planning online planning tool. If the public view setting is enabled, a attacker can upload a PHP-file that will be available for execution for a few milliseconds before it is removed, leading to execution of code on the underlying system. The vulnerability has been remediated in version 1.52.02.	9.8	More Details
CVE-2024-27115	A unauthenticated Remote Code Execution (RCE) vulnerability is found in the SO Planning online planning tool. With this vulnerability, an attacker can upload executable files that are moved to a publicly accessible folder before verifying any requirements. This leads to the possibility of execution of code on the underlying system when the file is triggered. The vulnerability has been remediated in version 1.52.02.	9.8	More Details
CVE-2024-44466	COMFAST CF-XR11 V2.7.2 has a command injection vulnerability in function sub_424CB4. Attackers can send POST request messages to /usr/bin/webmgnt and inject commands into parameter iface.	9.8	More Details
CVE-2024-44541	evilnapsis Inventio Lite Versions v4 and before is vulnerable to SQL Injection via the "username" parameter in "/?action=processlogin."	9.8	More Details
CVE-2024-29847	Deserialization of untrusted data in the agent portal of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to achieve remote code execution.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45824	CVE-2024-45824 IMPACT A remote code vulnerability exists in the affected products. The vulnerability occurs when chained with Path Traversal, Command Injection, and XSS Vulnerabilities and allows for full unauthenticated remote code execution. The link in the mitigations section below contains patches to fix this issue.	9.8	More Details
CVE-2024-8695	A remote code execution (RCE) vulnerability via crafted extension description/changelog could be abused by a malicious extension in Docker Desktop before 4.34.2.	9.8	More Details
CVE-2024-8696	A remote code execution (RCE) vulnerability via crafted extension publisher-url/additional-urls could be abused by a malicious extension in Docker Desktop before 4.34.2.	9.8	More Details
CVE-2024-38183	An improper access control vulnerability in GroupMe allows an a unauthenticated attacker to elevate privileges over a network.	9.8	More Details
CVE-2024-7961	A path traversal vulnerability exists in the Rockwell Automation affected product. If exploited, the threat actor could upload arbitrary files to the server that could result in a remote code execution.	9.8	More Details
CVE-2024-6656	Use of Hard-coded Credentials vulnerability in TNB Mobile Solutions Cockpit Software allows Read Sensitive Strings Within an Executable.This issue affects Cockpit Software: before v2.13.	9.8	More Details
CVE-2024-41874	ColdFusion versions 2023.9, 2021.15 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability by providing crafted input to the application, which when deserialized, leads to execution of malicious code. Exploitation of this issue does not require user interaction.	9.8	More Details
CVE-2024-43978	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in highwarden Super Store Finder allows SQL Injection.This issue affects Super Store Finder: from n/a before 6.9.8.	9.3	More Details
CVE-2024-43976	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in highwarden Super Store Finder allows SQL Injection.This issue affects Super Store Finder: from n/a through 6.9.7.	9.3	More Details
CVE-2024-44004	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPTaskForce WPCargo Track & Trace allows SQL Injection.This issue affects WPCargo Track & Trace: from n/a through 7.0.6.	9.3	More Details
CVE-2024-46958	In Nextcloud Desktop Client 3.13.1 through 3.13.3 on Linux, synchronized files (between the server and client) may become world writable or world readable. This is fixed in 3.13.4.	9.1	More Details
CVE-2024-7387	A flaw was found in openshift/builder. This vulnerability allows command injection via path traversal, where a malicious user can execute arbitrary commands on the OpenShift node running the builder container. When using the “Docker” strategy, executable files inside the privileged build container can be overridden using the `spec.source.secrets.secret.destinationDir` attribute of the `BuildConfig` definition. An attacker running code in a privileged container could escalate their permissions on the node running the container.	9.1	More Details
CVE-2024-8669	The Backuply – Backup, Restore, Migrate and Clone plugin for WordPress is vulnerable to SQL Injection via the 'options' parameter passed to the backuply_wp_clone_sql() function in all versions up to, and including, 1.3.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.1	More Details
CVE-2024-7960	The Rockwell Automation affected product contains a vulnerability that allows a threat actor to view sensitive information and change settings. The vulnerability exists due to having an incorrect privilege matrix that allows users to have access to functions they should not.	9.1	More Details
CVE-2024-40457	No-IP Dynamic Update Client (DUC) v3.x uses cleartext credentials that may occur on a command line or in a file. NOTE: the vendor's position is that cleartext in /etc/default/noip-duc is recommended and is the intentional behavior.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8956	PTZOptics PT30X-SDI/NDI-xx before firmware 6.3.40 is vulnerable to an insufficient authentication issue. The camera does not properly enforce authentication to /cgi-bin/param.cgi when requests are sent without an HTTP Authorization header. The result is a remote and unauthenticated attacker can leak sensitive data such as usernames, password hashes, and configurations details. Additionally, the attacker can update individual configuration values or overwrite the whole file.	9.1	More Details
CVE-2019-25212	The video carousel slider with lightbox plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 1.0.6 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.	9.1	More Details
CVE-2024-28991	SolarWinds Access Rights Manager (ARM) was found to be susceptible to a remote code execution vulnerability. If exploited, this vulnerability would allow an authenticated user to abuse the service, resulting in remote code execution.	9.0	More Details
CVE-2024-45856	A cross-site scripting (XSS) vulnerability exists in all versions of the MindsDB platform, enabling the execution of a JavaScript payload whenever a user enumerates an ML Engine, database, project, or dataset containing arbitrary JavaScript code within the web UI.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-44570	RELY-PCIe v22.2.1 to v23.1.0 was discovered to contain a code injection vulnerability via the getParams function in phpinf.php.	8.8	More Details
CVE-2024-45852	Deserialization of untrusted data can occur in versions 23.3.2.0 and newer of the MindsDB platform, enabling a maliciously uploaded model to run arbitrary code on the server when interacted with.	8.8	More Details
CVE-2024-8905	Inappropriate implementation in V8 in Google Chrome prior to 129.0.6668.58 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-45850	An arbitrary code execution vulnerability exists in versions 23.10.5.0 up to 24.7.4.1 of the MindsDB platform, when the Microsoft SharePoint integration is installed on the server. For databases created with the SharePoint engine, an ‘INSERT’ query can be used for site column creation. If such a query is specially crafted to contain Python code and is run against the database, the code will be passed to an eval function and executed on the server.	8.8	More Details
CVE-2024-22303	Incorrect Privilege Assignment vulnerability in favethemes Houzez allows Privilege Escalation.This issue affects Houzez: from n/a through 3.2.4.	8.8	More Details
CVE-2024-45849	An arbitrary code execution vulnerability exists in versions 23.10.5.0 up to 24.7.4.1 of the MindsDB platform, when the Microsoft SharePoint integration is installed on the server. For databases created with the SharePoint engine, an ‘INSERT’ query can be used for list creation. If such a query is specially crafted to contain Python code and is run against the database, the code will be passed to an eval function and executed on the server.	8.8	More Details
CVE-2024-45848	An arbitrary code execution vulnerability exists in versions 23.12.4.0 up to 24.7.4.1 of the MindsDB platform, when the ChromaDB integration is installed on the server. If a specially crafted ‘INSERT’ query containing Python code is run against a database created with the ChromaDB engine, the code will be passed to an eval function and executed on the server.	8.8	More Details
CVE-2024-45847	An arbitrary code execution vulnerability exists in versions 23.11.4.2 up to 24.7.4.1 of the MindsDB platform, when one of several integrations is installed on the server. If a specially crafted ‘UPDATE’ query containing Python code is run against a database created with the specified integration engine, the code will be passed to an eval function and executed on the server.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8636	Heap buffer overflow in Skia in Google Chrome prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-8637	Use after free in Media Router in Google Chrome on Android prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-8638	Type Confusion in V8 in Google Chrome prior to 128.0.6613.137 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-8639	Use after free in Autofill in Google Chrome on Android prior to 128.0.6613.137 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-45846	An arbitrary code execution vulnerability exists in versions 23.10.3.0 up to 24.7.4.1 of the MindsDB platform, when the Weaviate integration is installed on the server. If a specially crafted ‘SELECT WHERE’ clause containing Python code is run against a database created with the Weaviate engine, the code will be passed to an eval function and executed on the server.	8.8	More Details
CVE-2024-44571	RELY-PCIe v22.2.1 to v23.1.0 was discovered to contain incorrect access control in the mService function at phpinf.php.	8.8	More Details
CVE-2024-46085	FrogCMS V0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/plugin/file_manager/rename	8.8	More Details
CVE-2024-45696	Certain models of D-Link wireless routers contain hidden functionality. By sending specific packets to the web service, the attacker can forcibly enable the telnet service and log in using hard-coded credentials. The telnet service enabled through this method can only be accessed from within the same local network as the device.	8.8	More Details
CVE-2024-8749	SQL injection vulnerability in idoit pro version 28. This vulnerability could allow an attacker to send a specially crafted query to the ID parameter in /var/www/html/src/classes/modules/api/model/cmdb/isys_api_model_cmdb_objects_by_relation.class.php and retrieve all the information stored in the database.	8.8	More Details
CVE-2024-46362	FrogCMS V0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/plugin/file_manager/create_directory	8.8	More Details
CVE-2024-45682	There is a command injection vulnerability that may allow an attacker to inject malicious input on the device's operating system.	8.8	More Details
CVE-2024-45368	The H2-DM1E PLC's authentication protocol appears to utilize either a custom encoding scheme or a challenge-response protocol. However, there's an observed anomaly in the H2-DM1E PLC's protocol execution, namely its acceptance of multiple distinct packets as valid authentication responses. This behavior deviates from standard security practices where a single, specific response or encoding pattern is expected for successful authentication.	8.8	More Details
CVE-2024-43099	The session hijacking attack targets the application layer's control mechanism, which manages authenticated sessions between a host PC and a PLC. During such sessions, a session key is utilized to maintain security. However, if an attacker captures this session key, they can inject traffic into an ongoing authenticated session. To successfully achieve this, the attacker also needs to spoof both the IP address and MAC address of the originating host which is typical of a session-based attack.	8.8	More Details
CVE-2024-21743	Privilege Escalation vulnerability in favethemes Houzez Login Register houzez-login-register.This issue affects Houzez Login Register: from n/a through 3.2.5.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44132	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sequoia 15. An app may be able to break out of its sandbox.	8.8	More Details
CVE-2024-45851	An arbitrary code execution vulnerability exists in versions 23.10.5.0 up to 24.7.4.1 of the MindsDB platform, when the Microsoft SharePoint integration is installed on the server. For databases created with the SharePoint engine, an ‘INSERT’ query can be used for list item creation. If such a query is specially crafted to contain Python code and is run against the database, the code will be passed to an eval function and executed on the server.	8.8	More Details
CVE-2024-8904	Type Confusion in V8 in Google Chrome prior to 129.0.6668.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-6482	The Login with phone number plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.7.49. This is due to a lack of validation and missing capability check on user-supplied data in the 'lwp_update_password_action' function. This makes it possible for authenticated attackers, with Subscriber-level access and above, to update their role to any other role, including Administrator. The vulnerability was partially patched in version 1.7.40. The login with phone number pro plugin was required to exploit the vulnerability in versions 1.7.40 - 1.7.49.	8.8	More Details
CVE-2024-7423	The Stream plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.0.1. This is due to missing or incorrect nonce validation on the network_options_action() function. This makes it possible for unauthenticated attackers to update arbitrary options that can lead to DoS or privilege escalation via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2024-8779	OMFLOW from The SYSCOM Group does not properly restrict access to the system settings modification functionality, allowing remote attackers with regular privileges to update system settings or create accounts with administrator privileges, thereby gaining control of the server.	8.8	More Details
CVE-2024-20381	A vulnerability in the JSON-RPC API feature in Cisco Crosswork Network Services Orchestrator (NSO) and ConfD that is used by the web-based management interfaces of Cisco Optical Site Manager and Cisco RV340 Dual WAN Gigabit VPN Routers could allow an authenticated, remote attacker to modify the configuration of an affected application or device. This vulnerability is due to improper authorization checks on the API. An attacker with privileges sufficient to access the affected application or device could exploit this vulnerability by sending malicious requests to the JSON-RPC API. A successful exploit could allow the attacker to make unauthorized modifications to the configuration of the affected application or device, including creating new user accounts or elevating their own privileges on an affected system.	8.8	More Details
CVE-2024-8246	The Post Form – Registration Form – Profile Form for User Profiles – Frontend Content Forms for User Submissions (UGC) plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 2.8.11. This is due to plugin not properly restricting what users have access to set the default role on registration forms. This makes it possible for authenticated attackers, with contributor-level access and above, to create a registration form with a custom role that allows them to register as administrators.	8.8	More Details
CVE-2024-8533	A privilege escalation vulnerability exists in the Rockwell Automation affected products. The vulnerability occurs due to improper default file permissions allowing users to exfiltrate credentials and escalate privileges.	8.8	More Details
CVE-2024-44574	RELY-PCIe v22.2.1 to v23.1.0 was discovered to contain a command injection vulnerability via the sys_conf function.	8.8	More Details
CVE-2024-8253	The Post Grid and Gutenberg Blocks plugin for WordPress is vulnerable to privilege escalation in all versions 2.2.87 to 2.2.90. This is due to the plugin not properly restricting what user meta values can be updated and ensuring a form is active. This makes it possible for authenticated attackers, with subscriber-level access and above, to update their user meta to become an administrator.	8.8	More Details
CVE-2024-44577	RELY-PCIe v22.2.1 to v23.1.0 was discovered to contain a command injection vulnerability via the time_date function.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20398	A vulnerability in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to obtain read/write file system access on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of user arguments that are passed to specific CLI commands. An attacker with a low-privileged account could exploit this vulnerability by using crafted commands at the prompt. A successful exploit could allow the attacker to elevate privileges to root.	8.8	More Details
CVE-2024-8490	The PropertyHive plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.0.19. This is due to missing or incorrect nonce validation on the 'save_account_details' function. This makes it possible for unauthenticated attackers to edit the name, email address, and password of an administrator account via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2024-44572	RELY-PCIe v22.2.1 to v23.1.0 was discovered to contain a command injection vulnerability via the sys_mgmt function.	8.8	More Details
CVE-2024-20304	A vulnerability in the multicast traceroute version 2 (Mtrace2) feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to exhaust the UDP packet memory of an affected device. This vulnerability exists because the Mtrace2 code does not properly handle packet memory. An attacker could exploit this vulnerability by sending crafted packets to an affected device. A successful exploit could allow the attacker to exhaust the incoming UDP packet memory. The affected device would not be able to process higher-level UDP-based protocols packets, possibly causing a denial of service (DoS) condition. Note: This vulnerability can be exploited using IPv4 or IPv6.	8.6	More Details
CVE-2024-28981	Hitachi Vantara Pentaho Data Integration & Analytics versions before 10.1.0.0 and 9.3.0.8, including 8.3.x, discloses database passwords when searching metadata injectable fields.	8.5	More Details
CVE-2024-8640	An issue has been discovered in GitLab EE affecting all versions starting from 16.11 prior to 17.1.7, from 17.2 prior to 17.2.5, and from 17.3 prior to 17.3.2. Due to incomplete input filtering, it was possible to inject commands into a connected Cube server.	8.5	More Details
CVE-2024-6658	Improper Input Validation vulnerability of Authenticated User in Progress LoadMaster allows OS Command Injection.This issue affects: Product Affected Versions LoadMaster From 7.2.55.0 to 7.2.60.0 (inclusive) From 7.2.49.0 to 7.2.54.11 (inclusive) 7.2.48.12 and all prior versions Multi-Tenant Hypervisor 7.1.35.11 and all prior versions ECS All prior versions to 7.2.60.0 (inclusive)	8.4	More Details
CVE-2024-20489	A vulnerability in the storage method of the PON Controller configuration file could allow an authenticated, local attacker with low privileges to obtain the MongoDB credentials. This vulnerability is due to improper storage of the unencrypted database credentials on the device that is running Cisco IOS XR Software. An attacker could exploit this vulnerability by accessing the configuration files on an affected system. A successful exploit could allow the attacker to view MongoDB credentials.	8.4	More Details
CVE-2024-45398	Contao is an Open Source CMS. In affected versions a back end user with access to the file manager can upload malicious files and execute them on the server. Users are advised to update to Contao 4.13.49, 5.3.15 or 5.4.3. Users unable to update are advised to configure their web server so it does not execute PHP files and other scripts in the Contao file upload directory.	8.3	More Details
CVE-2023-42772	Untrusted pointer dereference in UEFI firmware for some Intel(R) reference processors may allow a privileged user to potentially enable escalation of privilege via local access.	8.2	More Details
CVE-2024-47049	The czim/file-handling package before 1.5.0 and 2.x before 2.3.0 (used with PHP Composer) does not properly validate URLs within makeFromUrl and makeFromAny, leading to SSRF, and to directory traversal for the reading of local files.	8.2	More Details
CVE-2024-37397	An External XML Entity (XXE) vulnerability in the provisioning web service of Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote unauthenticated attacker to leak API secrets.	8.2	More Details
CVE-2024-5754	BT: Encryption procedure host vulnerability	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21529	Versions of the package dset before 3.1.4 are vulnerable to Prototype Pollution via the dset function due improper user input sanitization. This vulnerability allows the attacker to inject malicious object property using the built-in Object property __proto__, which is recursively assigned to all the objects in the program.	8.2	More Details
CVE-2024-43460	Improper authorization in Dynamics 365 Business Central resulted in a vulnerability that allows an authenticated attacker to elevate privileges over a network.	8.1	More Details
CVE-2024-8642	In Eclipse Dataspace Components, from version 0.5.0 and before version 0.9.0, the ConsumerPullTransferTokenValidationApiController does not check for token validity (expiry, not-before, issuance date), which can allow an attacker to bypass the check for token expiration. The issue requires to have a dataplane configured to support http proxy consumer pull AND include the module "transfer-data-plane". The affected code was marked deprecated from the version 0.6.0 in favour of Dataplane Signaling. In 0.9.0 the vulnerable code has been removed.	8.1	More Details
CVE-2024-45413	The HTTPD binary in multiple ZTE routers has a stack-based buffer overflow vulnerability in rsa_decrypt function. This function is an API wrapper for LUA to decrypt RSA encrypted ciphertext, the decrypted data is stored on the stack without checking its length. An authenticated attacker can get RCE as root by exploiting this vulnerability.	8.1	More Details
CVE-2024-45416	The HTTPD binary in multiple ZTE routers has a local file inclusion vulnerability in session_init function. The session -LUA- files are stored in the directory /var/lua_session, the function iterates on all files in this directory and executes them using the function dofile without any validation if it is a valid session file or not. An attacker who is able to write a malicious file in the sessions directory can get RCE as root.	8.1	More Details
CVE-2024-45823	CVE-2024-45823 IMPACT An authentication bypass vulnerability exists in the affected product. The vulnerability exists due to shared secrets across accounts and could allow a threat actor to impersonate a user if the threat actor is able to enumerate additional information required during authentication.	8.1	More Details
CVE-2024-6862	A Cross-Site Request Forgery (CSRF) vulnerability exists in lunary-ai/lunary version 1.2.34 due to overly permissive CORS settings. This vulnerability allows an attacker to sign up for and create projects or use the instance as if they were a user with local access. The main attack vector is for instances hosted locally on personal machines, which are not publicly accessible. The CORS settings in the backend permit all origins, exposing unauthenticated endpoints to CSRF attacks.	8.1	More Details
CVE-2021-27916	Prior to the patched version, logged in users of Mautic are vulnerable to Relative Path Traversal/Arbitrary File Deletion. Regardless of the level of access the Mautic user had, they could delete files other than those in the media folders such as system files, libraries or other important files. This vulnerability exists in the implementation of the GrapesJS builder in Mautic.	8.1	More Details
CVE-2024-7626	The WP Delicious – Recipe Plugin for Food Bloggers (formerly Delicious Recipes) plugin for WordPress is vulnerable to arbitrary file movement and reading due to insufficient file path validation in the save_edit_profile_details() function in all versions up to, and including, 1.6.9. This makes it possible for authenticated attackers, with subscriber-level access and above, to move arbitrary files on the server, which can easily lead to remote code execution when the right file is moved (such as wp-config.php). This can also lead to the reading of arbitrary files that may contain sensitive information like wp-config.php.	8.1	More Details
CVE-2024-43690	Inclusion of Functionality from Untrusted Control Sphere(CWE-829) in the Command Centre Server and Workstations may allow an attacker to perform Remote Code Execution (RCE). This issue affects: Command Centre Server and Command Centre Workstations 9.10 prior to vEL9.10.1530 (MR2), 9.00 prior to vEL9.00.2168 (MR4), 8.90 prior to vEL8.90.2155 (MR5), 8.80 prior to vEL8.80.1938 (MR6), all versions of 8.70 and prior.	8.0	More Details
CVE-2024-23599	Race condition in Seamless Firmware Updates for some Intel(R) reference platforms may allow a privileged user to potentially enable denial of service via local access.	7.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44162	This issue was addressed by enabling hardened runtime. This issue is fixed in Xcode 16. A malicious application may gain access to a user's Keychain items.	7.8	More Details
CVE-2024-39377	Media Encoder versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-31336	In PVRSRVBridgeRGXKickTA3D2 of server_rgxta3d_bridge.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-2024-39380	After Effects versions 23.6.6, 24.5 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-29779	there is a possible escalation of privilege due to an unusual root cause. 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-2024-46687	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix a use-after-free when hitting errors inside btrfs_submit_chunk() [BUG] There is an internal report that KASAN is reporting use-after-free, with the following backtrace: BUG: KASAN: slab-use-after-free in btrfs_check_read_bio+0xa68/0xb70 [btrfs] Read of size 4 at addr ffff8881117cec28 by task kworker/u16:2/45 CPU: 1 UID: 0 PID: 45 Comm: kworker/u16:2 Not tainted 6.11.0-rc2-next-20240805-default+ #76 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.2-3-gd478f380-rebuilt.opensuse.org 04/01/2014 Workqueue: btrfs-endio btrfs_end_bio_work [btrfs] Call Trace: dump_stack_lvl+0x61/0x80 print_address_description.constprop.0+0x5e/0x2f0 print_report+0x118/0x216 kasan_report+0x11d/0x1f0 btrfs_check_read_bio+0xa68/0xb70 [btrfs] process_one_work+0xce0/0x12a0 worker_thread+0x717/0x1250 kthread+0x2e3/0x3c0 ret_from_fork+0x2d/0x70 ret_from_fork_asm+0x11/0x20 Allocated by task 20917: kasan_save_stack+0x37/0x60 kasan_save_track+0x10/0x30 __kasan_slab_alloc+0x7d/0x80 kmem_cache_alloc_noprof+0x16e/0x3e0 mempool_alloc_noprof+0x12e/0x310 bio_alloc_bioset+0x3f0/0x7a0 btrfs_bio_alloc+0x2e/0x50 [btrfs] submit_extent_page+0x4d1/0xdb0 [btrfs] btrfs_do_readpage+0x8b4/0x12a0 [btrfs] btrfs_readahead+0x29a/0x430 [btrfs] read_pages+0x1a7/0xc60 page_cache_ra_unbounded+0x2ad/0x560 filemap_get_pages+0x629/0xa20 filemap_read+0x335/0xbf0 vfs_read+0x790/0xcb0 ksys_read+0xfd/0x1d0 do_syscall_64+0x6d/0x140 entry_SYSCALL_64_after_hwframe+0x4b/0x53 Freed by task 20917: kasan_save_stack+0x37/0x60 kasan_save_track+0x10/0x30 kasan_save_free_info+0x37/0x50 __kasan_slab_free+0x4b/0x60 kmem_cache_free+0x214/0x5d0 bio_free+0xed/0x180 end_bbio_data_read+0x1cc/0x580 [btrfs] btrfs_submit_chunk+0x98d/0x1880 [btrfs] btrfs_submit_bio+0x33/0x70 [btrfs] submit_one_bio+0xd4/0x130 [btrfs] submit_extent_page+0x3ea/0xdb0 [btrfs] btrfs_do_readpage+0x8b4/0x12a0 [btrfs] btrfs_readahead+0x29a/0x430 [btrfs] read_pages+0x1a7/0xc60 page_cache_ra_unbounded+0x2ad/0x560 filemap_get_pages+0x629/0xa20 filemap_read+0x335/0xbf0 vfs_read+0x790/0xcb0 ksys_read+0xfd/0x1d0 do_syscall_64+0x6d/0x140 entry_SYSCALL_64_after_hwframe+0x4b/0x53 [CAUSE] Although I cannot reproduce the error, the report itself is good enough to pin down the cause. The call trace is the regular endio workqueue context, but the free-by-task trace is showing that during btrfs_submit_chunk() we already hit a critical error, and is calling btrfs_bio_end_io() to error out. And the original endio function called bio_put() to free the whole bio. This means a double freeing thus causing use-after-free, e.g.: 1. Enter btrfs_submit_bio() with a read bio The read bio length is 128K, crossing two 64K stripes. 2. The first run of btrfs_submit_chunk() 2.1 Call btrfs_map_block(), which returns 64K 2.2 Call btrfs_split_bio() Now there are two bios, one referring to the first 64K, the other referring to the second 64K. 2.3 The first half is submitted. 3. The second run of btrfs_submit_chunk() 3.1 Call btrfs_map_block(), which by somehow failed Now we call btrfs_bio_end_io() to handle the error 3.2 btrfs_bio_end_io() calls the original endio function Which is end_bbio_data_read(), and it calls bio_put() for the original bio. Now the original bio is freed. 4. The submitted first 64K bio finished Now we call into btrfs_check_read_bio() and tries to advance the bio iter. But since the original bio (thus its iter) is already freed, we trigger the above use-after free. And even if the memory is not poisoned/corrupted, we will later call the original endio function, causing a double freeing. [FIX] Instead of calling btrfs_bio_end_io(), call btrfs_orig_bbio_end_io(), which has the extra check on split bios and do the pr ---truncated---	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46674	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: st: fix probed platform device ref count on probe error path The probe function never performs any paltform device allocation, thus error path "undo_platform_dev_alloc" is entirely bogus. It drops the reference count from the platform device being probed. If error path is triggered, this will lead to unbalanced device reference counts and premature release of device resources, thus possible use-after-free when releasing remaining devm-managed resources.	7.8	More Details
CVE-2024-46673	In the Linux kernel, the following vulnerability has been resolved: scsi: aacraid: Fix double-free on probe failure aac_probe_one() calls hardware-specific init functions through the aac_driver_ident::init pointer, all of which eventually call down to aac_init_adapter(). If aac_init_adapter() fails after allocating memory for aac_dev::queues, it frees the memory but does not clear that member. After the hardware-specific init function returns an error, aac_probe_one() goes down an error path that frees the memory pointed to by aac_dev::queues, resulting.in a double-free.	7.8	More Details
CVE-2024-44093	In ppmp_unprotect_buf of drm/code/drm_fw.c, there is a possible memory corruption 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-2024-44094	In ppmp_protect_mfcfw_buf of code/drm_fw.c, there is a possible memory corruption due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-44095	In ppmp_protect_mfcfw_buf of code/drm_fw.c, there is a possible corrupt memory 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-2024-45181	An issue was discovered in WibuKey64.sys in WIBU-SYSTEMS WibuKey before v6.70 and fixed in v.6.70. An improper bounds check allows crafted packets to cause an arbitrary address write, resulting in kernel memory corruption.	7.8	More Details
CVE-2024-46683	In the Linux kernel, the following vulnerability has been resolved: drm/xe: prevent UAF around preempt fence The fence lock is part of the queue, therefore in the current design anything locking the fence should then also hold a ref to the queue to prevent the queue from being freed. However, currently it looks like we signal the fence and then drop the queue ref, but if something is waiting on the fence, the waiter is kicked to wake up at some later point, where upon waking up it first grabs the lock before checking the fence state. But if we have already dropped the queue ref, then the lock might already be freed as part of the queue, leading to uaf. To prevent this, move the fence lock into the fence itself so we don't run into lifetime issues. Alternative might be to have device level lock, or only release the queue in the fence release callback, however that might require pushing to another worker to avoid locking issues. References: https://gitlab.freedesktop.org/drm/xe/kernel/-/issues/2454 References: https://gitlab.freedesktop.org/drm/xe/kernel/-/issues/2342 References: https://gitlab.freedesktop.org/drm/xe/kernel/-/issues/2020 (cherry picked from commit 7116c35aacedc38be6d15bd21b2fc936eed0008b)	7.8	More Details
CVE-2024-6510	Local Privilege Escalation in AVG Internet Security v24 on Windows allows a local unprivileged user to escalate privileges to SYSTEM via COM-Hijacking.	7.8	More Details
CVE-2024-42025	A Command Injection vulnerability found in a Self-Hosted UniFi Network Servers (Linux) with UniFi Network Application (Version 8.3.32 and earlier) allows a malicious actor with unifi user shell access to escalate privileges to root on the host device.	7.8	More Details
CVE-2024-46696	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix potential UAF in nfsd4_cb_getattr_release Once we drop the delegation reference, the fields embedded in it are no longer safe to access. Do that last.	7.8	More Details
CVE-2024-45857	Deserialization of untrusted data can occur in versions 2.4.0 or newer of the Cleanlab project, enabling a maliciously crafted datalab.pkl file to run arbitrary code on an end user's system when the data directory is loaded.	7.8	More Details
CVE-2024-27320	An arbitrary code execution vulnerability exists in versions 0.0.8 and newer of the Refuel Autolabel library because of the way its classification tasks handle provided CSV files. If a victim user creates a classification task using a maliciously crafted CSV file containing Python code, the code will be passed to an eval function which executes it.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46699	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Disable preemption while updating GPU stats We forgot to disable preemption around the write_seqcount_begin/end() pair while updating GPU stats: [ ] WARNING: CPU: 2 PID: 12 at include/linux/seqlock.h:221 __seqprop_assert.isra.0+0x128/0x150 [v3d] [ ] Workqueue: v3d_bin drm_sched_run_job_work [gpu_sched] <...snip...> [ ] Call trace: [ ] __seqprop_assert.isra.0+0x128/0x150 [v3d] [ ] v3d_job_start_stats.isra.0+0x90/0x218 [v3d] [ ] v3d_bin_job_run+0x23c/0x388 [v3d] [ ] drm_sched_run_job_work+0x520/0x6d0 [gpu_sched] [ ] process_one_work+0x62c/0xb48 [ ] worker_thread+0x468/0x5b0 [ ] kthread+0x1c4/0x1e0 [ ] ret_from_fork+0x10/0x20 Fix it.	7.8	More Details
CVE-2024-46700	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/mes: fix mes ring buffer overflow wait memory room until enough before writing mes packets to avoid ring buffer overflow. v2: squash in sched_hw_submission fix (cherry picked from commit 34e087e8920e635c62e2ed6a758b0cd27f836d13)	7.8	More Details
CVE-2024-34121	Illustrator versions 28.6, 27.9.5 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-40861	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15. An app may be able to gain root privileges.	7.8	More Details
CVE-2024-27321	An arbitrary code execution vulnerability exists in versions 0.0.8 and newer of the Refuel Autolabel library because of the way its multilabel classification tasks handle provided CSV files. If a user creates a multilabel classification task using a maliciously crafted CSV file containing Python code, the code will be passed to an eval function which executes it.	7.8	More Details
CVE-2024-44092	In TBD of TBD, there is a possible LCS signing enforcement missing due to test/debugging code left in a production build. 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-2024-8306	CWE-269: Improper Privilege Management vulnerability exists that could cause unauthorized access, loss of confidentiality, integrity and availability of the workstation when non-admin authenticated user tries to perform privilege escalation by tampering with the binaries.	7.8	More Details
CVE-2024-45026	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: fix error recovery leading to data corruption on ESE devices Extent Space Efficient (ESE) or thin provisioned volumes need to be formatted on demand during usual IO processing. The dasd_ese_needs_format function checks for error codes that signal the non existence of a proper track format. The check for incorrect length is to imprecise since other error cases leading to transport of insufficient data also have this flag set. This might lead to data corruption in certain error cases for example during a storage server warmstart. Fix by removing the check for incorrect length and replacing by explicitly checking for invalid track format in transport mode. Also remove the check for file protected since this is not a valid ESE handling case.	7.8	More Details
CVE-2024-41869	Acrobat Reader versions 24.002.21005, 24.001.30159, 20.005.30655, 24.003.20054 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-43758	Illustrator versions 28.6, 27.9.5 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-45112	Acrobat Reader versions 24.002.21005, 24.001.30159, 20.005.30655, 24.003.20054 and earlier are affected by a Type Confusion vulnerability that could result in arbitrary code execution in the context of the current user. This issue occurs when a resource is accessed using a type that is not compatible with the actual object type, leading to a logic error that an attacker could exploit. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-43756	Photoshop Desktop versions 24.7.4, 25.11 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41857	Illustrator versions 28.6, 27.9.5 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-39384	Premiere Pro versions 24.5, 23.6.8 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-43760	Photoshop Desktop versions 24.7.4, 25.11 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-45108	Photoshop Desktop versions 24.7.4, 25.11 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-45109	Photoshop Desktop versions 24.7.4, 25.11 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-39378	Audition versions 24.4.1, 23.6.6 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-7788	Improper Digital Signature Invalidation vulnerability in Zip Repair Mode of The Document Foundation LibreOffice allows Signature forgery vulnerability in LibreOfficeThis issue affects LibreOffice: from 24.2 before < 24.2.5.	7.8	More Details
CVE-2024-40658	In getConfig of SoftVideoDecoderOMXComponent.cpp, there is a possible out of bounds write due to a heap buffer 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-2024-40657	In addPreferencesForType of AccountTypePreferenceLoader.java, there is a possible way to disable apps for other users due to a confused deputy. 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-2024-40662	In scheme of Uri.java, there is a possible way to craft a malformed Uri object due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2024-41859	After Effects versions 23.6.6, 24.5 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-39381	After Effects versions 23.6.6, 24.5 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-40652	In onCreate of SettingsHomepageActivity.java, there is a possible way to access the Settings app while the device is provisioning due to a missing permission check. 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-2024-40655	In bindAndGetCallIdentification of CallScreeningServiceHelper.java, there is a possible way to maintain a while-in-use permission in the background due to a permissions bypass. 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-2024-40654	In multiple locations, there is a possible permission bypass due to a confused deputy. 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-2024-5760	The Samsung Universal Print Driver for Windows is potentially vulnerable to escalation of privilege allowing the creation of a reverse shell in the tool. This is only applicable for products in the application released or manufactured before 2018.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40650	In wifi_item_edit_content of styles.xml , there is a possible FRP bypass due to Missing check for FRP state. 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-2024-8635	A server-side request forgery issue has been discovered in GitLab EE affecting all versions starting from 16.8 prior to 17.1.7, from 17.2 prior to 17.2.5, and from 17.3 prior to 17.3.2. It was possible for an attacker to make requests to internal resources using a custom Maven Dependency Proxy URL	7.7	More Details
CVE-2024-6137	BT: Classic: SDP OOB access in get_att_search_list	7.6	More Details
CVE-2024-42798	An Incorrect Access Control vulnerability was found in /music/index.php?page=user_list and /music/index.php?page=edit_user in Kashipara Music Management System v1.0. This allows a low privileged attacker to take over the administrator account.	7.6	More Details
CVE-2024-6135	BT:Classic: Multiple missing buf length checks	7.6	More Details
CVE-2024-43969	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Spiffy Plugins Spiffy Calendar allows SQL Injection.This issue affects Spiffy Calendar: from n/a through 4.9.12.	7.6	More Details
CVE-2021-22532	Possible NLDAP Denial of Service attack Vulnerability in eDirectory has been discovered in OpenText™ eDirectory before 9.2.4.0000.	7.6	More Details
CVE-2024-6259	BT: HCI: adv_ext_report Improper discarding in adv_ext_report	7.6	More Details
CVE-2021-27915	Prior to the patched version, there is an XSS vulnerability in the description fields within the Mautic application which could be exploited by a logged in user of Mautic with the appropriate permissions. This could lead to the user having elevated access to the system.	7.6	More Details
CVE-2024-7609	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Vidco Software VOC TESTER allows Path Traversal.This issue affects VOC TESTER: before 12.34.8.	7.5	More Details
CVE-2024-34334	ORDAT FOSS-Online before v2.24.01 was discovered to contain a SQL injection vulnerability via the forgot password function.	7.5	More Details
CVE-2024-46937	An improper access control (IDOR) vulnerability in the /api-selfportal/get-info-token-properties endpoint in MFASOFT Secure Authentication Server (SAS) 1.8.x through 1.9.x before 1.9.040924 allows remote attackers gain access to user tokens without authentication. The is a brute-force attack on the serial parameter by number identifier: GA00001, GA00002, GA00003, etc.	7.5	More Details
CVE-2024-3305	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Utarit Information SoliClub allows Retrieve Embedded Sensitive Data.This issue affects SoliClub: before 4.4.0 for iOS, before 5.2.1 for Android.	7.5	More Details
CVE-2024-45113	ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access and affect the integrity of the application. Exploitation of this issue does not require user interaction.	7.5	More Details
CVE-2024-3306	Authorization Bypass Through User-Controlled Key vulnerability in Utarit Information SoliClub allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SoliClub: before 4.4.0 for iOS, before 5.2.1 for Android.	7.5	More Details
CVE-2024-8752	The Windows version of WebIQ 2.15.9 is affected by a directory traversal vulnerability that allows remote attackers to read any file on the system.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46424	TOTOLINK AC1200 T8 v4.1.5cu.861_B20230220 has a buffer overflow vulnerability in the UploadCustomModule function, which allows attackers to cause a Denial of Service (DoS) via the File parameter.	7.5	More Details
CVE-2024-44165	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, iOS 18 and iPadOS 18, macOS Sonoma 14.7, macOS Sequoia 15. Network traffic may leak outside a VPN tunnel.	7.5	More Details
CVE-2024-45327	An improper authorization vulnerability [CWE-285] in FortiSOAR version 7.4.0 through 7.4.3, 7.3.0 through 7.3.2, 7.2.0 through 7.2.2, 7.0.0 through 7.0.3 change password endpoint may allow an authenticated attacker to perform a brute force attack on users and administrators password via crafted HTTP requests.	7.5	More Details
CVE-2024-44189	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15. A logic issue existed where a process may be able to capture screen contents without user consent.	7.5	More Details
CVE-2024-45788	This vulnerability exists in Reedos aiM-Star version 2.0.1 due to missing rate limiting on OTP requests in certain API endpoints. An authenticated remote attacker could exploit this vulnerability by sending multiple OTP request through vulnerable API endpoints which could lead to the OTP bombing/flooding on the targeted system.	7.5	More Details
CVE-2024-38816	Applications serving static resources through the functional web frameworks WebMvc.fn or WebFlux.fn are vulnerable to path traversal attacks. An attacker can craft malicious HTTP requests and obtain any file on the file system that is also accessible to the process in which the Spring application is running. Specifically, an application is vulnerable when both of the following are true: * the web application uses RouterFunctions to serve static resources * resource handling is explicitly configured with a FileSystemResource location However, malicious requests are blocked and rejected when any of the following is true: * the Spring Security HTTP Firewall https://docs.spring.io/spring-security/reference/servlet/exploits/firewall.html is in use * the application runs on Tomcat or Jetty	7.5	More Details
CVE-2024-46982	Next.js is a React framework for building full-stack web applications. By sending a crafted HTTP request, it is possible to poison the cache of a non-dynamic server-side rendered route in the pages router (this does not affect the app router). When this crafted request is sent it could coerce Next.js to cache a route that is meant to not be cached and send a `Cache-Control: s-maxage=1, stale-while-revalidate` header which some upstream CDNs may cache as well. To be potentially affected all of the following must apply: 1. Next.js between 13.5.1 and 14.2.9, 2. Using pages router, & 3. Using non-dynamic server-side rendered routes e.g. `pages/dashboard.tsx` not `pages/blog/[slug].tsx`. This vulnerability was resolved in Next.js v13.5.7, v14.2.10, and later. We recommend upgrading regardless of whether you can reproduce the issue or not. There are no official or recommended workarounds for this issue, we recommend that users patch to a safe version.	7.5	More Details
CVE-2024-8110	Denial of Service (DoS) vulnerability has been found in Dual-redundant Platform for Computer. If a computer on which the affected product is installed receives a large number of UDP broadcast packets in a short period, occasionally that computer may restart. If both the active and standby computers are restarted at the same time, the functionality on that computer may be temporarily unavailable.	7.5	More Details
CVE-2024-8777	OMFLOW from The SYSCOM Group has an information leakage vulnerability, allowing unauthorized remote attackers to read arbitrary system configurations. If LDAP authentication is enabled, attackers can obtain plaintext credentials.	7.5	More Details
CVE-2024-45825	CVE-2024-45825 IMPACT A denial-of-service vulnerability exists in the affected products. The vulnerability occurs when a malformed CIP packet is sent over the network to the device and results in a major nonrecoverable fault causing a denial-of-service.	7.5	More Details
CVE-2024-8124	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.4 prior to 17.1.7, starting from 17.2 prior to 17.2.5, starting from 17.3 prior to 17.3.2 which could cause Denial of Service via sending a specific POST request.	7.5	More Details
CVE-2024-46943	An issue was discovered in OpenDaylight Authentication, Authorization and Accounting (AAA) through 0.19.3. A rogue controller can join a cluster to impersonate an offline peer, even if this rogue controller does not possess the complete cluster configuration information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39924	An issue was discovered in Vaultwarden (formerly Bitwarden_RS) 1.30.3. A vulnerability has been identified in the authentication and authorization process of the endpoint responsible for altering the metadata of an emergency access. It permits an attacker with granted emergency access to escalate their privileges by changing the access level and modifying the wait time. Consequently, the attacker can gain full control over the vault (when only intended to have read access) while bypassing the necessary wait period.	7.5	More Details
CVE-2024-46938	An issue was discovered in Sitecore Experience Platform (XP), Experience Manager (XM), and Experience Commerce (XC) 8.0 Initial Release through 10.4 Initial Release. An unauthenticated attacker can read arbitrary files.	7.5	More Details
CVE-2024-39925	An issue was discovered in Vaultwarden (formerly Bitwarden_RS) 1.30.3. It lacks an offboarding process for members who leave an organization. As a result, the shared organization key is not rotated when a member departs. Consequently, the departing member, whose access should be revoked, retains a copy of the organization key. Additionally, the application fails to adequately protect some encrypted data stored on the server. Consequently, an authenticated user could gain unauthorized access to encrypted data of any organization, even if the user is not a member of the targeted organization. However, the user would need to know the corresponding organizationId. Hence, if a user (whose access to an organization has been revoked) already possesses the organization key, that user could use the key to decrypt the leaked data.	7.5	More Details
CVE-2024-39926	An issue was discovered in Vaultwarden (formerly Bitwarden_RS) 1.30.3. A stored cross-site scripting (XSS) or, due to the default CSP, HTML injection vulnerability has been discovered in the admin dashboard. This potentially allows an authenticated attacker to inject malicious code into the dashboard, which is then executed or rendered in the context of an administrator's browser when viewing the injected content. However, it is important to note that the default Content Security Policy (CSP) of the application blocks most exploitation paths, significantly mitigating the potential impact.	7.5	More Details
CVE-2023-41833	A race condition in UEFI firmware for some Intel(R) processors may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2023-43626	Improper access control in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2024-21829	Improper input validation in UEFI firmware error handler for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2024-42760	SQL Injection vulnerability in Ellevo v.6.2.0.38160 allows a remote attacker to obtain sensitive information via the /api/mob/instrucao/conta/destinatarios component.	7.5	More Details
CVE-2024-27874	This issue was addressed through improved state management. This issue is fixed in iOS 18 and iPadOS 18. A remote attacker may be able to cause a denial-of-service.	7.5	More Details
CVE-2024-45624	Exposure of sensitive information due to incompatible policies issue exists in Pgpool-II. If a database user accesses a query cache, table data unauthorized for the user may be retrieved.	7.5	More Details
CVE-2024-40770	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. A non-privileged user may be able to modify restricted network settings.	7.5	More Details
CVE-2024-40848	A downgrade issue was addressed with additional code-signing restrictions. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An attacker may be able to read sensitive information.	7.5	More Details
CVE-2024-40856	An integrity issue was addressed with Beacon Protection. This issue is fixed in iOS 18 and iPadOS 18, tvOS 18, macOS Sequoia 15. An attacker may be able to force a device to disconnect from a secure network.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8768	A flaw was found in the vLLM library. A completions API request with an empty prompt will crash the vLLM API server, resulting in a denial of service.	7.5	More Details
CVE-2024-44459	A memory allocation issue in vernemq v2.0.1 allows attackers to cause a Denial of Service (DoS) via excessive memory consumption.	7.5	More Details
CVE-2024-38813	The vCenter Server contains a privilege escalation vulnerability. A malicious actor with network access to vCenter Server may trigger this vulnerability to escalate privileges to root by sending a specially crafted network packet.	7.5	More Details
CVE-2024-47047	An issue was discovered in the powermail extension through 12.4.0 for TYPO3. It fails to validate the mail parameter of the createAction, resulting in Insecure Direct Object Reference (IDOR) in some configurations. An unauthenticated attacker can use this to display user-submitted data of all forms persisted by the extension. The fixed versions are 7.5.1, 8.5.1, 10.9.1, and 12.4.1.	7.5	More Details
CVE-2024-44460	An invalid read size in Nanomq v0.21.9 allows attackers to cause a Denial of Service (DoS).	7.5	More Details
CVE-2024-6077	A denial-of-service vulnerability exists in the Rockwell Automation affected products when specially crafted packets are sent to the CIP Security Object. If exploited the device will become unavailable and require a factory reset to recover.	7.5	More Details
CVE-2024-8751	A vulnerability in the MSC800 allows an unauthenticated attacker to modify the product's IP address over Sopas ET. This can lead to Denial of Service. Users are recommended to upgrade both MSC800 and MSC800 LFT to version V4.26 and S2.93.20 respectively which fixes this issue.	7.5	More Details
CVE-2024-44152	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sequoia 15. An app may be able to access user-sensitive data.	7.5	More Details
CVE-2024-44149	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access protected user data.	7.5	More Details
CVE-2024-27795	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. A camera extension may be able to access the internet.	7.5	More Details
CVE-2024-27879	The issue was addressed with improved bounds checks. This issue is fixed in iOS 17.7 and iPadOS 17.7, iOS 18 and iPadOS 18. An attacker may be able to cause unexpected app termination.	7.5	More Details
CVE-2024-21871	Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	7.5	More Details
CVE-2024-8900	An attacker could write data to the user's clipboard, bypassing the user prompt, during a certain sequence of navigational events. This vulnerability affects Firefox < 129, Firefox ESR < 128.3, and Thunderbird < 128.3.	7.5	More Details
CVE-2024-46047	Tenda FH451 v1.0.0.9 has a stack overflow vulnerability in the fromDhcpListClient function.	7.5	More Details
CVE-2024-6587	A Server-Side Request Forgery (SSRF) vulnerability exists in berriai/litellm version 1.38.10. This vulnerability allows users to specify the `api_base` parameter when making requests to `POST /chat/completions`, causing the application to send the request to the domain specified by `api_base`. This request includes the OpenAI API key. A malicious user can set the `api_base` to their own domain and intercept the OpenAI API key, leading to unauthorized access and potential misuse of the API key.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45854	A Business Logic vulnerability in Shopkit 1.0 allows an attacker to add products with negative quantities to the shopping cart via the qtd parameter in the add-to-cart function.	7.5	More Details
CVE-2024-20317	A vulnerability in the handling of specific Ethernet frames by Cisco IOS XR Software for various Cisco Network Convergence System (NCS) platforms could allow an unauthenticated, adjacent attacker to cause critical priority packets to be dropped, resulting in a denial of service (DoS) condition. This vulnerability is due to incorrect classification of certain types of Ethernet frames that are received on an interface. An attacker could exploit this vulnerability by sending specific types of Ethernet frames to or through the affected device. A successful exploit could allow the attacker to cause control plane protocol relationships to fail, resulting in a DoS condition. 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.	7.4	More Details
CVE-2024-20406	A vulnerability in the segment routing feature for the Intermediate System-to-Intermediate System (IS-IS) protocol of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient input validation of ingress IS-IS packets. An attacker could exploit this vulnerability by sending specific IS-IS packets to an affected device after forming an adjacency. A successful exploit could allow the attacker to cause the IS-IS process on all affected devices that are participating in the Flexible Algorithm to crash and restart, resulting in a DoS condition. Note: The IS-IS protocol is a routing protocol. To exploit this vulnerability, an attacker must be Layer 2-adjacent to the affected device and must have formed an adjacency. This vulnerability affects segment routing for IS-IS over IPv4 and IPv6 control planes as well as devices that are configured as level 1, level 2, or multi-level routing IS-IS type.	7.4	More Details
CVE-2021-38133	Possible External Service Interaction attack in eDirectory has been discovered in OpenText™ eDirectory. This impact all version before 9.2.6.0000.	7.4	More Details
CVE-2024-20430	A vulnerability in Cisco Meraki Systems Manager (SM) Agent for Windows could allow an authenticated, local attacker to execute arbitrary code with elevated privileges. This vulnerability is due to incorrect handling of directory search paths at runtime. A low-privileged attacker could exploit this vulnerability by placing both malicious configuration files and malicious DLL files on an affected system, which would read and execute the files when Cisco Meraki SM launches on startup. A successful exploit could allow the attacker to execute arbitrary code on the affected system with SYSTEM privileges.	7.3	More Details
CVE-2024-8946	A vulnerability was found in MicroPython 1.23.0. It has been classified as critical. Affected is the function mp_vfs_umount of the file extmod/vfs.c of the component VFS Unmount Handler. The manipulation leads to heap-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 29943546343c92334e8518695a11fc0e2ceea68b. It is recommended to apply a patch to fix this issue. In the VFS unmount process, the comparison between the mounted path string and the unmount requested string is based solely on the length of the unmount string, which can lead to a heap buffer overflow read.	7.3	More Details
CVE-2024-8948	A vulnerability was found in MicroPython 1.23.0. It has been rated as critical. Affected by this issue is the function mpz_as_bytes of the file py/objint.c. The manipulation leads to heap-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The patch is identified as 908ab1ceca15ee6fd0ef82ca4cba770a3ec41894. It is recommended to apply a patch to fix this issue. In micropython objint component, converting zero from int to bytes leads to heap buffer-overflow-write at mpz_as_bytes.	7.3	More Details
CVE-2024-8944	A vulnerability, which was classified as critical, was found in code-projects Hospital Management System 1.0. This affects an unknown part of the file check_availability.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-2024-8868	A vulnerability was found in code-projects Crud Operation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file savedata.php. The manipulation of the argument sname 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 Number	Description	Base Score	Reference
CVE-2024-8269	The MStore API – Create Native Android & iOS Apps On The Cloud plugin for WordPress is vulnerable to unauthorized user registration in all versions up to, and including, 4.15.3. This is due to the plugin not checking that user registration is enabled prior to creating a user account through the register() function. This makes it possible for unauthenticated attackers to create user accounts on sites, even when user registration is disabled and plugin functionality is not activated.	7.3	More Details
CVE-2024-8479	The The Simple Spoiler plugin for WordPress is vulnerable to arbitrary shortcode execution in versions 1.2 to 1.3. This is due to the plugin adding the filter add_filter('comment_text', 'do_shortcode'); which will run all shortcodes in comments. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-8271	The The FOX – Currency Switcher Professional for WooCommerce plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.4.2.1. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode in the 'woocs_get_custom_price_html' function. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-8862	A vulnerability, which was classified as critical, has been found in h2oai h2o-3 3.46.0.4. This issue affects the function getConnectionSafe of the file /dtale/chart-data/1 of the component JDBC Connection Handler. The manipulation of the argument query leads to deserialization. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-45799	FluxCP is a web-based Control Panel for rAthena servers written in PHP. A javascript injection is possible via venders/buyers list pages and shop names, that are currently not sanitized. This allows executing arbitrary javascript code on the user's browser just by visiting the shop pages. As a result all logged in to fluxcp users can have their session info stolen. This issue has been addressed in release version 1.3. All users are advised to upgrade. There are no known workarounds for this vulnerability.	7.3	More Details
CVE-2024-7890	Local privilege escalation allows a low-privileged user to gain SYSTEM privileges in Citrix Workspace app for Windows	7.3	More Details
CVE-2024-45801	DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTML, MathML and SVG. It has been discovered that malicious HTML using special nesting techniques can bypass the depth checking added to DOMPurify in recent releases. It was also possible to use Prototype Pollution to weaken the depth check. This renders dompurify unable to avoid cross site scripting (XSS) attacks. This issue has been addressed in versions 2.5.4 and 3.1.3 of DOMPurify. All users are advised to upgrade. There are no known workarounds for this vulnerability.	7.3	More Details
CVE-2024-7889	Local privilege escalation allows a low-privileged user to gain SYSTEM privileges in Citrix Workspace app for Windows	7.3	More Details
CVE-2024-8279	A privilege escalation vulnerability was discovered in XCC that could allow a valid, authenticated XCC user with elevated privileges to perform command injection via specially crafted file uploads.	7.2	More Details
CVE-2024-8280	An input validation weakness was discovered in XCC that could allow a valid, authenticated XCC user with elevated privileges to perform command injection or cause a recoverable denial of service using a specially crafted file.	7.2	More Details
CVE-2024-8281	An input validation weakness was discovered in XCC that could allow a valid, authenticated XCC user with elevated privileges to perform command injection through specially crafted command line input in the XCC SSH captive shell.	7.2	More Details
CVE-2024-20483	Multiple vulnerabilities in Cisco Routed PON Controller Software, which runs as a docker container on hardware that is supported by Cisco IOS XR Software, could allow an authenticated, remote attacker with Administrator-level privileges on the PON Manager or direct access to the PON Manager MongoDB instance to perform command injection attacks on the PON Controller container and execute arbitrary commands as root. These vulnerabilities are due to insufficient validation of arguments that are passed to specific configuration commands. An attacker could exploit these vulnerabilities by including crafted input as the argument of an affected configuration command. A successful exploit could allow the attacker to execute arbitrary commands as root on the PON controller.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42501	An authenticated Path Traversal vulnerabilities exists in the ArubaOS. Successful exploitation of this vulnerability allows an attacker to install unsigned packages on the underlying operating system, enabling the threat actor to execute arbitrary code or install implants.	7.2	More Details
CVE-2024-7766	The Adicon Server WordPress plugin through 1.2 does not sanitize and escape a parameter before using it in a SQL statement, allowing admins to perform SQL injection attacks	7.2	More Details
CVE-2022-2446	The WP Editor plugin for WordPress is vulnerable to deserialization of untrusted input via the 'current_theme_root' parameter in versions up to, and including 1.2.9. This makes it possible for authenticated attackers with administrative privileges to call files using a PHAR wrapper that will deserialize and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present. It also requires that the attacker is successful in uploading a file with the serialized payload.	7.2	More Details
CVE-2024-8686	A command injection vulnerability in Palo Alto Networks PAN-OS software enables an authenticated administrator to bypass system restrictions and run arbitrary commands as root on the firewall.	7.2	More Details
CVE-2024-8761	The Share This Image plugin for WordPress is vulnerable to Open Redirect in all versions up to, and including, 2.03. This is due to insufficient validation on the redirect url supplied via the link parameter. This makes it possible for unauthenticated attackers to redirect users to potentially malicious sites if they can successfully trick them into performing an action.	7.2	More Details
CVE-2024-7129	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin WordPress plugin before 1.6.7.43 does not escape template syntax provided via user input, leading to Twig Template Injection which further exploited can result to remote code Execution by high privilege such as admins	7.2	More Details
CVE-2024-32840	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-32842	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-32843	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-32845	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-32848	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-34779	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-34783	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-34785	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-8278	A privilege escalation vulnerability was discovered in XCC that could allow a valid, authenticated XCC user with elevated privileges to perform command injection via specially crafted IPMI commands.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-32846	An unspecified SQL injection in Ivanti EPM before 2022 SU6, or the 2024 September update allows a remote authenticated attacker with admin privileges to achieve remote code execution.	7.2	More Details
CVE-2024-42503	Authenticated command execution vulnerability exist in the ArubaOS command line interface (CLI). Successful exploitation of this vulnerabilities result in the ability to run arbitrary commands as a priviledge user on the underlying operating system.	7.2	More Details
CVE-2024-21781	Improper input validation in UEFI firmware for some Intel(R) Processors may allow a privileged user to enable information disclosure or denial of service via local access.	7.2	More Details
CVE-2024-8957	PTZOptics PT30X-SDI/NDI-xx before firmware 6.3.40 is vulnerable to an OS command injection issue. The camera does not sufficiently validate the ntp_addr configuration value which may lead to arbitrary command execution when ntp_client is started. When chained with CVE-2024-8956, a remote and unauthenticated attacker can execute arbitrary OS commands on affected devices.	7.2	More Details
CVE-2024-42502	Authenticated command injection vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability result in the ability to inject shell commands on the underlying operating system.	7.2	More Details
CVE-2024-44064	Cross-Site Request Forgery (CSRF) vulnerability in LikeBtn Like Button Rating allows Cross-Site Scripting (XSS).This issue affects Like Button Rating: from n/a through 2.6.54.	7.1	More Details
CVE-2024-44007	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SKT Themes SKT Templates – Elementor & Gutenberg templates allows Reflected XSS.This issue affects SKT Templates – Elementor & Gutenberg templates: from n/a through 6.14.	7.1	More Details
CVE-2024-44009	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WC Lovers WCFM Marketplace allows Reflected XSS.This issue affects WCFM Marketplace: from n/a through 3.6.10.	7.1	More Details
CVE-2024-45459	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PickPlugins Product Slider for WooCommerce allows Reflected XSS.This issue affects Product Slider for WooCommerce: from n/a through 1.13.50.	7.1	More Details
CVE-2024-8687	An information exposure vulnerability exists in Palo Alto Networks PAN-OS software that enables a GlobalProtect end user to learn both the configured GlobalProtect uninstall password and the configured disable or disconnect passcode. After the password or passcode is known, end users can uninstall, disable, or disconnect GlobalProtect even if the GlobalProtect app configuration would not normally permit them to do so.	7.1	More Details
CVE-2024-8691	A vulnerability in the GlobalProtect portal in Palo Alto Networks PAN-OS software enables a malicious authenticated GlobalProtect user to impersonate another GlobalProtect user. Active GlobalProtect users impersonated by an attacker who is exploiting this vulnerability are disconnected from GlobalProtect. Upon exploitation, PAN-OS logs indicate that the impersonated user authenticated to GlobalProtect, which hides the identity of the attacker.	7.1	More Details
CVE-2024-44164	This issue was addressed with improved checks. This issue is fixed in iOS 17.7 and iPadOS 17.7, macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to bypass Privacy preferences.	7.1	More Details
CVE-2024-45854	Deserialization of untrusted data can occur in versions 23.10.3.0 and newer of the MindsDB platform, enabling a maliciously uploaded ‘inhouse’ model to run arbitrary code on the server when a ‘describe’ query is run on it.	7.1	More Details
CVE-2024-45855	Deserialization of untrusted data can occur in versions 23.10.2.0 and newer of the MindsDB platform, enabling a maliciously uploaded ‘inhouse’ model to run arbitrary code on the server when using ‘finetune’ on it.	7.1	More Details
CVE-2024-45458	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Spiffy Plugins Spiffy Calendar allows Reflected XSS.This issue affects Spiffy Calendar: from n/a through 4.9.13.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45853	Deserialization of untrusted data can occur in versions 23.10.2.0 and newer of the MindsDB platform, enabling a maliciously uploaded ‘inhouse’ model to run arbitrary code on the server when used for a prediction.	7.1	More Details
CVE-2024-45606	Sentry is a developer-first error tracking and performance monitoring platform. An authenticated user can mute alert rules from arbitrary organizations and projects with a know rule ID. The user does not need to be a member of the organization or have permissions on the project. In our review, we have identified no instances where alerts have been muted by unauthorized parties. A patch was issued to ensure authorization checks are properly scoped on requests to mute alert rules. Authenticated users who do not have the necessary permissions are no longer able to mute alerts. Sentry SaaS users do not need to take any action. Self-Hosted Sentry users should upgrade to version **24.9.0** or higher. The rule mute feature was generally available as of 23.6.0 but users with early access may have had the feature as of 23.4.0. Affected users are advised to upgrade to version 24.9.0. There are no known workarounds for this vulnerability.	7.1	More Details
CVE-2024-44060	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jennifer Hall Filmix allows Reflected XSS.This issue affects Filmix: from n/a through 1.1.	7.1	More Details
CVE-2024-45023	In the Linux kernel, the following vulnerability has been resolved: md/raid1: Fix data corruption for degraded array with slow disk read_balance() will avoid reading from slow disks as much as possible, however, if valid data only lands in slow disks, and a new normal disk is still in recovery, unrecovered data can be read: raid1_read_request read_balance raid1_should_read_first -> return false choose_best_rdev -> normal disk is not recovered, return -1 choose_bb_rdev -> missing the checking of recovery, return the normal disk -> read unrecovered data Root cause is that the checking of recovery is missing in choose_bb_rdev(). Hence add such checking to fix the problem. Also fix similar problem in choose_slow_rdev().	7.1	More Details
CVE-2024-44053	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Mohammad Arif Opor Ayam allows Reflected XSS.This issue affects Opor Ayam: from n/a through 1.8.	7.1	More Details
CVE-2024-23716	In DevmemIntPFNotify of devicemem_server.c, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	7.0	More Details
CVE-2024-6258	BT: Missing length checks of net_buf in rfcomm_handle_data	6.8	More Details
CVE-2024-7863	The Favicon Generator (CLOSED) WordPress plugin before 2.1 does not validate files to be uploaded and does not have CSRF checks, which could allow attackers to make logged in admin upload arbitrary files such as PHP on the server	6.8	More Details
CVE-2024-32034	decidim is a Free Open-Source participatory democracy, citizen participation and open government for cities and organizations. The admin panel is subject to potential Cross-site scripting (XSS) attach in case an admin assigns a valuator to a proposal, or does any other action that generates an admin activity log where one of the resources has an XSS crafted. This issue has been addressed in release version 0.27.7, 0.28.2, and newer. Users are advised to upgrade. Users unable to upgrade may redirect the pages /admin and /admin/logs to other admin pages to prevent this access (i.e. `/admin/organization/edit`).	6.8	More Details
CVE-2024-45826	CVE-2024-45826 IMPACT Due to improper input validation, a path traversal and remote code execution vulnerability exists when the ThinManager® processes a crafted POST request. If exploited, a user can install an executable file.	6.8	More Details
CVE-2024-7756	A potential vulnerability was reported in the ThinkPad L390 Yoga and 10w Notebook that could allow a local attacker to escalate privileges by accessing an embedded UEFI shell.	6.8	More Details
CVE-2024-45101	A privilege escalation vulnerability was discovered when Single Sign On (SSO) is enabled that could allow an attacker to intercept a valid, authenticated LXCA user’s XCC session if they can convince the user to click on a specially crafted URL.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8641	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.7 prior to 17.1.7, from 17.2 prior to 17.2.5, and from 17.3 prior to 17.3.2. It may have been possible for an attacker with a victim's CI_JOB_TOKEN to obtain a GitLab session token belonging to the victim.	6.7	More Details
CVE-2024-45105	An internal product security audit discovered a UEFI SMM (System Management Mode) callout vulnerability in some ThinkSystem servers that could allow a local attacker with elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2024-31414	The Eaton Foreseer software provides users the capability to customize the dashboard in WebView pages. However, the input fields for this feature in the Eaton Foreseer software lacked proper input sanitization on the server-side, which could lead to injection and execution of malicious scripts when abused by bad actors.	6.7	More Details
CVE-2024-34153	Uncontrolled search path element in Intel(R) RAID Web Console software for all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-3100	A potential buffer overflow vulnerability was reported in some Lenovo Notebook products that could allow a local attacker with elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2024-34543	Improper access control in Intel(R) RAID Web Console software for all versions may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-4550	A potential buffer overflow vulnerability was reported in some Lenovo ThinkSystem and ThinkStation products that could allow a local attacker with elevated privileges to execute arbitrary code.	6.7	More Details
CVE-2024-6840	An improper authorization flaw exists in the Ansible Automation Controller. This flaw allows an attacker using the k8S API server to send an HTTP request with a service account token mounted via `automountServiceAccountToken: true`, resulting in privilege escalation to a service account.	6.6	More Details
CVE-2024-46976	Backstage is an open framework for building developer portals. An attacker with control of the contents of the TechDocs storage buckets is able to inject executable scripts in the TechDocs content that will be executed in the victim's browser when browsing documentation or navigating to an attacker provided link. This has been fixed in the 1.10.13 release of the `@backstage/plugin-techdocs-backend` package. users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2024-8091	The Enhanced Search Box WordPress plugin through 0.6.1 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details
CVE-2024-8093	The Posts reminder WordPress plugin through 0.20 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details
CVE-2024-45537	Apache Druid allows users with certain permissions to read data from other database systems using JDBC. This functionality allows trusted users to set up Druid lookups or run ingestion tasks. Druid also allows administrators to configure a list of allowed properties that users are able to provide for their JDBC connections. By default, this allowed properties list restricts users to TLS-related properties only. However, when configuration a MySQL JDBC connection, users can use a particularly-crafted JDBC connection string to provide properties that are not on this allow list. Users without the permission to configure JDBC connections are not able to exploit this vulnerability. CVE-2021-26919 describes a similar vulnerability which was partially addressed in Apache Druid 0.20.2. This issue is fixed in Apache Druid 30.0.1.	6.5	More Details
CVE-2024-45605	Sentry is a developer-first error tracking and performance monitoring platform. An authenticated user delete the user issue alert notifications for arbitrary users given a know alert ID. A patch was issued to ensure authorization checks are properly scoped on requests to delete user alert notifications. Sentry SaaS users do not need to take any action. Self-Hosted Sentry users should upgrade to version 24.9.0 or higher. There are no known workarounds for this vulnerability.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45815	Backstage is an open framework for building developer portals. A malicious actor with authenticated access to a Backstage instance with the catalog backend plugin installed is able to interrupt the service using a specially crafted query to the catalog API. This has been fixed in the `1.26.0` release of the `@backstage/plugin-catalog-backend`. All users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2024-45816	Backstage is an open framework for building developer portals. When using the AWS S3 or GCS storage provider for TechDocs it is possible to access content in the entire storage bucket. This can leak contents of the bucket that are not intended to be accessible, as well as bypass permission checks in Backstage. This has been fixed in the 1.10.13 release of the `@backstage/plugin-techdocs-backend` package. All users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2024-43938	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Jeroen Peters Name Directory allows Reflected XSS.This issue affects Name Directory: from n/a through 1.29.0.	6.5	More Details
CVE-2024-8044	The infolinks Ad Wrap WordPress plugin through 1.0.2 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details
CVE-2024-43977	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in POSIMYTH The Plus Addons for Elementor Page Builder Lite allows Stored XSS.This issue affects The Plus Addons for Elementor Page Builder Lite: from n/a through 5.6.2.	6.5	More Details
CVE-2024-44008	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Dylan Kuhn Geo Mashup allows Stored XSS.This issue affects Geo Mashup: from n/a through 1.13.12.	6.5	More Details
CVE-2024-44047	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in IDX Broker IMPress for IDX Broker allows Stored XSS.This issue affects IMPress for IDX Broker: from n/a through 3.2.2.	6.5	More Details
CVE-2024-44049	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in ThemeHunk Gutenberg Blocks – Unlimited blocks For Gutenberg allows Stored XSS.This issue affects Gutenberg Blocks – Unlimited blocks For Gutenberg: from n/a through 1.2.7.	6.5	More Details
CVE-2024-44050	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Verbosa allows Stored XSS.This issue affects Verbosa: from n/a through 1.2.3.	6.5	More Details
CVE-2024-44051	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Johan van der Wijk Content Blocks (Custom Post Widget) allows Stored XSS.This issue affects Content Blocks (Custom Post Widget): from n/a through 3.3.5.	6.5	More Details
CVE-2024-45451	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Roseta allows Stored XSS.This issue affects Roseta: from n/a through 1.3.0.	6.5	More Details
CVE-2024-8047	The Visual Sound (old) WordPress plugin through 1.06 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details
CVE-2024-44063	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Happyforms allows Stored XSS.This issue affects Happyforms: from n/a through 1.26.0.	6.5	More Details
CVE-2024-44057	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Nirvana allows Stored XSS.This issue affects Nirvana: from n/a through 1.6.3.	6.5	More Details
CVE-2024-44187	A cross-origin issue existed with "iframe" elements. This was addressed with improved tracking of security origins. This issue is fixed in Safari 18, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, tvOS 18. A malicious website may exfiltrate data cross-origin.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44056	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Mantra allows Stored XSS.This issue affects Mantra: from n/a through 3.3.2.	6.5	More Details
CVE-2024-44058	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Parabola allows Stored XSS.This issue affects Parabola: from n/a through 2.4.1.	6.5	More Details
CVE-2024-44059	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MediaRon LLC Custom Query Blocks allows Stored XSS.This issue affects Custom Query Blocks: from n/a through 5.3.1.	6.5	More Details
CVE-2024-46942	In OpenDaylight Model-Driven Service Abstraction Layer (MD-SAL) through 13.0.1, a controller with a follower role can configure flow entries in an OpenDaylight clustering deployment.	6.5	More Details
CVE-2024-6867	An information disclosure vulnerability exists in the lunary-ai/lunary, specifically in the `runs/{run_id}/related` endpoint. This endpoint does not verify that the user has the necessary access rights to the run(s) they are accessing. As a result, it returns not only the specified run but also all runs that have the `run_id` listed as their parent run. This issue affects the main branch, commit a761d833. The vulnerability allows unauthorized users to obtain information about non-public runs and their related runs, given the `run_id` of a public or non-public run.	6.5	More Details
CVE-2024-44054	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Fluida allows Stored XSS.This issue affects Fluida: from n/a through 1.8.8.	6.5	More Details
CVE-2024-8778	OMFLOW from The SYSCOM Group does not properly validate user input of the download functionality, allowing remote attackers with regular privileges to read arbitrary system files.	6.5	More Details
CVE-2024-6087	An improper access control vulnerability exists in lunary-ai/lunary at the latest commit (a761d83) on the main branch. The vulnerability allows an attacker to use the auth tokens issued by the 'invite user' functionality to obtain valid JWT tokens. These tokens can be used to compromise target users upon registration for their own arbitrary organizations. The attacker can invite a target email, obtain a one-time use token, retract the invite, and later use the token to reset the password of the target user, leading to full account takeover.	6.5	More Details
CVE-2024-8780	OMFLOW from The SYSCOM Group does not properly restrict the query range of its data query functionality, allowing remote attackers with regular privileges to obtain accounts and password hashes of other users.	6.5	More Details
CVE-2024-32940	Improper access control in Intel(R) RAID Web Console software for all versions may allow an authenticated user to potentially enable denial of service via adjacent access.	6.5	More Details
CVE-2024-44062	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Hiroaki Miyashita Custom Field Template allows Stored XSS.This issue affects Custom Field Template: from n/a through 2.6.5.	6.5	More Details
CVE-2024-45457	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Spiffy Plugins Spiffy Calendar allows Stored XSS.This issue affects Spiffy Calendar: from n/a through 4.9.13.	6.5	More Details
CVE-2024-45456	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in JoomUnited WP Meta SEO allows Stored XSS.This issue affects WP Meta SEO: from n/a through 4.5.13.	6.5	More Details
CVE-2024-40866	The issue was addressed with improved UI. This issue is fixed in Safari 18, macOS Sequoia 15. Visiting a malicious website may lead to address bar spoofing.	6.5	More Details
CVE-2024-44124	This issue was addressed through improved state management. This issue is fixed in iOS 18 and iPadOS 18. A malicious Bluetooth input device may bypass pairing.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33848	Uncaught exception in Intel(R) RAID Web Console software all versions may allow an authenticated user to potentially enable denial of service via local access.	6.5	More Details
CVE-2024-45452	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Septera septera allows Stored XSS.This issue affects Septera: from n/a through 1.5.1.	6.5	More Details
CVE-2024-7862	The blogintroduction-wordpress-plugin WordPress plugin through 0.3.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details
CVE-2024-45787	This vulnerability exists in Reedos aiM-Star version 2.0.1 due to transmission of sensitive information in plain text in certain API endpoints. An authenticated remote attacker could exploit this vulnerability by manipulating a parameter through API request URL and intercepting response of the API request leading to exposure of sensitive information belonging to other users.	6.5	More Details
CVE-2024-7859	The Visual Sound WordPress plugin through 1.03 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details
CVE-2024-7820	The ILC Thickbox WordPress plugin through 1.0 does not have CSRF check in place when updating its settings, which could allow attackers to make a logged in admin change them via a CSRF attack	6.5	More Details
CVE-2024-7817	The Misiek Photo Album WordPress plugin through 1.4.3 does not have CSRF checks in some places, which could allow attackers to make logged in users delete arbitrary albums via a CSRF attack	6.5	More Details
CVE-2024-42484	ESP-NOW Component provides a connectionless Wi-Fi communication protocol. An Out-of-Bound (OOB) vulnerability was discovered in the implementation of the ESP-NOW group type message because there is no check for the addrs_num field of the group type message. This can result in memory corruption related attacks. Normally there are two fields in the group information that need to be checked, i.e., the addrs_num field and the addrs_list fileld. Since we only checked the addrs_list field, an attacker can send a group type message with an invalid addrs_num field, which will cause the message handled by the firmware to be much larger than the current buffer, thus causing a memory corruption issue that goes beyond the payload length.	6.5	More Details
CVE-2024-38222	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	6.5	More Details
CVE-2021-22533	Possible Insertion of Sensitive Information into Log File Vulnerability in eDirectory has been discovered in OpenText™ eDirectory 9.2.4.0000.	6.5	More Details
CVE-2024-42483	ESP-NOW Component provides a connectionless Wi-Fi communication protocol. An replay attacks vulnerability was discovered in the implementation of the ESP-NOW because the caches is not differentiated by message types, it is a single, shared resource for all kinds of messages, whether they are broadcast or unicast, and regardless of whether they are ciphertext or plaintext. This can result an attacker to clear the cache of its legitimate entries, there by creating an opportunity to re-inject previously captured packets. This vulnerability is fixed in 2.5.2.	6.5	More Details
CVE-2024-45786	This vulnerability exists in Reedos aiM-Star version 2.0.1 due to improper access controls on its certain API endpoints. An authenticated remote attacker could exploit this vulnerability by manipulating a parameter through API request URL which could lead to gain unauthorized access to sensitive information belonging to other users.	6.5	More Details
CVE-2024-8096	When curl is told to use the Certificate Status Request TLS extension, often referred to as OCSP stapling, to verify that the server certificate is valid, it might fail to detect some OCSP problems and instead wrongly consider the response as fine. If the returned status reports another error than 'revoked' (like for example 'unauthorized') it is not treated as a bad certficate.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4660	An issue has been discovered in GitLab EE affecting all versions starting from 11.2 before 17.1.7, all versions starting from 17.2 before 17.2.5, all versions starting from 17.3 before 17.3.2. It was possible for a guest to read the source code of a private project by using group templates.	6.5	More Details
CVE-2024-7864	The Favicon Generator (CLOSED) WordPress plugin before 2.1 does not have CSRF and path validation in the output_sub_admin_page_0() function, allowing attackers to make logged in admins delete arbitrary files on the server	6.5	More Details
CVE-2024-8311	An issue was discovered with pipeline execution policies in GitLab EE affecting all versions from 17.2 prior to 17.2.5, 17.3 prior to 17.3.2 which allows authenticated users to bypass variable overwrite protection via inclusion of a CI/CD template.	6.5	More Details
CVE-2024-24972	Buffer Copy without Checking Size of Input (CWE-120) in the Controller 6000 and Controller 7000 diagnostic web interface allows an authorised and authenticated operator to reboot the Controller, causing a Denial of Service. Gallagher recommend the diagnostic web page is not enabled (default is off) unless advised by Gallagher Technical support. This interface is intended only for diagnostic purposes. This issue affects: Controller 6000 and Controller 7000 9.10 prior to vCR9.10.240816a (distributed in 9.10.1530 (MR2)), 9.00 prior to vCR9.00.240816a (distributed in 9.00.2168 (MR4)), 8.90 prior to vCR8.90.240816a (distributed in 8.90.2155 (MR5)), 8.80 prior to vCR8.80.240816b (distributed in 8.80.1938 (MR6)), all versions of 8.70 and prior.	6.5	More Details
CVE-2024-4612	An issue has been discovered in GitLab EE affecting all versions starting from 12.9 before 17.1.7, 17.2 before 17.2.5, and 17.3 before 17.3.2. Under certain conditions an open redirect vulnerability could allow for an account takeover by breaking the OAuth flow.	6.4	More Details
CVE-2024-5870	The Tweaker5 theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘url’ parameter within the theme's Button shortcode in all versions up to, and including, 1.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5869	The Neighborly theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘url’ parameter within the theme's Button shortcode 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 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-2024-5867	The Delicate theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'link' parameter within the theme's Button shortcode in all versions up to, and including, 3.5.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-5789	The Triton Lite theme for WordPress is vulnerable to Stored Cross-Site Scripting via the 'url' attribute within the theme's Button shortcode in all versions up to, and including, 1.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8754	An issue has been discovered in GitLab EE/CE affecting all versions from 16.9.7 prior to 17.1.7, 17.2 prior to 17.2.5, and 17.3 prior to 17.3.2. An improper input validation error allows attacker to squat on accounts via linking arbitrary unclaimed provider identities when JWT authentication is configured.	6.4	More Details
CVE-2024-5884	The Beauty theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘tpl_featured_cat_id’ parameter in all versions up to, and including, 1.1.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8747	The Email Obfuscate Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'email-obfuscate' shortcode in all versions up to, and including, 2.0 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 Number	Description	Base Score	Reference
CVE-2024-8045	The Advanced WordPress Backgrounds plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'imageTag' parameter in all versions up to, and including, 1.12.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-45812	Vite a frontend build tooling framework for javascript. Affected versions of vite were discovered to contain a DOM Clobbering vulnerability when building scripts to `cjs`/`iife`/`umd` output format. The DOM Clobbering gadget in the module can lead to cross-site scripting (XSS) in web pages where scriptless attacker-controlled HTML elements (e.g., an img tag with an unsanitized name attribute) are present. DOM Clobbering is a type of code-reuse attack where the attacker first embeds a piece of non-script, seemingly benign HTML markups in the webpage (e.g. through a post or comment) and leverages the gadgets (pieces of js code) living in the existing javascript code to transform it into executable code. We have identified a DOM Clobbering vulnerability in Vite bundled scripts, particularly when the scripts dynamically import other scripts from the assets folder and the developer sets the build output format to `cjs`, `iife`, or `umd`. In such cases, Vite replaces relative paths starting with `__VITE_ASSET__` using the URL retrieved from `document.currentScript`. However, this implementation is vulnerable to a DOM Clobbering attack. The `document.currentScript` lookup can be shadowed by an attacker via the browser's named DOM tree element access mechanism. This manipulation allows an attacker to replace the intended script element with a malicious HTML element. When this happens, the src attribute of the attacker-controlled element is used as the URL for importing scripts, potentially leading to the dynamic loading of scripts from an attacker-controlled server. This vulnerability can result in cross-site scripting (XSS) attacks on websites that include Vite-bundled files (configured with an output format of `cjs`, `iife`, or `umd`) and allow users to inject certain scriptless HTML tags without properly sanitizing the name or id attributes. This issue has been patched in versions 5.4.6, 5.3.6, 5.2.14, 4.5.5, and 3.2.11. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.4	More Details
CVE-2024-8440	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Fancy Text widget in all versions up to, and including, 6.0.3 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-2024-8742	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 plugin's Filterable Gallery widget in all versions up to, and including, 6.0.3 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-2024-5567	The Betheme theme for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 27.5.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-5628	The Avada | Website Builder For WordPress & eCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's fusion_button shortcode in all versions up to, and including, 3.11.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. NOTE: This vulnerability was partially fixed in 3.11.9. Additional hardening for alternate attack vectors was added to version 3.11.10.	6.4	More Details
CVE-2024-4283	An issue has been discovered in GitLab EE affecting all versions starting from 11.1 before 17.1.7, 17.2 before 17.2.5, and 17.3 before 17.3.2. Under certain conditions an open redirect vulnerability could allow for an account takeover by breaking the OAuth flow.	6.4	More Details
CVE-2024-8705	A vulnerability was found in Shandong Star Measurement and Control Equipment Heating Network Wireless Monitoring System 5.6.2 and classified as critical. Affected by this issue is the function GetDataKindByType of the file /DataSrvs/UCCGSrv.asmx. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8949	A vulnerability classified as critical has been found in SourceCodester Online Eyewear Shop 1.0. This affects an unknown part of the file /classes/Master.php of the component Cart Content Handler. The manipulation of the argument cart_id/id leads to improper ownership management. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43793	Halo is an open source website building tool. A security vulnerability has been identified in versions prior to 2.19.0 of the Halo project. This vulnerability allows an attacker to execute malicious scripts in the user's browser through specific HTML and JavaScript code, potentially leading to a Cross-Site Scripting (XSS) attack. This vulnerability is fixed in 2.19.0.	6.3	More Details
CVE-2024-8709	A vulnerability classified as critical has been found in SourceCodester Best House Rental Management System 1.0. Affected is the function delete_user/save_user of the file /admin_class.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-28990	SolarWinds Access Rights Manager (ARM) was found to contain a hard-coded credential authentication bypass vulnerability. If exploited, this vulnerability would allow access to the RabbitMQ management console. We thank Trend Micro Zero Day Initiative (ZDI) for its ongoing partnership in coordinating with SolarWinds on responsible disclosure of this and other potential vulnerabilities.	6.3	More Details
CVE-2024-8710	A vulnerability classified as critical was found in code-projects Inventory Management 1.0. Affected by this vulnerability is an unknown functionality of the file /model/viewProduct.php of the component Products Table Page. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-31415	The Eaton Foreseer software provides the feasibility for the user to configure external servers for multiple purposes such as network management, user management, etc. The software uses encryption to store these configurations securely on the host machine. However, the keys used for this encryption were insecurely stored, which could be abused to possibly change or remove the server configuration.	6.3	More Details
CVE-2024-8762	A vulnerability was found in code-projects Crud Operation System 1.0. It has been classified as critical. This affects an unknown part of the file /updatedata.php. The manipulation of the argument sid leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-5931	BT: Unchecked user input in bap_broadcast_assistant	6.3	More Details
CVE-2024-8784	A vulnerability classified as critical was found in QDocs Smart School Management System 7.0.0. Affected by this vulnerability is an unknown functionality of the file /user/chat/mynewuser of the component Chat. The manipulation of the argument users[] with the input 1'+AND+(SELECT+3220+FROM+(SELECT(SLEEP(5)))ZNun)+AND+'WwBM'%3d'WwBM as part of POST Request Parameter leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 7.0.1 is able to address this issue. It is recommended to upgrade the affected component.	6.3	More Details
CVE-2024-8782	A vulnerability was found in JFinalCMS up to 1.0. It has been rated as critical. This issue affects the function delete of the file /admin/template/edit. The manipulation of the argument name leads to path traversal. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-45104	A valid, authenticated LXCA user without sufficient privileges may be able to use the device identifier to modify an LXCA managed device through a specially crafted web API call.	6.3	More Details
CVE-2024-38315	IBM Aspera Shares 1.0 through 1.10.0 PL3 does not invalidate session after a password reset which could allow an authenticated user to impersonate another user on the system.	6.3	More Details
CVE-2024-7888	The Classified Listing – Classified ads & Business Directory Plugin plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on several functions like export_forms(), import_forms(), update_fb_options(), and many more in all versions up to, and including, 3.1.7. This makes it possible for authenticated attackers, with subscriber-level access and above, to modify forms and various other settings.	6.3	More Details
CVE-2024-8939	A vulnerability was found in the ilab model serve component, where improper handling of the best_of parameter in the vllm JSON web API can lead to a Denial of Service (DoS). The API used for LLM-based sentence or chat completion accepts a best_of parameter to return the best completion from several options. When this parameter is set to a large value, the API does not handle timeouts or resource exhaustion properly, allowing an attacker to cause a DoS by consuming excessive system resources. This leads to the API becoming unresponsive, preventing legitimate users from accessing the service.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8054	The MM-Breaking News WordPress plugin through 0.7.9 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	6.1	More Details
CVE-2024-6017	The Music Request Manager WordPress plugin through 1.3 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack	6.1	More Details
CVE-2024-8646	In Eclipse Glassfish versions prior to 7.0.10, a URL redirection vulnerability to untrusted sites existed. This vulnerability is caused by the vulnerability (CVE-2023-41080) in the Apache code included in GlassFish. This vulnerability only affects applications that are explicitly deployed to the root context ('/').	6.1	More Details
CVE-2024-8730	The Exit Notifier plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.9.1. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-8714	The WordPress Affiliates Plugin — SliceWP Affiliates 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, 1.1.20. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-8724	The Waitlist Woocommerce (Back in stock notifier) plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.7.5. 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-2024-8797	The WP Booking System – Booking Calendar 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, 2.0.19.8. 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-2024-45303	Discourse Calendar plugin adds the ability to create a dynamic calendar in the first post of a topic to Discourse. Rendering event names can be susceptible to XSS attacks. This vulnerability only affects sites which have modified or disabled Discourse's default Content Security Policy. The issue is patched in version 0.5 of the Discourse Calendar plugin.	6.1	More Details
CVE-2024-40857	This issue was addressed through improved state management. This issue is fixed in Safari 18, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, tvOS 18. Processing maliciously crafted web content may lead to universal cross site scripting.	6.1	More Details
CVE-2024-45803	Wire UI is a library of components and resources to empower Laravel and Livewire application development. A potential Cross-Site Scripting (XSS) vulnerability has been identified in the `/wireui/button` endpoint, specifically through the `label` query parameter. Malicious actors could exploit this vulnerability by injecting JavaScript into the `label` parameter, leading to the execution of arbitrary code in the victim's browser. The `/wireui/button` endpoint dynamically renders button labels based on user-provided input via the `label` query parameter. Due to insufficient sanitization or escaping of this input, an attacker can inject malicious JavaScript. By crafting such a request, an attacker can inject arbitrary code that will be executed by the browser when the endpoint is accessed. If exploited, this vulnerability could allow an attacker to execute arbitrary JavaScript code in the context of the affected website. This could lead to: **Session Hijacking**: Stealing session cookies, tokens, or other sensitive information. **User Impersonation**: Performing unauthorized actions on behalf of authenticated users. **Phishing**: Redirecting users to malicious websites. **Content Manipulation**: Altering the appearance or behavior of the affected page to mislead users or execute further attacks. The severity of this vulnerability depends on the context of where the affected component is used, but in all cases, it poses a significant risk to user security. This issue has been addressed in release versions 1.19.3 and 2.1.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.1	More Details
CVE-2024-8052	The Review Ratings WordPress plugin through 1.6 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40826	A privacy issue was addressed with improved handling of files. This issue is fixed in iOS 18 and iPadOS 18, macOS Sequoia 15. An unencrypted document may be written to a temporary file when using print preview.	6.1	More Details
CVE-2024-40797	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. Visiting a malicious website may lead to user interface spoofing.	6.1	More Details
CVE-2024-8776	SmartRobot from INTUMIT does not properly validate a specific page parameter, allowing unautheticated remote attackers to inject JavaScript code to the parameter for Reflected Cross-site Scripting attacks.	6.1	More Details
CVE-2024-7312	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Payara Platform Payara Server (REST Management Interface modules) allows Session Hijacking.This issue affects Payara Server: from 6.0.0 before 6.18.0, from 6.2022.1 before 6.2024.9, from 5.2020.2 before 5.2022.5, from 5.20.0 before 5.67.0, from 4.1.2.191.0 before 4.1.2.191.50.	6.1	More Details
CVE-2024-6018	The Music Request Manager WordPress plugin through 1.3 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could lead to Reflected Cross-Site Scripting in old web browsers	6.1	More Details
CVE-2024-8731	The Cron Jobs plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.2.9. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-22351	Out-of-bounds write in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.1	More Details
CVE-2023-23904	NULL pointer dereference in the UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	6.1	More Details
CVE-2024-6019	The Music Request Manager WordPress plugin through 1.3 does not sanitise and escape incoming music requests, which could allow unauthenticated users to perform Cross-Site Scripting attacks against administrators	6.1	More Details
CVE-2024-8622	The amCharts: Charts and Maps plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'amcharts_javascript' parameter in all versions up to, and including, 1.4.4 due to the ability to supply arbitrary JavaScript a lack of nonce validation on the preview functionality. 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-2024-8663	The WP Simple Booking Calendar 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, 2.0.10. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-2010	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in TE Informatics V5 allows Reflected XSS.This issue affects V5: before 6.2.	6.1	More Details
CVE-2024-8056	The MM-Breaking News WordPress plugin through 0.7.9 does not escape the $_SERVER['REQUEST_URI'] parameter before outputting it back in an attribute, which could lead to Reflected Cross-Site Scripting in old web browsers	6.1	More Details
CVE-2024-8897	Under certain conditions, an attacker with the ability to redirect users to a malicious site via an open redirect on a trusted site, may be able to spoof the address bar contents. This can lead to a malicious site to appear to have the same URL as the trusted site. *This bug only affects Firefox for Android. Other versions of Firefox are unaffected.* This vulnerability affects Firefox for Android < 130.0.1.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7861	The Misiek Paypal WordPress plugin through 1.1.20090324 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	6.1	More Details
CVE-2024-7860	The Simple Headline Rotator WordPress plugin through 1.0 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	6.1	More Details
CVE-2024-7816	The Gixaw Chat WordPress plugin through 1.0 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	6.1	More Details
CVE-2024-7822	The Quick Code WordPress plugin through 1.0 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	6.1	More Details
CVE-2024-7818	The Misiek Photo Album WordPress plugin through 1.4.3 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	6.1	More Details
CVE-2024-8656	The WPFactory Helper plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.7.0. 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-2024-34335	ORDAT FOSS-Online before version 2.24.01 was discovered to contain a reflected cross-site scripting (XSS) vulnerability via the login page.	6.1	More Details
CVE-2024-38860	Improper neutralization of input in Checkmk before versions 2.3.0p16 and 2.2.0p34 allows attackers to craft malicious links that can facilitate phishing attacks.	6.1	More Details
CVE-2024-8664	The WP Test Email plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.1.7. 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-2024-8737	The PDF Thumbnail Generator plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.3. 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-2024-8665	The YITH Custom Login plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.7.3. 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-2024-8732	The Roles & Capabilities plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.1.9. 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-2024-8734	The Lucas String Replace 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, 2.0.5. 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-2024-8907	Insufficient data validation in Omnibox in Google Chrome on Android prior to 129.0.6668.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to inject arbitrary scripts or HTML (XSS) via a crafted set of UI gestures. (Chromium security severity: Medium)	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23906	Improper Neutralization of Input During Web Page Generation (CWE-79) in the Controller 6000 and Controller 7000 diagnostic webpage allows an attacker to modify Controller configuration during an authenticated Operator's session. This issue affects: Controller 6000 and Controller 7000 9.10 prior to vCR9.10.240816a (distributed in 9.10.1530 (MR2)), 9.00 prior to vCR9.00.240816a (distributed in 9.00.2168 (MR4)), 8.90 prior to vCR8.90.240816a (distributed in 8.90.2155 (MR5)), 8.80 prior to vCR8.80.240816b (distributed in 8.80.1938 (MR6)), all versions of 8.70 and prior.	6.1	More Details
CVE-2024-4465	An access control vulnerability was discovered in the Reports section due to a specific access restriction not being properly enforced for users with limited privileges. If a logged-in user with reporting privileges learns how to create a specific application request, they might be able to make limited changes to the reporting configuration. This could result in a partial loss of data integrity. In Guardian/CMC instances with a reporting configuration, there could be limited Denial of Service (DoS) impacts, as the reports may not reach their intended destination, and there could also be limited information disclosure impacts. Furthermore, modifying the destination SMTP server for the reports could lead to the compromise of external credentials, as they might be sent to an unauthorized server. This could expand the scope of the attack.	6.0	More Details
CVE-2024-45455	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in JoomUnited WP Meta SEO allows Stored XSS.This issue affects WP Meta SEO: from n/a through 4.5.13.	5.9	More Details
CVE-2024-42796	An Incorrect Access Control vulnerability was found in /music/ajax.php?action=delete_genre in Kashipara Music Management System v1.0. This vulnerability allows an unauthenticated attacker to delete the valid music genre entries.	5.9	More Details
CVE-2024-43985	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in MagePeople Team Bus Ticket Booking with Seat Reservation allows Stored XSS.This issue affects Bus Ticket Booking with Seat Reservation: from n/a through 5.3.5.	5.9	More Details
CVE-2024-45460	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Manu225 Flipping Cards allows Stored XSS.This issue affects Flipping Cards: from n/a through 1.30.	5.9	More Details
CVE-2024-37985	Windows Kernel Information Disclosure Vulnerability	5.9	More Details
CVE-2021-22518	A vulnerability identified in OpenText™ Identity Manager AzureAD Driver that allows logging of sensitive information into log file. This impacts all versions before 5.1.4.0	5.8	More Details
CVE-2024-45607	whatsapp-api-js is a TypeScript server agnostic Whatsapp's Official API framework. It's possible to check the payload validation using the WhatsAppAPI.verifyRequestSignature and expect false when the signature is valid. Incorrect Access Control, anyone using the post or verifyRequestSignature methods to handle messages is impacted. This vulnerability is fixed in 4.0.3.	5.8	More Details
CVE-2024-8880	A vulnerability classified as critical has been found in playSMS 1.4.4/1.4.5/1.4.6/1.4.7. Affected is an unknown function of the file /playsms/index.php?app=main&inc=core_auth&route=forgot&op=forgot of the component Template Handler. The manipulation of the argument username/email/captcha leads to code injection. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The project maintainer was informed early about the issue. Investigation shows that playSMS up to 1.4.3 contained a fix but later versions re-introduced the flaw. As long as the latest version of the playsms/tpl package is used, the software is not affected. Version >=1.4.4 shall fix this issue for sure.	5.6	More Details
CVE-2024-8947	A vulnerability was found in MicroPython 1.22.2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file py/objarray.c. The manipulation leads to use after free. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. Upgrading to version 1.23.0 is able to address this issue. The identifier of the patch is 4bed614e707c0644c06e117f848fa12605c711cd. It is recommended to upgrade the affected component. In micropython objarray component, when a bytes object is resized and copied into itself, it may reference memory that has already been freed.	5.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31416	The Eaton Foreseer software provides multiple customizable input fields for the users to configure parameters in the tool like alarms, reports, etc. Some of these input fields were not checking the length and bounds of the entered value. The exploit of this security flaw by a bad actor may result in excessive memory consumption or integer overflow.	5.6	More Details
CVE-2024-45029	In the Linux kernel, the following vulnerability has been resolved: i2c: tegra: Do not mark ACPI devices as irq safe On ACPI machines, the tegra i2c module encounters an issue due to a mutex being called inside a spinlock. This leads to the following bug: BUG: sleeping function called from invalid context at kernel/locking/mutex.c:585 ... Call trace: __might_sleep __mutex_lock_common mutex_lock_nested acpi_subsys_runtime_resume rpm_resume tegra_i2c_xfer The problem arises because during __pm_runtime_resume(), the spinlock &dev->power.lock is acquired before rpm_resume() is called. Later, rpm_resume() invokes acpi_subsys_runtime_resume(), which relies on mutexes, triggering the error. To address this issue, devices on ACPI are now marked as not IRQ-safe, considering the dependency of acpi_subsys_runtime_resume() on mutexes.	5.5	More Details
CVE-2024-44176	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, macOS Sonoma 14.7, tvOS 18. Processing an image may lead to a denial-of-service.	5.5	More Details
CVE-2024-27880	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in iOS 17.7 and iPadOS 17.7, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, macOS Sonoma 14.7, tvOS 18. Processing a maliciously crafted file may lead to unexpected app termination.	5.5	More Details
CVE-2024-20343	A vulnerability in the CLI of Cisco IOS XR Software could allow an authenticated, local attacker to read any file in the file system of the underlying Linux operating system. The attacker must have valid credentials on the affected device. This vulnerability is due to incorrect validation of the arguments that are passed to a specific CLI command. An attacker could exploit this vulnerability by logging in to an affected device with low-privileged credentials and using the affected command. A successful exploit could allow the attacker access files in read-only mode on the Linux file system.	5.5	More Details
CVE-2024-27876	A race condition was addressed with improved locking. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, iOS 18 and iPadOS 18, macOS Sonoma 14.7, macOS Sequoia 15. Unpacking a maliciously crafted archive may allow an attacker to write arbitrary files.	5.5	More Details
CVE-2024-27875	A logic issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15. Privacy Indicators for microphone or camera access may be attributed incorrectly.	5.5	More Details
CVE-2024-44177	A privacy issue was addressed by removing sensitive data. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-27869	The issue was addressed with improved checks. This issue is fixed in iOS 18 and iPadOS 18, macOS Sequoia 15. An app may be able to record the screen without an indicator.	5.5	More Details
CVE-2024-27861	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15. An application may be able to read restricted memory.	5.5	More Details
CVE-2024-27860	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15. An application may be able to read restricted memory.	5.5	More Details
CVE-2024-27858	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access protected user data.	5.5	More Details
CVE-2024-46705	In the Linux kernel, the following vulnerability has been resolved: drm/xe: reset mmio mappings with devm Set our various mmio mappings to NULL. This should make it easier to catch something rogue trying to mess with mmio after device removal. For example, we might unmap everything and then start hitting some mmio address which has already been unmamped by us and then remapped by something else, causing all kinds of carnage.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23237	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15. An app may be able to cause a denial-of-service.	5.5	More Details
CVE-2024-46672	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: cfg80211: Handle SSID based pmksa deletion wpa_supplicant 2.11 sends since 1efdba5fdc2c ("Handle PMKSA flush in the driver for SAE/OWE offload cases") SSID based PMKSA del commands. brcmfmac is not prepared and tries to dereference the NULL bssid and pmkid pointers in cfg80211_pmksa. PMKID_V3 operations support SSID based updates so copy the SSID.	5.5	More Details
CVE-2024-45111	Illustrator versions 28.6, 27.9.5 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-2024-44170	A privacy issue was addressed by moving sensitive data to a more secure location. This issue is fixed in iOS 18 and iPadOS 18, watchOS 11, macOS Sequoia 15. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-44163	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. A malicious application may be able to access private information.	5.5	More Details
CVE-2024-44183	A logic error was addressed with improved error handling. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, macOS Sonoma 14.7, tvOS 18. An app may be able to cause a denial-of-service.	5.5	More Details
CVE-2024-45025	In the Linux kernel, the following vulnerability has been resolved: fix bitmap corruption on close_range() with CLOSE_RANGE_UNSHARE copy_fd_bitmaps(new, old, count) is expected to copy the first count/BITS_PER_LONG bits from old->full_fds_bits[] and fill the rest with zeroes. What it does is copying enough words (BITS_TO_LONGS(count/BITS_PER_LONG)), then memsets the rest. That works fine, *if* all bits past the cutoff point are clear. Otherwise we are risking garbage from the last word we'd copied. For most of the callers that is true - expand_fdtable() has count equal to old->max_fds, so there's no open descriptors past count, let alone fully occupied words in ->open_fds[], which is what bits in ->full_fds_bits[] correspond to. The other caller (dup_fd()) passes sane_fdtable_size(old_fdt, max_fds), which is the smallest multiple of BITS_PER_LONG that covers all opened descriptors below max_fds. In the common case (copying on fork()) max_fds is ~0U, so all opened descriptors will be below it and we are fine, by the same reasons why the call in expand_fdtable() is safe. Unfortunately, there is a case where max_fds is less than that and where we might, indeed, end up with junk in ->full_fds_bits[] - close_range(from, to, CLOSE_RANGE_UNSHARE) with * descriptor table being currently shared * 'to' being above the current capacity of descriptor table * 'from' being just under some chunk of opened descriptors. In that case we end up with observably wrong behaviour - e.g. spawn a child with CLONE_FILES, get all descriptors in range 0..127 open, then close_range(64, ~0U, CLOSE_RANGE_UNSHARE) and watch dup(0) ending up with descriptor #128, despite #64 being observably not open. The minimally invasive fix would be to deal with that in dup_fd(). If this proves to add measurable overhead, we can go that way, but let's try to fix copy_fd_bitmaps() first. * new helper: bitmap_copy_and_expand(to, from, bits_to_copy, size). * make copy_fd_bitmaps() take the bitmap size in words, rather than bits; it's 'count' argument is always a multiple of BITS_PER_LONG, so we are not losing any information, and that way we can use the same helper for all three bitmaps - compiler will see that count is a multiple of BITS_PER_LONG for the large ones, so it'll generate plain memcpy()+memset(). Reproducer added to tools/testing/selftests/core/close_range_test.c	5.5	More Details
CVE-2024-44166	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-44167	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.7, visionOS 2, iOS 18 and iPadOS 18, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to overwrite arbitrary files.	5.5	More Details
CVE-2024-44168	A library injection issue was addressed with additional restrictions. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to modify protected parts of the file system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45030	In the Linux kernel, the following vulnerability has been resolved: igb: cope with large MAX_SKB_FRAGS Sabrina reports that the igb driver does not cope well with large MAX_SKB_FRAG values: setting MAX_SKB_FRAG to 45 causes payload corruption on TX. An easy reproducer is to run ssh to connect to the machine. With MAX_SKB_FRAGS=17 it works, with MAX_SKB_FRAGS=45 it fails. This has been reported originally in https://bugzilla.redhat.com/show_bug.cgi?id=2265320 The root cause of the issue is that the driver does not take into account properly the (possibly large) shared info size when selecting the ring layout, and will try to fit two packets inside the same 4K page even when the 1st fraglist will trump over the 2nd head. Address the issue by checking if 2K buffers are insufficient.	5.5	More Details
CVE-2024-45027	In the Linux kernel, the following vulnerability has been resolved: usb: xhci: Check for xhci->interrupters being allocated in xhci_mem_clearup() If xhci_mem_init() fails, it calls into xhci_mem_cleanup() to mop up the damage. If it fails early enough, before xhci->interrupters is allocated but after xhci->max_interrupters has been set, which happens in most (all?) cases, things get uglier, as xhci_mem_cleanup() unconditionally derefences xhci->interrupters. With prejudice. Gate the interrupt freeing loop with a check on xhci->interrupters being non-NULL. Found while debugging a DMA allocation issue that led the XHCI driver on this exact path.	5.5	More Details
CVE-2024-45028	In the Linux kernel, the following vulnerability has been resolved: mmc: mmc_test: Fix NULL dereference on allocation failure If the "test->highmem = alloc_pages()" allocation fails then calling __free_pages(test->highmem) will result in a NULL dereference. Also change the error code to -ENOMEM instead of returning success.	5.5	More Details
CVE-2024-44169	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, macOS Sonoma 14.7, tvOS 18. An app may be able to cause unexpected system termination.	5.5	More Details
CVE-2024-44182	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access sensitive data logged when a shortcut fails to launch another app.	5.5	More Details
CVE-2024-44184	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, iOS 18 and iPadOS 18, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-44188	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access protected user data.	5.5	More Details
CVE-2024-40790	The issue was addressed with improved handling of caches. This issue is fixed in visionOS 2. An app may be able to read sensitive data from the GPU memory.	5.5	More Details
CVE-2024-44151	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2024-40860	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2024-46707	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Make ICC_*SGI*_EL1 undef in the absence of a vGICv3 On a system with a GICv3, if a guest hasn't been configured with GICv3 and that the host is not capable of GICv2 emulation, a write to any of the ICC_*SGI*_EL1 registers is trapped to EL2. We therefore try to emulate the SGI access, only to hit a NULL pointer as no private interrupt is allocated (no GIC, remember?). The obvious fix is to give the guest what it deserves, in the shape of a UNDEF exception.	5.5	More Details
CVE-2024-40863	This issue was addressed with improved data protection. This issue is fixed in iOS 18 and iPadOS 18. An app may be able to leak sensitive user information.	5.5	More Details
CVE-2024-44198	An integer overflow was addressed through improved input validation. This issue is fixed in visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, tvOS 18. Processing maliciously crafted web content may lead to an unexpected process crash.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44125	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. A malicious application may be able to leak sensitive user information.	5.5	More Details
CVE-2024-44186	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access protected user data.	5.5	More Details
CVE-2024-44128	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An Automator Quick Action workflow may be able to bypass Gatekeeper.	5.5	More Details
CVE-2024-44129	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7, macOS Sequoia 15. An app may be able to leak sensitive user information.	5.5	More Details
CVE-2024-44161	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted texture may lead to unexpected app termination.	5.5	More Details
CVE-2024-44191	This issue was addressed through improved state management. This issue is fixed in iOS 17.7 and iPadOS 17.7, Xcode 16, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, tvOS 18. An app may gain unauthorized access to Bluetooth.	5.5	More Details
CVE-2024-41867	After Effects versions 23.6.6, 24.5 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-2024-44131	This issue was addressed with improved validation of symlinks. This issue is fixed in iOS 18 and iPadOS 18, macOS Sequoia 15. An app may be able to access sensitive user data.	5.5	More Details
CVE-2024-44190	A path handling issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to read arbitrary files.	5.5	More Details
CVE-2024-44147	This issue was addressed through improved state management. This issue is fixed in iOS 18 and iPadOS 18. An app may gain unauthorized access to Local Network.	5.5	More Details
CVE-2024-44133	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15. On MDM managed devices, an app may be able to bypass certain Privacy preferences.	5.5	More Details
CVE-2024-44134	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sequoia 15. An app may be able to read sensitive location information.	5.5	More Details
CVE-2024-40859	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-44153	The issue was addressed with improved permissions logic. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access user-sensitive data.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45024	In the Linux kernel, the following vulnerability has been resolved: mm/hugetlb: fix hugetlb vs. core-mm PT locking We recently made GUP's common page table walking code to also walk hugetlb VMAs without most hugetlb special-casing, preparing for the future of having less hugetlb-specific page table walking code in the codebase. Turns out that we missed one page table locking detail: page table locking for hugetlb folios that are not mapped using a single PMD/PUD. Assume we have hugetlb folio that spans multiple PTEs (e.g., 64 KiB hugetlb folios on arm64 with 4 KiB base page size). GUP, as it walks the page tables, will perform a pte_offset_map_lock() to grab the PTE table lock. However, hugetlb that concurrently modifies these page tables would actually grab the mm->page_table_lock: with USE_SPLIT_PTE_PTLOCKS, the locks would differ. Something similar can happen right now with hugetlb folios that span multiple PMDs when USE_SPLIT_PMD_PTLOCKS. This issue can be reproduced [1], for example triggering: [3105.936100] ----------[cut here]----------- [3105.939323] WARNING: CPU: 31 PID: 2732 at mm/gup.c:142 try_grab_folio+0x11c/0x188 [3105.944634] Modules linked in: [...] [3105.974841] CPU: 31 PID: 2732 Comm: reproducer Not tainted 6.10.0-64.eln141.aarch64 #1 [3105.980406] Hardware name: QEMU KVM Virtual Machine, BIOS edk2-20240524-4.fc40 05/24/2024 [3105.986185] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [3105.991108] pc : try_grab_folio+0x11c/0x188 [3105.994013] lr : follow_page_pte+0xd8/0x430 [3105.996986] sp : ffff80008eafb8f0 [3105.999346] x29: ffff80008eafb900 x28: ffffffe8d481f380 x27: 00f80001207cff43 [3106.004414] x26: 0000000000000001 x25: 0000000000000000 x24: ffff80008eafba48 [3106.009520] x23: 0000ffff9372f000 x22: ffff7a54459e2000 x21: ffff7a546c1aa978 [3106.014529] x20: ffffffe8d481f3c0 x19: 0000000000610041 x18: 0000000000000001 [3106.019506] x17: 0000000000000001 x16: ffffffffffffffff x15: 0000000000000000 [3106.024494] x14: ffffb85477fdfe08 x13: 0000ffff9372ffff x12: 0000000000000000 [3106.029469] x11: 1fffef4a88a96be1 x10: ffff7a54454b5f0c x9 : ffffb854771b12f0 [3106.034324] x8 : 0008000000000000 x7 : ffff7a546c1aa980 x6 : 0008000000000080 [3106.038902] x5 : 00000000001207cf x4 : 0000ffff9372f000 x3 : ffffffe8d481f000 [3106.043420] x2 : 0000000000610041 x1 : 0000000000000001 x0 : 0000000000000000 [3106.047957] Call trace: [3106.049522] try_grab_folio+0x11c/0x188 [3106.051996] follow_pmd_mask.constprop.0.isra.0+0x150/0x2e0 [3106.055527] follow_page_mask+0x1a0/0x2b8 [3106.058118] __get_user_pages+0xf0/0x348 [3106.060647] faultin_page_range+0xb0/0x360 [3106.063651] do_madvise+0x340/0x598 Let's make huge_pte_lockptr() effectively use the same PT locks as any core-mm page table walker would. Add ptep_lockptr() to obtain the PTE page table lock using a pte pointer -- unfortunately we cannot convert pte_lockptr() because virt_to_page() doesn't work with kmap'ed page tables we can have with CONFIG_HIGHPTE. Handle CONFIG_PGTABLE_LEVELS correctly by checking in reverse order, such that when e.g., CONFIG_PGTABLE_LEVELS==2 with PGDIR_SIZE==P4D_SIZE==PUD_SIZE==PMD_SIZE will work as expected. Document why that works. There is one ugly case: powerpc 8xx, whereby we have an 8 MiB hugetlb folio being mapped using two PTE page tables. While hugetlb wants to take the PMD table lock, core-mm would grab the PTE table lock of one of both PTE page tables. In such corner cases, we have to make sure that both locks match, which is (fortunately!) currently guaranteed for 8xx as it does not support SMP and consequently doesn't use split PT locks. [1] https://lore.kernel.org/all/1bbfcc7f-f222-45a5-ac44-c5a1381c596d@redhat.com/	5.5	More Details
CVE-2024-46706	In the Linux kernel, the following vulnerability has been resolved: tty: serial: fsl_lpuart: mark last busy before uart_add_one_port With "earlycon initcall_debug=1 loglevel=8" in bootargs, kernel sometimes boot hang. It is because normal console still is not ready, but runtime suspend is called, so early console putchar will hang in waiting TRDE set in UARTSTAT. The lpuart driver has auto suspend delay set to 3000ms, but during uart_add_one_port, a child device serial ctrl will added and probed with its pm runtime enabled(see serial_ctrl.c). The runtime suspend call path is: device_add l-> bus_probe_device l->device_initial_probe l->__device_attach l-> pm_runtime_get_sync(dev->parent); l-> pm_request_idle(dev); l-> pm_runtime_put(dev->parent); So in the end, before normal console ready, the lpuart get runtime suspended. And earlycon putchar will hang. To address the issue, mark last busy just after pm_runtime_enable, three seconds is long enough to switch from bootconsole to normal console.	5.5	More Details
CVE-2024-40801	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access protected user data.	5.5	More Details
CVE-2024-44135	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access protected files within an App Sandbox container.	5.5	More Details
CVE-2024-44158	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 17.7 and iPadOS 17.7, macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. A shortcut may output sensitive user data without consent.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40831	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access a user's Photos Library.	5.5	More Details
CVE-2024-40837	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access protected user data.	5.5	More Details
CVE-2024-40841	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted video file may lead to unexpected app termination.	5.5	More Details
CVE-2024-40842	An issue was addressed with improved validation of environment variables. This issue is fixed in macOS Sequoia 15. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-40843	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2024-40844	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in iOS 17.7 and iPadOS 17.7, macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to observe data displayed to the user by Shortcuts.	5.5	More Details
CVE-2024-40845	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted video file may lead to unexpected app termination.	5.5	More Details
CVE-2024-40846	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted video file may lead to unexpected app termination.	5.5	More Details
CVE-2024-40847	The issue was addressed with additional code-signing restrictions. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access sensitive user data.	5.5	More Details
CVE-2024-43759	Illustrator versions 28.6, 27.9.5 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacker could exploit this vulnerability to crash the application, resulting in a DoS condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-44154	A memory initialization issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted file may lead to unexpected app termination.	5.5	More Details
CVE-2024-40850	A file access issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, macOS Sonoma 14.7, tvOS 18. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2024-44160	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted texture may lead to unexpected app termination.	5.5	More Details
CVE-2024-44178	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to modify protected parts of the file system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45022	In the Linux kernel, the following vulnerability has been resolved: mm/vmalloc: fix page mapping if vm_area_alloc_pages() with high order fallback to order 0 The __vmap_pages_range_noflush() assumes its argument pages** contains pages with the same page shift. However, since commit e9c3cda4d86e ("mm, vmalloc: fix high order __GFP_NOFAIL allocations"), if gfp_flags includes __GFP_NOFAIL with high order in vm_area_alloc_pages() and page allocation failed for high order, the pages** may contain two different page shifts (high order and order-0). This could lead __vmap_pages_range_noflush() to perform incorrect mappings, potentially resulting in memory corruption. Users might encounter this as follows (vmap_allow_huge = true, 2M is for PMD_SIZE): kvmalloc(2M, __GFP_NOFAILIGFP_X) __vmalloc_node_range_noprof(vm_flags=VM_ALLOW_HUGE_VMAP) vm_area_alloc_pages(order=9) ---> order-9 allocation failed and fallback to order-0 vmap_pages_range() vmap_pages_range_noflush() __vmap_pages_range_noflush(page_shift = 21) ----> wrong mapping happens We can remove the fallback code because if a high-order allocation fails, __vmalloc_node_range_noprof() will retry with order-0. Therefore, it is unnecessary to fallback to order-0 here. Therefore, fix this by removing the fallback code.	5.5	More Details
CVE-2024-41868	Audition versions 24.4.1, 23.6.6 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-2024-46677	In the Linux kernel, the following vulnerability has been resolved: gtp: fix a potential NULL pointer dereference When sockfd_lookup() fails, gtp_encap_enable_socket() returns a NULL pointer, but its callers only check for error pointers thus miss the NULL pointer case. Fix it by returning an error pointer with the error code carried from sockfd_lookup(). (I found this bug during code inspection.)	5.5	More Details
CVE-2024-46676	In the Linux kernel, the following vulnerability has been resolved: nfc: pn533: Add poll mod list filling check In case of im_protocols value is 1 and tm_protocols value is 0 this combination successfully passes the check 'if (!im_protocols && !tm_protocols)' in the nfc_start_poll(). But then after pn533_poll_create_mod_list() call in pn533_start_poll() poll mod list will remain empty and dev->poll_mod_count will remain 0 which lead to division by zero. Normally no im protocol has value 1 in the mask, so this combination is not expected by driver. But these protocol values actually come from userspace via Netlink interface (NFC_CMD_START_POLL operation). So a broken or malicious program may pass a message containing a "bad" combination of protocol parameter values so that dev->poll_mod_count is not incremented inside pn533_poll_create_mod_list(), thus leading to division by zero. Call trace looks like: nfc_genl_start_poll() nfc_start_poll() ->start_poll() pn533_start_poll() Add poll mod list filling check. Found by Linux Verification Center (linuxtesting.org) with SVACE.	5.5	More Details
CVE-2024-46675	In the Linux kernel, the following vulnerability has been resolved: usb: dwc3: core: Prevent USB core invalid event buffer address access This commit addresses an issue where the USB core could access an invalid event buffer address during runtime suspend, potentially causing SMMU faults and other memory issues in Exynos platforms. The problem arises from the following sequence. 1. In dwc3_gadget_suspend, there is a chance of a timeout when moving the USB core to the halt state after clearing the run/stop bit by software. 2. In dwc3_core_exit, the event buffer is cleared regardless of the USB core's status, which may lead to an SMMU faults and other memory issues. if the USB core tries to access the event buffer address. To prevent this hardware quirk on Exynos platforms, this commit ensures that the event buffer address is not cleared by software when the USB core is active during runtime suspend by checking its status before clearing the buffer address.	5.5	More Details
CVE-2024-39385	Premiere Pro versions 24.5, 23.6.8 and earlier are affected by a Use After Free 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-2024-8775	A flaw was found in Ansible, where sensitive information stored in Ansible Vault files can be exposed in plaintext during the execution of a playbook. This occurs when using tasks such as include_vars to load vaulted variables without setting the no_log: true parameter, resulting in sensitive data being printed in the playbook output or logs. This can lead to the unintentional disclosure of secrets like passwords or API keys, compromising security and potentially allowing unauthorized access or actions.	5.5	More Details
CVE-2024-46709	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Fix prime with external buffers Make sure that for external buffers mapping goes through the dma_buf interface instead of trying to access pages directly. External buffers might not provide direct access to readable/writable pages so to make sure the bo's created from external dma_bufs can be read dma_buf interface has to be used. Fixes crashes in IGT's kms_prime with vgem. Regular desktop usage won't trigger this due to the fact that virtual machines will not have multiple GPUs but it enables better test coverage in IGT.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45182	An issue was discovered in WibuKey64.sys in WIBU-SYSTEMS WibuKey before v6.70 and fixed in v.6.70 An improper bounds check allows specially crafted packets to cause an arbitrary address read, resulting in Denial of Service.	5.5	More Details
CVE-2024-8864	A vulnerability has been found in composiohq composio up to 0.5.6 and classified as critical. Affected by this vulnerability is the function Calculator of the file python/composio/tools/local/mathematical/actions/calculator.py. The manipulation leads to code injection. 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.	5.5	More Details
CVE-2024-8945	A vulnerability has been found in CodeCanyon RISE Ultimate Project Manager 3.7.0 and classified as critical. This vulnerability affects unknown code of the file /index.php/dashboard/save. 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. It is recommended to upgrade the affected component.	5.5	More Details
CVE-2024-46708	In the Linux kernel, the following vulnerability has been resolved: pinctrl: qcom: x1e80100: Fix special pin offsets Remove the erroneus 0x100000 offset to prevent the boards from crashing on pin state setting, as well as for the intended state changes to take effect.	5.5	More Details
CVE-2024-45009	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: only decrement add_addr_accepted for MPJ req Adding the following warning ... WARN_ON_ONCE(msk->pm.add_addr_accepted == 0) ... before decrementing the add_addr_accepted counter helped to find a bug when running the "remove single subflow" subtest from the mptcp_join.sh selftest. Removing a 'subflow' endpoint will first trigger a RM_ADDR, then the subflow closure. Before this patch, and upon the reception of the RM_ADDR, the other peer will then try to decrement this add_addr_accepted. That's not correct because the attached subflows have not been created upon the reception of an ADD_ADDR. A way to solve that is to decrement the counter only if the attached subflow was an MP_JOIN to a remote id that was not 0, and initiated by the host receiving the RM_ADDR.	5.5	More Details
CVE-2024-45010	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: only mark 'subflow' endp as available Adding the following warning ... WARN_ON_ONCE(msk->pm.local_addr_used == 0) ... before decrementing the local_addr_used counter helped to find a bug when running the "remove single address" subtest from the mptcp_join.sh selftests. Removing a 'signal' endpoint will trigger the removal of all subflows linked to this endpoint via mptcp_pm_nl_rm_addr_or_subflow() with rm_type == MPTCP_MIB_RMSUBFLOW. This will decrement the local_addr_used counter, which is wrong in this case because this counter is linked to 'subflow' endpoints, and here it is a 'signal' endpoint that is being removed. Now, the counter is decremented, only if the ID is being used outside of mptcp_pm_nl_rm_addr_or_subflow(), only for 'subflow' endpoints, and if the ID is not 0 -- local_addr_used is not taking into account these ones. This marking of the ID as being available, and the decrement is done no matter if a subflow using this ID is currently available, because the subflow could have been closed before.	5.5	More Details
CVE-2024-41629	An issue in Texas Instruments Fusion Digital Power Designer v.7.10.1 allows a local attacker to obtain sensitive information via the plaintext storage of credentials	5.5	More Details
CVE-2024-8631	A privilege escalation issue has been discovered in GitLab EE affecting all versions starting from 16.6 prior to 17.1.7, from 17.2 prior to 17.2.5, and from 17.3 prior to 17.3.2. A user assigned the Admin Group Member custom role could have escalated their privileges to include other custom roles.	5.5	More Details
CVE-2024-45021	In the Linux kernel, the following vulnerability has been resolved: memcg_write_event_control(): fix a user-triggerable oops we are *not* guaranteed that anything past the terminating NUL is mapped (let alone initialized with anything sane).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45012	In the Linux kernel, the following vulnerability has been resolved: nouveau/firmware: use dma non-coherent allocator Currently, enabling SG_DEBUG in the kernel will cause nouveau to hit a BUG() on startup, when the iommu is enabled: kernel BUG at include/linux/scatterlist.h:187! invalid opcode: 0000 [#1] PREEMPT SMP NOPTI CPU: 7 PID: 930 Comm: (udev-worker) Not tainted 6.9.0-rc3Lyude-Test+ #30 Hardware name: MSI MS-7A39/A320M GAMING PRO (MS-7A39), BIOS 1.I0 01/22/2019 RIP: 0010:sg_init_one+0x85/0xa0 Code: 69 88 32 01 83 e1 03 f6 c3 03 75 20 a8 01 75 1e 48 09 cb 41 89 54 24 08 49 89 1c 24 41 89 6c 24 0c 5b 5d 41 5c e9 7b b9 88 00 <0f> 0b 0f 0b 0f 0b 48 8b 05 5e 46 9a 01 eb b2 66 66 2e 0f 1f 84 00 RSP: 0018:ffffa776017bf6a0 EFLAGS: 00010246 RAX: 0000000000000000 RBX: ffffa77600d87000 RCX: 000000000000002b RDX: 0000000000000001 RSI: 0000000000000000 RDI: ffffa77680d87000 RBP: 000000000000e000 R08: 0000000000000000 R09: 0000000000000000 R10: ffff98f4c46aa508 R11: 0000000000000000 R12: ffff98f4c46aa508 R13: ffff98f4c46aa008 R14: ffffa77600d4a000 R15: ffffa77600d4a018 FS: 00007feeb5aae980(0000) GS:ffff98f5c4dc0000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f22cb9a4520 CR3: 00000001043ba000 CR4: 00000000003506f0 Call Trace: <TASK> ? die+0x36/0x90 ? do_trap+0xdd/0x100 ? sg_init_one+0x85/0xa0 ? do_error_trap+0x65/0x80 ? sg_init_one+0x85/0xa0 ? exc_invalid_op+0x50/0x70 ? sg_init_one+0x85/0xa0 ? asm_exc_invalid_op+0x1a/0x20 ? sg_init_one+0x85/0xa0 nvkm_firmware_ctor+0x14a/0x250 [nouveau] nvkm_falcon_fw_ctor+0x42/0x70 [nouveau] ga102_gsp_booter_ctor+0xb4/0x1a0 [nouveau] r535_gsp_oneinit+0xb3/0x15f0 [nouveau] ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? nvkm_udevice_new+0x95/0x140 [nouveau] ? srso_return_thunk+0x5/0x5f ? srso_return_thunk+0x5/0x5f ? ktime_get+0x47/0xb0 Fix this by using the non-coherent allocator instead, I think there might be a better answer to this, but it involve ripping up some of APIs using sg lists.	5.5	More Details
CVE-2024-46678	In the Linux kernel, the following vulnerability has been resolved: bonding: change ipsec_lock from spin lock to mutex In the cited commit, bond->ipsec_lock is added to protect ipsec_list, hence xdo_dev_state_add and xdo_dev_state_delete are called inside this lock. As ipsec_lock is a spin lock and such xfrmdev ops may sleep, "scheduling while atomic" will be triggered when changing bond's active slave. [101.055189] BUG: scheduling while atomic: bash/902/0x00000200 [101.055726] Modules linked in: [101.058211] CPU: 3 PID: 902 Comm: bash Not tainted 6.9.0-rc4+ #1 [101.058760] Hardware name: [101.059434] Call Trace: [101.059436] <TASK> [101.060873] dump_stack_lvl+0x51/0x60 [101.061275] __schedule_bug+0x4e/0x60 [101.061682] __schedule+0x612/0x7c0 [101.062078] ? __mod_timer+0x25c/0x370 [101.062486] schedule+0x25/0xd0 [101.062845] schedule_timeout+0x77/0xf0 [101.063265] ? asm_common_interrupt+0x22/0x40 [101.063724] ? __bpf_trace_itimer_state+0x10/0x10 [101.064215] __wait_for_common+0x87/0x190 [101.064648] ? usleep_range_state+0x90/0x90 [101.065091] cmd_exec+0x437/0xb20 [mlx5_core] [101.065569] mlx5_cmd_do+0x1e/0x40 [mlx5_core] [101.066051] mlx5_cmd_exec+0x18/0x30 [mlx5_core] [101.066552] mlx5_crypto_create_dek_key+0xea/0x120 [mlx5_core] [101.067163] ? bonding_sysfs_store_option+0x4d/0x80 [bonding] [101.067738] ? kmalloc_trace+0x4d/0x350 [101.068156] mlx5_ipsec_create_sa_ctx+0x33/0x100 [mlx5_core] [101.068747] mlx5e_xfrm_add_state+0x47b/0xaa0 [mlx5_core] [101.069312] bond_change_active_slave+0x392/0x900 [bonding] [101.069868] bond_option_active_slave_set+0x1c2/0x240 [bonding] [101.070454] __bond_opt_set+0xa6/0x430 [bonding] [101.070935] __bond_opt_set_notify+0x2f/0x90 [bonding] [101.071453] bond_opt_tryset_rtnl+0x72/0xb0 [bonding] [101.071965] bonding_sysfs_store_option+0x4d/0x80 [bonding] [101.072567] kernfs_fop_write_iter+0x10c/0x1a0 [101.073033] vfs_write+0x2d8/0x400 [101.073416] ? alloc_fd+0x48/0x180 [101.073798] ksys_write+0x5f/0xe0 [101.074175] do_syscall_64+0x52/0x110 [101.074576] entry_SYSCALL_64_after_hwframe+0x4b/0x53 As bond_ipsec_add_sa_all and bond_ipsec_del_sa_all are only called from bond_change_active_slave, which requires holding the RTNL lock. And bond_ipsec_add_sa and bond_ipsec_del_sa are xfrm state xdo_dev_state_add and xdo_dev_state_delete APIs, which are in user context. So ipsec_lock doesn't have to be spin lock, change it to mutex, and thus the above issue can be resolved.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46680	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btnxpuart: Fix random crash seen while removing driver This fixes the random kernel crash seen while removing the driver, when running the load/unload test over multiple iterations. 1) modprobe btnxpuart 2) hciconfig hci0 reset 3) hciconfig (check hci0 interface up with valid BD address) 4) modprobe -r btnxpuart Repeat steps 1 to 4 The ps_wakeup() call in btnxpuart_close() schedules the psdata->work(), which gets scheduled after module is removed, causing a kernel crash. This hidden issue got highlighted after enabling Power Save by default in 4183a7be7700 (Bluetooth: btnxpuart: Enable Power Save feature on startup) The new ps_cleanup() deasserts UART break immediately while closing serdev device, cancels any scheduled ps_work and destroys the ps_lock mutex. [85.884604] Unable to handle kernel paging request at virtual address ffffd4a61638f258 [85.884624] Mem abort info: [85.884625] ESR = 0x0000000086000007 [85.884628] EC = 0x21: IABT (current EL), IL = 32 bits [85.884633] SET = 0, FnV = 0 [85.884636] EA = 0, S1PTW = 0 [85.884638] FSC = 0x07: level 3 translation fault [85.884642] swapper pgtable: 4k pages, 48-bit VAs, pgdp=0000000041dd0000 [85.884646] [ffffd4a61638f258] pgd=1000000095fff003, p4d=1000000095fff003, pud=100000004823d003, pmd=100000004823e003, pte=0000000000000000 [85.884662] Internal error: Oops: 0000000086000007 [#1] PREEMPT SMP [85.890932] Modules linked in: algif_hash algif_skcipher af_alg overlay fsl_jr_uio caam_jr caamkeyblob_desc caamhash_desc caamalg_desc crypto_engine authenc libdes crct10dif_ce polyval_ce polyval_generic snd_soc_imx_spdif snd_soc_imx_card snd_soc_ak5558 snd_soc_ak4458 caam secvio error snd_soc_fsl_spdif snd_soc_fsl_micfil snd_soc_fsl_sai snd_soc_fsl_utils gpio_ir_recv rc_core fuse [last unloaded: btnxpuart(O)] [85.927297] CPU: 1 PID: 67 Comm: kworker/1:3 Tainted: G O 6.1.36+g937b1be4345a #1 [85.936176] Hardware name: FSL i.MX8MM EVK board (DT) [85.936182] Workqueue: events 0xffffd4a61638f380 [85.936198] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [85.952817] pc : 0xffffd4a61638f258 [85.952823] lr : 0xffffd4a61638f258 [85.952827] sp : ffff8000084fbd70 [85.952829] x29: ffff8000084fbd70 x28: 0000000000000000 x27: 0000000000000000 [85.963112] x26: ffffd4a69133f000 x25: ffff4bf1c8540990 x24: ffff4bf215b87305 [85.963119] x23: ffff4bf215b87300 x22: ffff4bf1c85409d0 x21: ffff4bf1c8540970 [85.977382] x20: 0000000000000000 x19: ffff4bf1c8540880 x18: 0000000000000000 [85.977391] x17: 0000000000000000 x16: 0000000000000133 x15: 0000ffffe2217090 [85.977399] x14: 0000000000000001 x13: 0000000000000133 x12: 0000000000000139 [85.977407] x11: 0000000000000001 x10: 0000000000000a60 x9 : ffff8000084fbc50 [85.977417] x8 : ffff4bf215b7d000 x7 : ffff4bf215b83b40 x6 : 00000000000003e8 [85.977424] x5 : 00000000410fd030 x4 : 0000000000000000 x3 : 0000000000000000 [85.977432] x2 : 0000000000000000 x1 : ffff4bf1c4265880 x0 : 0000000000000000 [85.977443] Call trace: [85.977446] 0xffffd4a61638f258 [85.977451] 0xffffd4a61638f3e8 [85.977455] process_one_work+0x1d4/0x330 [85.977464] worker_thread+0x6c/0x430 [85.977471] kthread+0x108/0x10c [85.977476] ret_from_fork+0x10/0x20 [85.977488] Code: bad PC value [85.977491] ---[end trace 0000000000000000]--- Preset since v6.9.11	5.5	More Details
CVE-2024-46681	In the Linux kernel, the following vulnerability has been resolved: pktgen: use cpus_read_lock() in pg_net_init() I have seen the WARN_ON(smp_processor_id() != cpu) firing in pktgen_thread_worker() during tests. We must use cpus_read_lock()/cpus_read_unlock() around the for_each_online_cpu(cpu) loop. While we are at it use WARN_ON_ONCE() to avoid a possible syslog flood.	5.5	More Details
CVE-2024-46682	In the Linux kernel, the following vulnerability has been resolved: nfsd: prevent panic for nfsv4.0 closed files in nfs4_show_open Prior to commit 3f29cc82a84c ("nfsd: split sc_status out of sc_type") states_show() relied on sc_type field to be of valid type before calling into a subfunction to show content of a particular stateid. From that commit, we split the validity of the stateid into sc_status and no longer changed sc_type to 0 while unhashing the stateid. This resulted in kernel oopsing for nfsv4.0 opens that stay around and in nfs4_show_open() would derefence sc_file which was NULL. Instead, for closed open stateids forgo displaying information that relies of having a valid sc_file. To reproduce: mount the server with 4.0, read and close a file and then on the server cat /proc/fs/nfsd/clients/2/states [513.590804] Call trace: [513.590925] _raw_spin_lock+0xcc/0x160 [513.591119] nfs4_show_open+0x78/0x2c0 [nfsd] [513.591412] states_show+0x44c/0x488 [nfsd] [513.591681] seq_read_iter+0x5d8/0x760 [513.591896] seq_read+0x188/0x208 [513.592075] vfs_read+0x148/0x470 [513.592241] ksys_read+0xcc/0x178	5.5	More Details
CVE-2024-40656	In handleCreateConferenceComplete of ConnectionServiceWrapper.java, there is a possible way to reveal images across users due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	5.5	More Details
CVE-2024-40659	In getRegistration of RemoteProvisioningService.java, there is a possible way to permanently disable the AndroidKeyStore key generation feature by updating the attestation keys of all installed apps due to improper input validation. 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 Number	Description	Base Score	Reference
CVE-2024-46698	In the Linux kernel, the following vulnerability has been resolved: video/aperture: optionally match the device in sysfb_disable() In aperture_remove_conflicting_pci_devices(), we currently only call sysfb_disable() on vga class devices. This leads to the following problem when the pimary device is not VGA compatible: 1. A PCI device with a non-VGA class is the boot display 2. That device is probed first and it is not a VGA device so sysfb_disable() is not called, but the device resources are freed by aperture_detach_platform_device() 3. Non-primary GPU has a VGA class and it ends up calling sysfb_disable() 4. NULL pointer dereference via sysfb_disable() since the resources have already been freed by aperture_detach_platform_device() when it was called by the other device. Fix this by passing a device pointer to sysfb_disable() and checking the device to determine if we should execute it or not. v2: Fix build when CONFIG_SCREEN_INFO is not set v3: Move device check into the mutex Drop primary variable in aperture_remove_conflicting_pci_devices() Drop __init on pci sysfb_pci_dev_is_enabled()	5.5	More Details
CVE-2024-46697	In the Linux kernel, the following vulnerability has been resolved: nfsd: ensure that nfsd4_fattr_args.context is zeroed out If nfsd4_encode_fattr4 ends up doing a "goto out" before we get to checking for the security label, then args.context will be set to uninitialized junk on the stack, which we'll then try to free. Initialize it early.	5.5	More Details
CVE-2024-46694	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: avoid using null object of framebuffer Instead of using state->fb->obj[0] directly, get object from framebuffer by calling drm_gem_fb_get_obj() and return error code when object is null to avoid using null object of framebuffer. (cherry picked from commit 73dd0ad9e5dad53766ea3e631303430116f834b3)	5.5	More Details
CVE-2024-46712	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Disable coherent dumb buffers without 3d Coherent surfaces make only sense if the host renders to them using accelerated apis. Without 3d the entire content of dumb buffers stays in the guest making all of the extra work they're doing to synchronize between guest and host useless. Configurations without 3d also tend to run with very low graphics memory limits. The pinned console fb, mob cursors and graphical login manager tend to run out of 16MB graphics memory that those guests use. Fix it by making sure the coherent dumb buffers are only used on configs with 3d enabled.	5.5	More Details
CVE-2024-46692	In the Linux kernel, the following vulnerability has been resolved: firmware: qcom: scm: Mark get_wq_ctx() as atomic call Currently get_wq_ctx() is wrongly configured as a standard call. When two SMC calls are in sleep and one SMC wakes up, it calls get_wq_ctx() to resume the corresponding sleeping thread. But if get_wq_ctx() is interrupted, goes to sleep and another SMC call is waiting to be allocated a waitq context, it leads to a deadlock. To avoid this get_wq_ctx() must be an atomic call and can't be a standard SMC call. Hence mark get_wq_ctx() as a fast call.	5.5	More Details
CVE-2024-46691	In the Linux kernel, the following vulnerability has been resolved: usb: typec: ucsi: Move unregister out of atomic section Commit '9329933699b3 ("soc: qcom: pmic_glink: Make client-lock non-sleeping")' moved the pmic_glink client list under a spinlock, as it is accessed by the rpmsg/glink callback, which in turn is invoked from IRQ context. This means that ucsi_unregister() is now called from atomic context, which isn't feasible as it's expecting a sleepable context. An effort is under way to get GLINK to invoke its callbacks in a sleepable context, but until then lets schedule the unregistration. A side effect of this is that ucsi_unregister() can now happen after the remote processor, and thereby the communication link with it, is gone. pmic_glink_send() is amended with a check to avoid the resulting NULL pointer dereference. This does however result in the user being informed about this error by the following entry in the kernel log: ucsi_glink.pmic_glink_ucsi pmic_glink.ucsi.0: failed to send UCSI write request: -5	5.5	More Details
CVE-2024-46690	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix nfsd4_deleg_getattr_conflict in presence of third party lease It is not safe to dereference fl->c.flc_owner without first confirming fl->fl_lmops is the expected manager. nfsd4_deleg_getattr_conflict() tests fl_lmops but largely ignores the result and assumes that flc_owner is an nfs4_delegation anyway. This is wrong. With this patch we restore the "!= &nfsd_lease_mng_ops" case to behave as it did before the change mentioned below. This is the same as the current code, but without any reference to a possible delegation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46689	In the Linux kernel, the following vulnerability has been resolved: soc: qcom: cmd-db: Map shared memory as WC, not WB Linux does not write into cmd-db region. This region of memory is write protected by XPU. XPU may sometime falsely detect clean cache eviction as "write" into the write protected region leading to secure interrupt which causes an endless loop somewhere in Trust Zone. The only reason it is working right now is because Qualcomm Hypervisor maps the same region as Non-Cacheable memory in Stage 2 translation tables. The issue manifests if we want to use another hypervisor (like Xen or KVM), which does not know anything about those specific mappings. Changing the mapping of cmd-db memory from MEMREMAP_WB to MEMREMAP_WT/WC removes dependency on correct mappings in Stage 2 tables. This patch fixes the issue by updating the mapping to MEMREMAP_WC. I tested this on SA8155P with Xen.	5.5	More Details
CVE-2024-46688	In the Linux kernel, the following vulnerability has been resolved: erofs: fix out-of-bound access when z_erofs_gbuf_growsize() partially fails If z_erofs_gbuf_growsize() partially fails on a global buffer due to memory allocation failure or fault injection (as reported by syzbot [1]), new pages need to be freed by comparing to the existing pages to avoid memory leaks. However, the old gbuf->pages[] array may not be large enough, which can lead to null-ptr-deref or out-of-bound access. Fix this by checking against gbuf->nrpages in advance. [1] https://lore.kernel.org/r/000000000000f7b96e062018c6e3@google.com	5.5	More Details
CVE-2024-46686	In the Linux kernel, the following vulnerability has been resolved: smb/client: avoid dereferencing rdata=NULL in smb2_new_read_req() This happens when called from SMB2_read() while using rdma and reaching the rdma_readwrite_threshold.	5.5	More Details
CVE-2024-39382	After Effects versions 23.6.6, 24.5 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-2024-46685	In the Linux kernel, the following vulnerability has been resolved: pinctrl: single: fix potential NULL dereference in pcs_get_function() pinmux_generic_get_function() can return NULL and the pointer 'function' was dereferenced without checking against NULL. Add checking of pointer 'function' in pcs_get_function(). Found by code review.	5.5	More Details
CVE-2024-46684	In the Linux kernel, the following vulnerability has been resolved: binfmt_elf_fdpic: fix AUXV size calculation when ELF_HWCAP2 is defined create_elf_fdpic_tables() does not correctly account the space for the AUX vector when an architecture has ELF_HWCAP2 defined. Prior to the commit 10e29251be0e ("binfmt_elf_fdpic: fix /proc/<pid>/auxv") it resulted in the last entry of the AUX vector being set to zero, but with that change it results in a kernel BUG. Fix that by adding one to the number of AUXV entries (nitems) when ELF_HWCAP2 is defined.	5.5	More Details
CVE-2024-41870	Media Encoder versions 24.5, 23.6.8 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-2024-45011	In the Linux kernel, the following vulnerability has been resolved: char: xillybus: Check USB endpoints when probing device Ensure, as the driver probes the device, that all endpoints that the driver may attempt to access exist and are of the correct type. All XillyUSB devices must have a Bulk IN and Bulk OUT endpoint at address 1. This is verified in xillyusb_setup_base_eps(). On top of that, a XillyUSB device may have additional Bulk OUT endpoints. The information about these endpoints' addresses is deduced from a data structure (the IDT) that the driver fetches from the device while probing it. These endpoints are checked in setup_channels(). A XillyUSB device never has more than one IN endpoint, as all data towards the host is multiplexed in this single Bulk IN endpoint. This is why setup_channels() only checks OUT endpoints.	5.5	More Details
CVE-2024-46702	In the Linux kernel, the following vulnerability has been resolved: thunderbolt: Mark XDomain as unplugged when router is removed I noticed that when we do discrete host router NVM upgrade and it gets hot-removed from the PCIe side as a result of NVM firmware authentication, if there is another host connected with enabled paths we hang in tearing them down. This is due to fact that the Thunderbolt networking driver also tries to cleanup the paths and ends up blocking in tb_disconnect_xdomain_paths() waiting for the domain lock. However, at this point we already cleaned the paths in tb_stop() so there is really no need for tb_disconnect_xdomain_paths() to do that anymore. Furthermore it already checks if the XDomain is unplugged and bails out early so take advantage of that and mark the XDomain as unplugged when we remove the parent router.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6700	Pega Platform versions 8.1 to Infinity 24.1.2 are affected by an XSS issue with App name.	5.5	More Details
CVE-2024-45017	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix IPsec RoCE MPV trace call Prevent the call trace below from happening, by not allowing IPsec creation over a slave, if master device doesn't support IPsec. WARNING: CPU: 44 PID: 16136 at kernel/locking/rwsem.c:240 down_read+0x75/0x94 Modules linked in: esp4_offload esp4 act_mirred act_vlan cls_flower sch_ingress mlx5_vdpa vringh vhost_iotlb vdpa mst_pciconf(OE) nfsv3 nfs_acl nfs lockd grace fscache netfs xt_CHECKSUM xt_MASQUERADE xt_conntrack ipt_REJECT nf_reject_ipv4 nft_compat nft_counter nft_chain_nat nf_nat nf_conntrack nf_defrag_ipv6 nf_defrag_ipv4 rfkill cuse fuse rpcrdma sunrpc rdma_ucm ib_srpt ib_isert iscsi_target_mod target_core_mod ib_umad ib_iser libiscsi scsi_transport_iscsi rdma_cm ib_ipoib iw_cm ib_cm ipmi_ssif intel_rapl_msr intel_rapl_common amd64_edac edac_mce_amd kvm_amd kvm irqbypass crct10dif_pclmul crc32_pclmul mlx5_ib ghash_clmulni_intel sha1_ssse3 dell_smbios ib_uverbs aesni_intel crypto_simd dcdbas wmi_bmof dell_wmi_descriptor cryptd pcspkr ib_core acpi_ipmi sp5100_tco ccp i2c_piix4 ipmi_si ptdma k10temp ipmi_devintf ipmi_msghandler acpi_power_meter acpi_cpufreq ext4 mbcache jbd2 sd_mod t10_pi sg mgag200 drm_kms_helper syscopyarea sysfillrect mlx5_core sysimgblt fb_sys_fops cec ahci libahci mlxfw drm pci_hyperv_intf libata tg3 sha256_ssse3 tls megaraid_sas i2c_algo_bit psample wmi dm_mirror dm_region_hash dm_log dm_mod [last unloaded: mst_pci] CPU: 44 PID: 16136 Comm: kworker/44:3 Kdump: loaded Tainted: GOE 5.15.0-20240509.el8uek.uek7_u3_update_v6.6_ipsec_bf.x86_64 #2 Hardware name: Dell Inc. PowerEdge R7525/074H08, BIOS 2.0.3 01/15/2021 Workqueue: events xfrm_state_gc_task RIP: 0010:down_read+0x75/0x94 Code: 00 48 8b 45 08 65 48 8b 14 25 80 fc 01 00 83 e0 02 48 09 d0 48 83 c8 01 48 89 45 08 5d 31 c0 89 c2 89 c6 89 c7 e9 cb 88 3b 00 <0f> 0b 48 8b 45 08 a8 01 74 b2 a8 02 75 ae 48 89 c2 48 83 ca 02 f0 RSP: 0018:ffffb26387773da8 EFLAGS: 00010282 RAX: 0000000000000000 RBX: ffffa08b658af900 RCX: 0000000000000001 RDX: 0000000000000000 RSI: ff886bc5e1366f2f RDI: 0000000000000000 RBP: ffffa08b658af940 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffa0a9bfb31540 R13: ffffa0a9bfb37900 R14: 0000000000000000 R15: ffffa0a9bfb37905 FS: 0000000000000000(0000) GS:ffffa0a9bfb00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000055a45ed814e8 CR3: 000000109038a000 CR4: 0000000000350ee0 Call Trace: <TASK> ? show_trace_log_lvl+0x1d6/0x2f9 ? show_trace_log_lvl+0x1d6/0x2f9 ? mlx5_devcom_for_each_peer_begin+0x29/0x60 [mlx5_core] ? down_read+0x75/0x94 ? __warn+0x80/0x113 ? down_read+0x75/0x94 ? report_bug+0xa4/0x11d ? handle_bug+0x35/0x8b ? exc_invalid_op+0x14/0x75 ? asm_exc_invalid_op+0x16/0x1b ? down_read+0x75/0x94 ? down_read+0xe/0x94 mlx5_devcom_for_each_peer_begin+0x29/0x60 [mlx5_core] mlx5_ipsec_fs_roce_tx_destroy+0xb1/0x130 [mlx5_core] tx_destroy+0x1b/0xc0 [mlx5_core] tx_ft_put+0x53/0xc0 [mlx5_core] mlx5e_xfrm_free_state+0x45/0x90 [mlx5_core] ___xfrm_state_destroy+0x10f/0x1a2 xfrm_state_gc_task+0x81/0xa9 process_one_work+0x1f1/0x3c6 worker_thread+0x53/0x3e4 ? process_one_work.cold+0x46/0x3c kthread+0x127/0x144 ? set_kthread_struct+0x60/0x52 ret_from_fork+0x22/0x2d </TASK> ---[end trace 5ef7896144d398e1]---	5.5	More Details
CVE-2024-45016	In the Linux kernel, the following vulnerability has been resolved: netem: fix return value if duplicate enqueue fails There is a bug in netem_enqueue() introduced by commit 5845f706388a ("net: netem: fix skb length BUG_ON in __skb_to_sgvec") that can lead to a use-after-free. This commit made netem_enqueue() always return NET_XMIT_SUCCESS when a packet is duplicated, which can cause the parent qdisc's q.qlen to be mistakenly incremented. When this happens qlen_notify() may be skipped on the parent during destruction, leaving a dangling pointer for some classful qdiscs like DRR. There are two ways for the bug happen: - If the duplicated packet is dropped by rootq->enqueue() and then the original packet is also dropped. - If rootq->enqueue() sends the duplicated packet to a different qdisc and the original packet is dropped. In both cases NET_XMIT_SUCCESS is returned even though no packets are enqueued at the netem qdisc. The fix is to defer the enqueue of the duplicate packet until after the original packet has been guaranteed to return NET_XMIT_SUCCESS.	5.5	More Details
CVE-2024-45018	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: initialise extack before use Fix missing initialisation of extack in flow offload.	5.5	More Details
CVE-2024-38380	This vulnerability occurs when user-supplied input is improperly sanitized and then reflected back to the user's browser, allowing an attacker to execute arbitrary JavaScript in the context of the victim's browser session.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45015	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dpu: move dpu_encoder's connector assignment to atomic_enable() For cases where the crtc's connectors_changed was set without enable/active getting toggled , there is an atomic_enable() call followed by an atomic_disable() but without an atomic_mode_set(). This results in a NULL ptr access for the dpu_encoder_get_drm_fmt() call in the atomic_enable() as the dpu_encoder's connector was cleared in the atomic_disable() but not re-assigned as there was no atomic_mode_set() call. Fix the NULL ptr access by moving the assignment for atomic_enable() and also use drm_atomic_get_new_connector_for_encoder() to get the connector from the atomic_state. Patchwork: https://patchwork.freedesktop.org/patch/606729/	5.5	More Details
CVE-2024-41872	Media Encoder versions 24.5, 23.6.8 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-2024-41871	Media Encoder versions 24.5, 23.6.8 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-2024-45014	In the Linux kernel, the following vulnerability has been resolved: s390/boot: Avoid possible physmem_info segment corruption When physical memory for the kernel image is allocated it does not consider extra memory required for offsetting the image start to match it with the lower 20 bits of KASLR virtual base address. That might lead to kernel access beyond its memory range.	5.5	More Details
CVE-2024-44181	An issue was addressed with improved handling of temporary files. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to read sensitive location information.	5.5	More Details
CVE-2024-46701	In the Linux kernel, the following vulnerability has been resolved: libfs: fix infinite directory reads for offset dir After we switch tmpfs dir operations from simple_dir_operations to simple_offset_dir_operations, every rename happened will fill new dentry to dest dir's maple tree(&SHMEM_I(inode)->dir_offsets->mt) with a free key starting with octx->newx_offset, and then set newx_offset equals to free key + 1. This will lead to infinite readdir combine with rename happened at the same time, which fail generic/736 in xfstests(detail show as below). 1. create 5000 files(1 2 3...) under one dir 2. call readdir(man 3 readdir) once, and get one entry 3. rename(entry, "TEMPFILE"), then rename("TEMPFILE", entry) 4. loop 2~3, until readdir return nothing or we loop too many times(tmpfs break test with the second condition) We choose the same logic what commit 9b378f6ad48cf ("btrfs: fix infinite directory reads") to fix it, record the last_index when we open dir, and do not emit the entry which index >= last_index. The file->private_data now used in offset dir can use directly to do this, and we also update the last_index when we llseek the dir file. [brauner: only update last_index after seek when offset is zero like Jan suggested]	5.5	More Details
CVE-2024-41873	Media Encoder versions 24.5, 23.6.8 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-2024-6701	Pega Platform versions 8.1 to Infinity 24.1.2 are affected by an XSS issue with case type.	5.5	More Details
CVE-2024-45013	In the Linux kernel, the following vulnerability has been resolved: nvme: move stopping keep-alive into nvme_uninit_ctrl() Commit 4733b65d82bd ("nvme: start keep-alive after admin queue setup") moves starting keep-alive from nvme_start_ctrl() into nvme_init_ctrl_finish(), but don't move stopping keep-alive into nvme_uninit_ctrl(), so keep-alive work can be started and keep pending after failing to start controller, finally use-after-free is triggered if nvme host driver is unloaded. This patch fixes kernel panic when running nvme/004 in case that connection failure is triggered, by moving stopping keep-alive into nvme_uninit_ctrl(). This way is reasonable because keep-alive is now started in nvme_init_ctrl_finish().	5.5	More Details
CVE-2024-45019	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Take state lock during tx timeout reporter mlx5e_safe_reopen_channels() requires the state lock taken. The referenced changed in the Fixes tag removed the lock to fix another issue. This patch adds it back but at a later point (when calling mlx5e_safe_reopen_channels()) to avoid the deadlock referenced in the Fixes tag.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45020	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix a kernel verifier crash in stacksafe() Daniel Hodges reported a kernel verifier crash when playing with sched-ext. Further investigation shows that the crash is due to invalid memory access in stacksafe(). More specifically, it is the following code: if (exact != NOT_EXACT && old->stack[spi].slot_type[i % BPF_REG_SIZE] != cur->stack[spi].slot_type[i % BPF_REG_SIZE]) return false; The 'i' iterates old->allocated_stack. If cur->allocated_stack < old->allocated_stack the out-of-bound access will happen. To fix the issue add 'i >= cur->allocated_stack' check such that if the condition is true, stacksafe() should fail. Otherwise, cur->stack[spi].slot_type[i % BPF_REG_SIZE] memory access is legal.	5.5	More Details
CVE-2024-46703	In the Linux kernel, the following vulnerability has been resolved: Revert "serial: 8250_omap: Set the console genpd always on if no console suspend" This reverts commit 68e6939ea9ec3d6579eadeab16060339cdeaf940. Kevin reported that this causes a crash during suspend on platforms that dont use PM domains.	5.5	More Details
CVE-2024-8875	A vulnerability classified as critical was found in vedees wcms up to 0.3.2. Affected by this vulnerability is an unknown functionality of the file /wex/finder.php. The manipulation of the argument p leads to path traversal. 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.	5.4	More Details
CVE-2021-22503	Possible Improper Neutralization of Input During Web Page Generation Vulnerability in eDirectory has been discovered in OpenText™ eDirectory 9.2.3.0000.	5.4	More Details
CVE-2021-38131	Possible Cross-Site Scripting (XSS) Vulnerability in eDirectory has been discovered in OpenText™ eDirectory 9.2.5.0000.	5.4	More Details
CVE-2024-5416	The Elementor Website Builder – More than Just a Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the url parameter of multiple widgets in all versions up to, and including, 3.23.4 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 Elementor Editor pages. This was partially patched in version 3.23.2.	5.4	More Details
CVE-2024-39910	decidim is a Free Open-Source participatory democracy, citizen participation and open government for cities and organizations. The WYSWYG editor QuillJS is subject to potential XSS attach in case the attacker manages to modify the HTML before being uploaded to the server. The attacker is able to change e.g. to <svg onload=alert('XSS')> if they know how to craft these requests themselves. This issue has been addressed in release version 0.27.7. All users are advised to upgrade. Users unable to upgrade should review the user accounts that have access to the admin panel (i.e. general Administrators, and participatory space's Administrators) and remove access to them if they don't need it. Disable the "Enable rich text editor for participants" setting in the admin dashboard	5.4	More Details
CVE-2024-8043	The Vikinghammer Tweet WordPress plugin through 0.2.4 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	5.4	More Details
CVE-2024-8051	The Special Feed Items WordPress plugin through 1.0.1 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	5.4	More Details
CVE-2024-8092	The Accordion Image Menu WordPress plugin through 3.1.3 does not have CSRF check in some places, and is missing sanitisation as well as escaping, which could allow attackers to make logged in admin add Stored XSS payloads via a CSRF attack.	5.4	More Details
CVE-2023-3410	The Bricks theme for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘customTag' attribute in versions up to, and including, 1.10.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with access to the Bricks Builder (admin-only by default), to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This becomes more of an issue when Bricks Builder access is granted to lower-privileged users.	5.4	More Details
CVE-2024-8750	Cross-site Scripting (XSS) vulnerability in idoit pro version 28. This vulnerability allows an attacker to retrieve session details of an authenticated user due to lack of proper sanitization of the following parameters (id,lang,mNavID,name,pID,treeNode,type,view).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44851	A stored cross-site scripting (XSS) vulnerability in the Discussion section of Perfex CRM v1.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Content parameter.	5.4	More Details
CVE-2024-22013	U-Boot environment is read from unauthenticated partition.	5.3	More Details
CVE-2023-43753	Improper conditions check in some Intel(R) Processors with Intel(R) SGX may allow a privileged user to potentially enable information disclosure via local access.	5.3	More Details
CVE-2024-7727	The HTML5 Video Player – mp4 Video Player Plugin and Block plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on multiple functions called via the 'h5vp_ajax_handler' ajax action in all versions up to, and including, 2.5.32. This makes it possible for unauthenticated attackers to call these functions to manipulate data.	5.3	More Details
CVE-2024-24968	Improper finite state machines (FSMs) in hardware logic in some Intel(R) Processors may allow an privileged user to potentially enable a denial of service via local access.	5.3	More Details
CVE-2024-23984	Observable discrepancy in RAPL interface for some Intel(R) Processors may allow a privileged user to potentially enable information disclosure via local access.	5.3	More Details
CVE-2024-8692	A vulnerability classified as critical was found in TDuckCloud TDuckPro up to 6.3. Affected by this vulnerability is an unknown functionality. The manipulation leads to weak password recovery. 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.	5.3	More Details
CVE-2024-1578	The MiCard PLUS Ci and MiCard PLUS BLE reader products developed by rf IDEAS and rebranded by NT-ware have a firmware fault that may result in characters randomly being dropped from some ID card reads, which would result in the wrong ID card number being assigned during ID card self-registration and might result in failed login attempts for end-users. Random characters being dropped from ID card numbers compromises the uniqueness of ID cards that can, therefore, result in a security issue if the users are using the ‘ID card self-registration’ function.	5.3	More Details
CVE-2021-38132	Possible External Service Interaction attack in eDirectory has been discovered in OpenText™ eDirectory. This impact all version before 9.2.6.0000.	5.3	More Details
CVE-2024-40852	This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 18 and iPadOS 18. An attacker may be able to see recent photos without authentication in Assistive Access.	5.3	More Details
CVE-2024-2743	An issue was discovered in GitLab-EE starting with version 13.3 before 17.1.7, 17.2 before 17.2.5, and 17.3 before 17.3.2 that would allow an attacker to modify an on-demand DAST scan without permissions and leak variables.	5.3	More Details
CVE-2024-6544	The Custom Post Limits plugin for WordPress is vulnerable to full path disclosure in all versions up to, and including, 4.4.1. This is due to the plugin utilizing bootstrap and leaving test files with display_errors on. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2024-45384	Padding Oracle vulnerability in Apache Druid extension, druid-pac4j. This could allow an attacker to manipulate a pac4j session cookie. This issue affects Apache Druid versions 0.18.0 through 30.0.0. Since the druid-pac4j extension is optional and disabled by default, Druid installations not using the druid-pac4j extension are not affected by this vulnerability. While we are not aware of a way to meaningfully exploit this flaw, we nevertheless recommend upgrading to version 30.0.1 or higher which fixes the issue and ensuring you have a strong druid.auth.pac4j.cookiePassphrase as a precaution.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20390	A vulnerability in the Dedicated XML Agent feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) on XML TCP listen port 38751. This vulnerability is due to a lack of proper error validation of ingress XML packets. An attacker could exploit this vulnerability by sending a sustained, crafted stream of XML traffic to a targeted device. A successful exploit could allow the attacker to cause XML TCP port 38751 to become unreachable while the attack traffic persists.	5.3	More Details
CVE-2024-45612	Contao is an Open Source CMS. In affected versions an untrusted user can inject insert tags into the canonical tag, which are then replaced on the web page (front end). Users are advised to update to Contao 4.13.49, 5.3.15 or 5.4.3. Users unable to upgrade should disable canonical tags in the root page settings.	5.3	More Details
CVE-2024-39613	Mattermost Desktop App versions <=5.8.0 fail to specify an absolute path when searching the cmd.exe file, which allows a local attacker who is able to put an cmd.exe file in the Downloads folder of a user's machine to cause remote code execution on that machine.	5.3	More Details
CVE-2024-8796	Under the default configuration, Devise-Two-Factor versions >= 2.2.0 & < 6.0.0 generate TOTP shared secrets that are 120 bits instead of the 128-bit minimum defined by RFC 4226. Using a shared secret shorter than the minimum to generate a multi-factor authentication code could make it easier for an attacker to guess the shared secret and generate valid TOTP codes.	5.3	More Details
CVE-2024-34336	User enumeration vulnerability in ORDAT FOSS-Online before v2.24.01 allows attackers to determine if an account exists in the application by comparing the server responses of the forgot password functionality.	5.3	More Details
CVE-2024-40862	A privacy issue was addressed by removing sensitive data. This issue is fixed in Xcode 16. An attacker may be able to determine the Apple ID of the owner of the computer.	5.3	More Details
CVE-2024-8711	A vulnerability, which was classified as problematic, has been found in SourceCodester Food Ordering Management System 1.0. Affected by this issue is some unknown functionality of the file /includes/. The manipulation leads to exposure of information through directory listing. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2024-44202	An authentication issue was addressed with improved state management. This issue is fixed in iOS 18 and iPadOS 18. Private Browsing tabs may be accessed without authentication.	5.3	More Details
CVE-2024-44127	This issue was addressed through improved state management. This issue is fixed in iOS 17.7 and iPadOS 17.7, iOS 18 and iPadOS 18. Private Browsing tabs may be accessed without authentication.	5.3	More Details
CVE-2022-3459	The WooCommerce Multiple Free Gift plugin for WordPress is vulnerable to gift manipulation in all versions up to, and including, 1.2.3. This is due to plugin not enforcing server-side checks on the products that can be added as a gift. This makes it possible for unauthenticated attackers to add non-gift items to their cart as a gift.	5.3	More Details
CVE-2024-6702	Pega Platform versions 8.1 to Infinity 24.1.2 are affected by an HTML Injection issue with Stage.	5.2	More Details
CVE-2024-34545	Improper input validation in some Intel(R) RAID Web Console software all versions may allow an authenticated user to potentially enable information disclosure via adjacent access.	5.2	More Details
CVE-2024-44685	Titan SFTP and Titan MFT Server 2.0.25.2426 and earlier have a vulnerability a vulnerability where sensitive information, including passwords, is exposed in clear text within the JSON response when configuring SMTP settings via the Web UI.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45800	Snappymail is an open source web-based email client. SnappyMail uses the `cleanHtml()` function to cleanup HTML and CSS in emails. Research discovered that the function has a few bugs which cause an mXSS exploit. Because the function allowed too many (invalid) HTML elements, it was possible (with incorrect markup) to trick the browser to "fix" the broken markup into valid markup. As a result a motivated attacker may be able to inject javascript. However, due to the default Content Security Policy the impact of the exploit is minimal. It could be possible to create an attack which leaks some data when loading images through the proxy. This way it might be possible to use the proxy to attack the local system, like with `http://localhost:5000/leak`. Another attack could be to load a JavaScript attachment of the email. This is very tricky as the email must link to every possible UID as each email has a unique UID which has a value between 1 and 18446744073709551615 **v2.38.0** and up now remove unsupported HTML elements which mitigates the issue. Users are advised to upgrade. Older versions can install an extension named "Security mXSS" as a mitigation. This will be available at the administration area at `/?admin#/packages`. **NOTE:** this extension can not "fix" malicious code in encrypted messages or (html) attachments as it can't manipulate the JavaScript code for this. It only protects normal message HTML.	5.0	More Details
CVE-2024-45383	A mishandling of IRP requests vulnerability exists in the HDAudBus_DMA interface of Microsoft High Definition Audio Bus Driver 10.0.19041.3636 (WinBuild.160101.0800). A specially crafted application can issue multiple IRP Complete requests which leads to a local denial-of-service. An attacker can execute malicious script/application to trigger this vulnerability.	5.0	More Details
CVE-2024-8869	A vulnerability classified as critical has been found in TOTOLINK A720R 4.1.5. Affected is the function exportOvpn. The manipulation leads to os command injection. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.	5.0	More Details
CVE-2024-46918	app/Controller/UserLoginProfilesController.php in MISP before 2.4.198 does not prevent an org admin from viewing sensitive login fields of another org admin in the same org.	4.9	More Details
CVE-2022-26322	Possible Insertion of Sensitive Information into Log File Vulnerability in Identity Manager has been discovered in OpenText™ Identity Manager REST Driver. This impact version before 1.1.2.0200.	4.9	More Details
CVE-2024-3899	The Gallery Plugin for WordPress WordPress plugin before 1.8.15 does not sanitise and escape some of its image settings, which could allow users with post-writing privilege such as Author to perform Cross-Site Scripting attacks.	4.8	More Details
CVE-2024-8660	Concrete CMS versions 9.0.0 through 9.3.3 are affected by a stored XSS vulnerability in the "Top Navigator Bar" block. Since the "Top Navigator Bar" output was not sufficiently sanitized, a rogue administrator could add a malicious payload that could be executed when targeted users visited the home page.The Concrete CMS Security Team gave this vulnerability a CVSS v4 score of 4.6 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N . This does not affect versions below 9.0.0 since they do not have the Top Navigator Bar Block. Thanks, Chu Quoc Khanh for reporting.	4.8	More Details
CVE-2024-44798	phpgurukul Bus Pass Management System 1.0 is vulnerable to Cross-site scripting (XSS) in /admin/pass-bwdates-reports-details.php via fromdate and todate parameters.	4.8	More Details
CVE-2024-7716	The Logo Slider WordPress plugin before 3.6.9 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2024-6887	The Giveaways and Contests by RafflePress WordPress plugin before 1.12.16 does not sanitise and escape some of its Giveaways settings, which could allow high privilege users such as editor and above to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-5170	The Logo Manager For Enamad WordPress plugin through 0.7.1 does not sanitise and escape in its widgets settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7133	The Floating Notification Bar, Sticky Menu on Scroll, Announcement Banner, and Sticky Header for Any WordPress plugin before 2.7.3 does not validate and escape some of its settings before outputting them back in the page, which could allow users with a high role to perform Stored Cross-Site Scripting attacks.	4.8	More Details
CVE-2024-8661	Concrete CMS versions 9.0.0 to 9.3.3 and below 8.5.19 are vulnerable to Stored XSS in the "Next&Previous Nav" block. A rogue administrator could add a malicious payload by executing it in the browsers of targeted users. The Concrete CMS Security Team gave this vulnerability a CVSS v4 score of 4.6 with vector CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:A/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N Since the "Next&Previous Nav" block output was not sufficiently sanitized, the malicious payload could be executed in the browsers of targeted users. Thanks, Chu Quoc Khanh for reporting.	4.8	More Details
CVE-2024-6493	The NinjaTeam Header Footer Custom Code WordPress plugin before 1.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-6850	The Carousel Slider WordPress plugin before 2.2.4 does not sanitise and escape some of its settings, which could allow high privilege users such as editors to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2024-6617	The NinjaTeam Header Footer Custom Code WordPress plugin before 1.2 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-45811	Vite a frontend build tooling framework for javascript. In affected versions the contents of arbitrary files can be returned to the browser. `@fs` denies access to files outside of Vite serving allow list. Adding `?import&raw` to the URL bypasses this limitation and returns the file content if it exists. This issue has been patched in versions 5.4.6, 5.3.6, 5.2.14, 4.5.5, and 3.2.11. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.8	More Details
CVE-2024-5799	The CM Pop-Up Banners for WordPress plugin before 1.7.3 does not sanitise and escape some of its popup fields, which could allow high privilege users such as Contributors to perform Cross-Site Scripting attacks.	4.8	More Details
CVE-2024-46711	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: fix ID 0 endp usage after multiple re-creations 'local_addr_used' and 'add_addr_accepted' are decremented for addresses not related to the initial subflow (ID0), because the source and destination addresses of the initial subflows are known from the beginning: they don't count as "additional local address being used" or "ADD_ADDR being accepted". It is then required not to increment them when the entrypoint used by the initial subflow is removed and re-added during a connection. Without this modification, this entrypoint cannot be removed and re-added more than once.	4.7	More Details
CVE-2024-46710	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: Prevent unmapping active read buffers The kms paths keep a persistent map active to read and compare the cursor buffer. These maps can race with each other in simple scenario where: a) buffer "a" mapped for update b) buffer "a" mapped for compare c) do the compare d) unmap "a" for compare e) update the cursor f) unmap "a" for update At step "e" the buffer has been unmapped and the read contents is bogus. Prevent unmapping of active read buffers by simply keeping a count of how many paths have currently active maps and unmap only when the count reaches 0.	4.7	More Details
CVE-2024-42794	Kashipara Music Management System v1.0 is vulnerable to Incorrect Access Control via /music/ajax.php?action=save_user.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46704	In the Linux kernel, the following vulnerability has been resolved: workqueue: Fix spruious data race in __flush_work() When flushing a work item for cancellation, __flush_work() knows that it exclusively owns the work item through its PENDING bit. 134874e2eee9 ("workqueue: Allow cancel_work_sync() and disable_work() from atomic contexts on BH work items") added a read of @work->data to determine whether to use busy wait for BH work items that are being canceled. While the read is safe when @from_cancel, @work->data was read before testing @from_cancel to simplify code structure: data = *work_data_bits(work); if (from_cancel && !WARN_ON_ONCE(data & WORK_STRUCT_PWQ) && (data & WORK_OFFQ_BH)) { While the read data was never used if !@from_cancel, this could trigger KCSAN data race detection spuriously: ========== BUG: KCSAN: data-race in __flush_work / __flush_work write to 0xffff8881223aa3e8 of 8 bytes by task 3998 on cpu 0: instrument_write include/linux/instrumented.h:41 [inline] ___set_bit include/asm-generic/bitops/instrumented-non-atomic.h:28 [inline] insert_wq_barrier kernel/workqueue.c:3790 [inline] start_flush_work kernel/workqueue.c:4142 [inline] __flush_work+0x30b/0x570 kernel/workqueue.c:4178 flush_work kernel/workqueue.c:4229 [inline] ... read to 0xffff8881223aa3e8 of 8 bytes by task 50 on cpu 1: __flush_work+0x42a/0x570 kernel/workqueue.c:4188 flush_work kernel/workqueue.c:4229 [inline] flush_delayed_work+0x66/0x70 kernel/workqueue.c:4251 ... value changed: 0x0000000000400000 -> 0xffff88810006c00d Reorganize the code so that @from_cancel is tested before @work->data is accessed. The only problem is triggering KCSAN detection spuriously. This shouldn't need READ_ONCE() or other access qualifiers. No functional changes.	4.7	More Details
CVE-2024-46679	In the Linux kernel, the following vulnerability has been resolved: ethtool: check device is present when getting link settings A sysfs reader can race with a device reset or removal, attempting to read device state when the device is not actually present. eg: [exception RIP: qed_get_current_link+17] #8 [ffffb9e4f2907c48] qede_get_link_ksettings at ffffffffc07a994a [qede] #9 [ffffb9e4f2907cd8] __rh_call_get_link_ksettings at ffffffff992b01a3 #10 [ffffb9e4f2907d38] __ethtool_get_link_ksettings at ffffffff992b04e4 #11 [ffffb9e4f2907d90] duplex_show at ffffffff99260300 #12 [ffffb9e4f2907e38] dev_attr_show at ffffffff9905a01c #13 [ffffb9e4f2907e50] sysfs_kf_seq_show at ffffffff98e0145b #14 [ffffb9e4f2907e68] seq_read at ffffffff98d902e3 #15 [ffffb9e4f2907ec8] vfs_read at ffffffff98d657d1 #16 [ffffb9e4f2907f00] ksys_read at ffffffff98d65c3f #17 [ffffb9e4f2907f38] do_syscall_64 at ffffffff98a052fb crash> struct net_device.state ffff9a9d21336000 state = 5, state 5 is __LINK_STATE_START (0b1) and __LINK_STATE_NOCARRIER (0b100). The device is not present, note lack of __LINK_STATE_PRESENT (0b10). This is the same sort of panic as observed in commit 4224cfd7fb65 ("net-sysfs: add check for netdevice being present to speed_show"). There are many other callers of __ethtool_get_link_ksettings() which don't have a device presence check. Move this check into ethtool to protect all callers.	4.7	More Details
CVE-2024-32666	NULL pointer dereference in Intel(R) RAID Web Console software for all versions may allow an authenticated user to potentially enable denial of service via local access.	4.7	More Details
CVE-2024-46693	In the Linux kernel, the following vulnerability has been resolved: soc: qcom: pmic_glink: Fix race during initialization As pointed out by Stephen Boyd it is possible that during initialization of the pmic_glink child drivers, the protection-domain notifiers fires, and the associated work is scheduled, before the client registration returns and as a result the local "client" pointer has been initialized. The outcome of this is a NULL pointer dereference as the "client" pointer is blindly dereferenced. Timeline provided by Stephen: CPU0 CPU1 ---- ---- ucsi->client = NULL; devm_pmic_glink_register_client() client->pdr_notify(client->priv, pg->client_state) pmic_glink_ucsi_pdr_notify() schedule_work(&ucsi->register_work) <schedule away> pmic_glink_ucsi_register() ucsi_register() pmic_glink_ucsi_read_version() pmic_glink_ucsi_read() pmic_glink_ucsi_read() pmic_glink_send(ucsi->client) <client is NULL BAD> ucsi->client = client // Too late! This code is identical across the altmode, battery manager and usci child drivers. Resolve this by splitting the allocation of the "client" object and the registration thereof into two operations. This only happens if the protection domain registry is populated at the time of registration, which by the introduction of commit '1ebcde047c54 ("soc: qcom: add pd-mapper implementation")' became much more likely.	4.7	More Details
CVE-2024-6723	The AI Engine WordPress plugin before 2.4.8 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by admin users when viewing chatbot discussions.	4.7	More Details
CVE-2024-44573	A stored cross-site scripting (XSS) vulnerability in the VLAN configuration of RELY-PCIe v22.2.1 to v23.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44171	This issue was addressed through improved state management. This issue is fixed in iOS 17.7 and iPadOS 17.7, iOS 18 and iPadOS 18, watchOS 11. An attacker with physical access to a locked device may be able to Control Nearby Devices via accessibility features.	4.6	More Details
CVE-2024-39808	Incorrect Calculation of Buffer Size (CWE-131) in the Controller 6000 and Controller 7000 OSDP message handling, allows an attacker with physical access to Controller wiring to instigate a reboot leading to a denial of service. This issue affects: Controller 6000 and Controller 7000 9.10 prior to vCR9.10.240816a (distributed in 9.10.1530 (MR2)), 9.00 prior to vCR9.00.240816a (distributed in 9.00.2168 (MR4)), 8.90 prior to vCR8.90.240816a (distributed in 8.90.2155 (MR5)), 8.80 prior to vCR8.80.240816b (distributed in 8.80.1938 (MR6)), all versions of 8.70 and prior.	4.6	More Details
CVE-2024-36247	Improper access control in Intel(R) RAID Web Console all versions may allow an authenticated user to potentially enable denial of service via adjacent access.	4.6	More Details
CVE-2024-40840	This issue was addressed through improved state management. This issue is fixed in iOS 18 and iPadOS 18. An attacker with physical access may be able to use Siri to access sensitive user data.	4.6	More Details
CVE-2024-45833	Mattermost Mobile Apps versions <=2.18.0 fail to disable autocomplete during login while typing the password and visible password is selected, which allows the password to get saved in the dictionary when the user has Swiftkey as the default keyboard, the masking is off and the password contains a special character..	4.5	More Details
CVE-2024-5435	An issue has been discovered discovered in GitLab EE/CE affecting all versions starting from 15.10 before 17.1.7, all versions starting from 17.2 before 17.2.5, all versions starting from 17.3 before 17.3.2 will disclose user password from repository mirror configuration.	4.5	More Details
CVE-2024-44130	This issue was addressed with improved data protection. This issue is fixed in macOS Sequoia 15. An app with root privileges may be able to access private information.	4.4	More Details
CVE-2024-8688	An improper neutralization of matching symbols vulnerability in the Palo Alto Networks PAN-OS command line interface (CLI) enables authenticated administrators (including read-only administrators) with access to the CLI to to read arbitrary files on the firewall.	4.4	More Details
CVE-2024-46695	In the Linux kernel, the following vulnerability has been resolved: selinux,smack: don't bypass permissions check in inode_setsecctx hook Marek Gresko reports that the root user on an NFS client is able to change the security labels on files on an NFS filesystem that is exported with root squashing enabled. The end of the kerneldoc comment for __vfs_setxattr_noperm() states: * This function requires the caller to lock the inode's i_mutex before it * is executed. It also assumes that the caller will make the appropriate * permission checks. nfsd_setattr() does do permissions checking via fh_verify() and nfsd_permission(), but those don't do all the same permissions checks that are done by security_inode_setxattr() and its related LSM hooks do. Since nfsd_setattr() is the only consumer of security_inode_setsecctx(), simplest solution appears to be to replace the call to __vfs_setxattr_noperm() with a call to __vfs_setxattr_locked(). This fixes the above issue and has the added benefit of causing nfsd to recall conflicting delegations on a file when a client tries to change its security label.	4.4	More Details
CVE-2024-44096	there is a possible arbitrary read due to an insecure default value. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	4.4	More Details
CVE-2024-8690	A problem with a detection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices enables a user with Windows administrator privileges to disable the agent. This issue may be leveraged by malware to disable the Cortex XDR agent and then to perform malicious activity.	4.4	More Details
CVE-2024-40825	The issue was addressed with improved checks. This issue is fixed in visionOS 2, macOS Sequoia 15. A malicious app with root privileges may be able to modify the contents of system files.	4.4	More Details
CVE-2024-45604	Contao is an Open Source CMS. In affected versions authenticated users in the back end can list files outside the document root in the file selector widget. Users are advised to update to Contao 4.13.49. There are no known workarounds for this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8866	A vulnerability was found in AutoCMS 5.4. It has been classified as problematic. This affects an unknown part of the file /admin/robot.php. The manipulation of the argument sidebar 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-2024-25270	An issue in Mirapolis LMS 4.6.XX allows authenticated users to exploit an Insecure Direct Object Reference (IDOR) vulnerability by manipulating the ID parameter and increment STEP parameter, leading to the exposure of sensitive user data.	4.3	More Details
CVE-2024-8908	Inappropriate implementation in Autofill in Google Chrome prior to 129.0.6668.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2024-43180	IBM Concert 1.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic.	4.3	More Details
CVE-2024-45789	This vulnerability exists in Reedos aiM-Star version 2.0.1 due to improper validation of the ‘mode’ parameter in the API endpoint used during the registration process. An authenticated remote attacker could exploit this vulnerability by manipulating parameter in the API request body on the vulnerable application. Successful exploitation of this vulnerability could allow the attacker to bypass certain constraints in the registration process leading to creation of multiple accounts.	4.3	More Details
CVE-2024-8906	Incorrect security UI in Downloads in Google Chrome prior to 129.0.6668.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-8242	The MStore API – Create Native Android & iOS Apps On The Cloud plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the update_user_profile() function in all versions up to, and including, 4.15.3. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload arbitrary files (not including PHP files) on the affected site's server which may make remote code execution possible. This can be paired with a registration endpoint for unauthenticated users to exploit the issue.	4.3	More Details
CVE-2024-8909	Inappropriate implementation in UI in Google Chrome on iOS prior to 129.0.6668.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2024-8059	IPMI credentials may be captured in XCC audit log entries when the account username length is 16 characters.	4.3	More Details
CVE-2024-45103	A valid, authenticated LXCA user may be able to unmanage an LXCA managed device in through the LXCA web interface without sufficient privileges.	4.3	More Details
CVE-2024-6582	A broken access control vulnerability exists in the latest version of lunary-ai/lunary. The `saml.ts` file allows a user from one organization to update the Identity Provider (IDP) settings and view the SSO metadata of another organization. This vulnerability can lead to unauthorized access and potential account takeover if the email of a user in the target organization is known.	4.3	More Details
CVE-2024-7721	The HTML5 Video Player – mp4 Video Player Plugin and Block plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'save_password' function in all versions up to, and including, 2.5.34. This makes it possible for authenticated attackers, with Subscriber-level access and above, to set any options that are not explicitly checked as false to an array, including enabling user registration if it has been disabled.	4.3	More Details
CVE-2020-24061	Cross Site Scripting (XSS) Vulnerability in Firewall menu in Control Panel in KASDA KW5515 version 4.3.1.0, allows attackers to execute arbitrary code and steal cookies via a crafted script	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8876	A vulnerability, which was classified as problematic, has been found in xiaohe4966 TpMeCMS up to 1.3.3.1. Affected by this issue is some unknown functionality of the file /index/ajax/lang. The manipulation of the argument lang leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 1.3.3.2 is able to address this issue. It is recommended to upgrade the affected component.	4.3	More Details
CVE-2024-3163	The Easy Property Listings WordPress plugin before 3.5.4 does not have CSRF check when deleting contacts in bulk, which could allow attackers to make a logged in admin delete them via a CSRF attack	4.3	More Details
CVE-2024-8707	A vulnerability was found in 云课网络科技有限公司 Yunke Online School System up to 3.0.6. It has been declared as problematic. This vulnerability affects the function downfile of the file application/admin/controller/Appadmin.php. The manipulation of the argument url leads to path traversal. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2024-6389	An issue was discovered in GitLab-CE/EE affecting all versions starting with 17.0 before 17.1.7, 17.2 before 17.2.5, and 17.3 before 17.3.2. An attacker as a guest user was able to access commit information via the release Atom endpoint, contrary to permissions.	4.3	More Details
CVE-2024-8706	A vulnerability was found in JFinalCMS up to 20240903. It has been classified as problematic. This affects the function update of the file /admin/template/update of the component com.cms.util.TemplateUtils. The manipulation of the argument fileName leads to path traversal. 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-2024-42795	An Incorrect Access Control vulnerability was found in /music/view_user.php?id=3 and /music/controller.php?page=edit_user&id=3 in Kashipara Music Management System v1.0. This vulnerability allows an unauthenticated attacker to view valid user details.	4.2	More Details
CVE-2024-4472	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.5 prior to 17.1.7, starting from 17.2 prior to 17.2.5, and starting from 17.3 prior to 17.3.2, where dependency proxy credentials are retained in graphql Logs.	4.0	More Details
CVE-2024-8694	A vulnerability, which was classified as problematic, was found in JFinalCMS up to 20240903. This affects the function update of the file /admin/template/update of the component com.cms.controller.admin.TemplateController. The manipulation of the argument fileName leads to path traversal. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.8	More Details
CVE-2024-44575	RELY-PCIe v22.2.1 to v23.1.0 does not set the Secure attribute for sensitive cookies in HTTPS sessions, which could cause the user agent to send those cookies in cleartext over an HTTP session.	3.7	More Details
CVE-2024-39772	Mattermost Desktop App versions <=5.8.0 fail to safeguard screen capture functionality which allows an attacker to silently capture high-quality screenshots via JavaScript APIs.	3.7	More Details
CVE-2024-6446	An issue has been discovered in GitLab affecting all versions starting from 17.1 to 17.1.7, 17.2 prior to 17.2.5 and 17.3 prior to 17.3.2. A crafted URL could be used to trick a victim to trust an attacker controlled application.	3.5	More Details
CVE-2024-36261	Improper access control in Intel(R) RAID Web Console software all versions may allow an authenticated user to potentially enable denial of service via adjacent access.	3.5	More Details
CVE-2024-8708	A vulnerability was found in SourceCodester Best House Rental Management System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file categories.php. The manipulation leads to cross site scripting. The attack may be initiated remotely.	3.5	More Details
CVE-2024-8783	A vulnerability classified as problematic has been found in OpenTibiaBR MyAAC up to 0.8.16. Affected is an unknown function of the file system/pages/forum/new_post.php of the component Post Reply Handler. The manipulation of the argument post_topic 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 patch is identified as bf6ae3df0d32fa22552bb44ca4f8489a6e78cc1c. It is recommended to apply a patch to fix this issue.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8951	A vulnerability classified as problematic was found in SourceCodester Resort Reservation System 1.0. Affected by this vulnerability is an unknown functionality of the file manage_fee.php. The manipulation of the argument toview leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-8863	A vulnerability, which was classified as problematic, was found in aimhubio aim up to 3.24. Affected is the function dangerouslySetInnerHTML of the file textbox.tsx of the component Text Explorer. The manipulation of the argument query leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-8865	A vulnerability was found in composiohq composio up to 0.5.8 and classified as problematic. Affected by this issue is the function path of the file composio\server\api.py. The manipulation of the argument file leads to path traversal. 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-2024-8867	A vulnerability was found in Perfex CRM 3.1.6. It has been declared as problematic. This vulnerability affects unknown code of the file application/controllers/Clients.php of the component Parameter Handler. The manipulation of the argument message leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue.	3.5	More Details
CVE-2024-40838	A privacy issue was addressed by moving sensitive data to a protected location. This issue is fixed in macOS Sequoia 15. A malicious app may be able to access notifications from the user's device.	3.3	More Details
CVE-2024-28170	Improper access control in Intel(R) RAID Web Console all versions may allow an authenticated user to potentially enable information disclosure via local access.	3.3	More Details
CVE-2024-46970	In JetBrains IntelliJ IDEA before 2024.1 hTML injection via the project name was possible	3.3	More Details
CVE-2024-40791	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, iOS 18 and iPadOS 18, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access information about a user's contacts.	3.3	More Details
CVE-2024-40830	This issue was addressed with improved data protection. This issue is fixed in iOS 18 and iPadOS 18. An app may be able to enumerate a user's installed apps.	3.3	More Details
CVE-2024-36066	The CMP CLI client in KeyFactor EJBCA before 8.3.1 has only 6 octets of salt, and is thus not compliant with the security requirements of RFC 4211, and might make man-in-the-middle attacks easier. CMP includes password-based MAC as one of the options for message integrity and authentication (the other option is certificate-based). RFC 4211 section 4.4 requires that password-based MAC parameters use a salt with a random value of at least 8 octets. This helps to inhibit dictionary attacks. Because the standalone CMP client originally was developed as test code, the salt was instead hardcoded and only 6 octets long.	3.1	More Details
CVE-2024-6685	An issue was discovered in GitLab CE/EE affecting all versions starting from 16.7 prior to 17.1.7, 17.2 prior to 17.2.5, and 17.3 prior to 17.3.2, where group runners information was disclosed to unauthorised group members.	3.1	More Details
CVE-2024-1656	Affected versions of Octopus Server had a weak content security policy.	2.6	More Details
CVE-2023-25546	Out-of-bounds read in UEFI firmware for some Intel(R) Processors may allow a privileged user to potentially enable denial of service via local access.	2.5	More Details
CVE-2024-45835	Mattermost Desktop App versions <=5.8.0 fail to sufficiently configure Electron Fuses which allows an attacker to gather Chromium cookies or abuse other misconfigurations via remote/local access.	2.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44139	The issue was addressed with improved checks. This issue is fixed in iOS 18 and iPadOS 18. An attacker with physical access may be able to access contacts from the lock screen.	2.4	More Details
CVE-2024-8693	A vulnerability, which was classified as problematic, has been found in Kaon CG3000 1.01.43. Affected by this issue is some unknown functionality of the component dhcpcd Command Handler. The manipulation of the argument -h with the input <script>alert('XSS')</script> leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2.4	More Details
CVE-2024-44180	The issue was addressed with improved checks. This issue is fixed in iOS 18 and iPadOS 18. An attacker with physical access may be able to access contacts from the lock screen.	2.4	More Details
CVE-2024-8767	Sensitive data disclosure and manipulation due to unnecessary privileges assignment. The following products are affected: Acronis Backup plugin for cPanel & WHM (Linux) before build 619, Acronis Backup extension for Plesk (Linux) before build 555, Acronis Backup plugin for DirectAdmin (Linux) before build 147.	N/A	More Details
CVE-2024-8097	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Payara Platform Payara Server (Logging modules) allows Sensitive credentials posted in plain-text on the server log.This issue affects Payara Server: from 6.0.0 before 6.18.0, from 6.2022.1 before 6.2024.9, from 5.20.0 before 5.67.0, from 5.2020.2 before 5.2022.5, from 4.1.2.191.0 before 4.1.2.191.50.	N/A	More Details
CVE-2024-5998	A vulnerability in the FAISS.deserialize_from_bytes function of langchain-ai/langchain allows for pickle deserialization of untrusted data. This can lead to the execution of arbitrary commands via the os.system function. The issue affects the latest version of the product.	N/A	More Details
CVE-2024-8766	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Cyber Protect Cloud Agent (Windows) before build 38235, Acronis Cyber Protect 16 (Windows) before build 39169.	N/A	More Details
CVE-2024-44445	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2024-34016	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Cyber Protect Cloud Agent (Windows) before build 38235.	N/A	More Details
CVE-2024-7805	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-8689	A problem with the ActiveMQ integration for both Cortex XSOAR and Cortex XSIAM can result in the cleartext exposure of the configured ActiveMQ credentials in log bundles.	N/A	More Details
CVE-2024-46713	In the Linux kernel, the following vulnerability has been resolved: perf/aux: Fix AUX buffer serialization Ole reported that event->mmap_mutex is strictly insufficient to serialize the AUX buffer, add a per RB mutex to fully serialize it. Note that in the lock order comment the perf_event::mmap_mutex order was already wrong, that is, it nesting under mmap_lock is not new with this patch.	N/A	More Details
CVE-2024-45804	Rejected reason: This CVE is a duplicate of another CVE.	N/A	More Details
CVE-2024-7873	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting'), Improper Encoding or Escaping of Output, CWE - 83 Improper Neutralization of Script in Attributes in a Web Page vulnerability in Veribilim Software Veribase Order allows Stored XSS, Cross-Site Scripting (XSS), Exploit Script-Based APIs, XSS Through HTTP Headers.This issue affects Veribase Order: before v4.010.3.	N/A	More Details