SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 06 November 2024

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-50531	Unrestricted Upload of File with Dangerous Type vulnerability in David F. Carr RSVPMaker for Toastmasters allows Upload a Web Shell to a Web Server.This issue affects RSVPMaker for Toastmasters: from n/a through 6.2.4.	10.0	More Details
CVE-2024-50527	Unrestricted Upload of File with Dangerous Type vulnerability in Stacks Stacks Mobile App Builder allows Upload a Web Shell to a Web Server.This issue affects Stacks Mobile App Builder: from n/a through 5.2.3.	10.0	More Details
CVE-2024-50510	Unrestricted Upload of File with Dangerous Type vulnerability in Web and Print Design AR For Woocommerce allows Upload a Web Shell to a Web Server.This issue affects AR For Woocommerce: from n/a through 6.2.	10.0	More Details
CVE-2024-50526	Unrestricted Upload of File with Dangerous Type vulnerability in mahlamusa Multi Purpose Mail Form allows Upload a Web Shell to a Web Server.This issue affects Multi Purpose Mail Form: from n/a through 1.0.2.	10.0	More Details
CVE-2024-50525	Unrestricted Upload of File with Dangerous Type vulnerability in Helloprint Plug your WooCommerce into the largest catalog of customized print products from Helloprint allows Upload a Web Shell to a Web Server.This issue affects Plug your WooCommerce into the largest catalog of customized print products from Helloprint: from n/a through 2.0.2.	10.0	More Details
CVE-2024-50523	Unrestricted Upload of File with Dangerous Type vulnerability in RainbowLink Inc. All Post Contact Form allows Upload a Web Shell to a Web Server.This issue affects All Post Contact Form: from n/a through 1.7.3.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50530	Unrestricted Upload of File with Dangerous Type vulnerability in Myriad Solutionz Stars SMTP Mailer allows Upload a Web Shell to a Web Server.This issue affects Stars SMTP Mailer: from n/a through 1.7.	9.9	More Details
CVE-2024-51478	YesWiki is a wiki system written in PHP. Prior to 4.4.5, the use of a weak cryptographic algorithm and a hard-coded salt to hash the password reset key allows it to be recovered and used to reset the password of any account. This issue is fixed in 4.4.5.	9.9	More Details
CVE-2024-51482	ZoneMinder is a free, open source closed-circuit television software application. ZoneMinder v1.37.* <= 1.37.64 is vulnerable to boolean-based SQL Injection in function of web/ajax/event.php. This is fixed in 1.37.65.	9.9	More Details
CVE-2024-50529	Unrestricted Upload of File with Dangerous Type vulnerability in Rudra Innnovative Software Training – Courses allows Upload a Web Shell to a Web Server.This issue affects Training – Courses: from n/a through 2.0.1.	9.9	More Details
CVE-2024-33699	The LevelOne WBR-6012 router's web application has a vulnerability in its firmware version R0.40e6, allowing attackers to change the administrator password and gain higher privileges without the current password.	9.9	More Details
CVE-2024-42515	Glossarizer through 1.5.2 improperly tries to convert text into HTML. Even though the application itself escapes special characters (e.g., <>), the underlying library converts these encoded characters into legitimate HTML, thereby possibly causing stored XSS. Attackers can append a XSS payload to a word that has a corresponding glossary entry.	9.9	More Details
CVE-2024-50511	Unrestricted Upload of File with Dangerous Type vulnerability in David DONISA WP donimedia carousel allows Upload a Web Shell to a Web Server.This issue affects WP donimedia carousel: from n/a through 1.0.1.	9.9	More Details
CVE-2024-51252	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the restore function.	9.8	More Details
CVE-2024-51558	This vulnerability exists in the Wave 2.0 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 OTP, MPIN or password, which could lead to gain unauthorized access and compromise other user accounts.	9.8	More Details
CVE-2024-51431	LB-LINK BL-WR 1300H v.1.0.4 contains hardcoded credentials stored in /etc/shadow which are easily guessable.	9.8	More Details
CVE-2024-7456	A SQL injection vulnerability exists in the `/api/v1/external-users` route of lunary-ai/lunary version v1.4.2. The `order by` clause of the SQL query uses `sql.unsafe` without prior sanitization, allowing for SQL injection. The `orderByClause` variable is constructed without server-side validation or sanitization, enabling an attacker to execute arbitrary SQL commands. Successful exploitation can lead to complete data loss, modification, or corruption.	9.8	More Details
CVE-2024-10035	Improper Control of Generation of Code ('Code Injection') vulnerability in BG-TEK Informatics Security Technologies CoslatV3 allows Command Injection.This issue affects CoslatV3: through 3.1069. NOTE: The vendor was contacted and it was learned that the product is not supported.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50503	Authentication Bypass Using an Alternate Path or Channel vulnerability in Deryck Oñate User Toolkit allows Authentication Bypass.This issue affects User Toolkit: from n/a through 1.2.3.	9.8	More Details
CVE-2024-51065	Phpgurukul Beauty Parlour Management System v1.1 is vulnerable to SQL Injection in admin/index.php via the the username parameter.	9.8	More Details
CVE-2024-51136	An XML External Entity (XXE) vulnerability in Dmoz2CSV in openimaj v1.3.10 allows attackers to access sensitive information or execute arbitrary code via supplying a crafted XML file.	9.8	More Details
CVE-2024-51327	SQL Injection in loginform.php in ProjectWorld's Travel Management System v1.0 allows remote attackers to bypass authentication via SQL Injection in the 'username' and 'password' fields.	9.8	More Details
CVE-2024-48050	In agentscope <=v0.0.4, the file agentscope\web\workstation\workflow_utils.py has the function is_callable_expression. Within this function, the line result = eval(s) poses a security risk as it can directly execute user-provided commands.	9.8	More Details
CVE-2024-48061	langflow <=1.0.18 is vulnerable to Remote Code Execution (RCE) as any component provided the code functionality and the components run on the local machine rather than in a sandbox.	9.8	More Details
CVE-2024-10687	The Photos, Files, YouTube, Twitter, Instagram, TikTok, Ecommerce Contest Gallery – Upload, Vote, Sell via PayPal, Social Share Buttons plugin for WordPress is vulnerable to time-based SQL Injection via the $collectedIds parameter in all versions up to, and including, 24.0.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.8	More Details
CVE-2024-51132	An XML External Entity (XXE) vulnerability in HAPI FHIR before v6.4.0 allows attackers to access sensitive information or execute arbitrary code via supplying a crafted request containing malicious XML entities.	9.8	More Details
CVE-2024-42509	Command injection vulnerability in the underlying CLI service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.8	More Details
CVE-2024-48176	Lylme Spage v1.9.5 is vulnerable to Incorrect Access Control. There is no limit on the number of login attempts, and the verification code will not be refreshed after a failed login, which allows attackers to blast the username and password and log into the system backend.	9.8	More Details
CVE-2024-48746	An issue in Lens Visual integration with Power BI v.4.0.0.3 allows a remote attacker to execute arbitrary code via the Natural language processing component	9.8	More Details
CVE-2024-51115	DCME-320 v7.4.12.90 was discovered to contain a command injection vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50507	Deserialization of Untrusted Data vulnerability in Daniel Schmitzer DS.DownloadList allows Object Injection.This issue affects DS.DownloadList: from n/a through 1.3.	9.8	More Details
CVE-2024-48359	Qualitor v8.24 was discovered to contain a remote code execution (RCE) vulnerability via the gridValoresPopHidden parameter.	9.8	More Details
CVE-2024-51064	Phpgurukul Teachers Record Management System v2.1 is vulnerable to SQL Injection via the tid parameter to admin/queries.php.	9.8	More Details
CVE-2024-51259	DrayTek Vigor3900 1.5.1.3 allows attackers to inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the setup_cacertificate function.	9.8	More Details
CVE-2024-51298	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the doGRETunnel function.	9.8	More Details
CVE-2024-10456	Delta Electronics InfraSuite Device Master versions prior to 1.0.12 are affected by a deserialization vulnerability that targets the Device-Gateway, which could allow deserialization of arbitrary .NET objects prior to authentication.	9.8	More Details
CVE-2024-48202	icecms <=3.4.7 has a File Upload vulnerability in FileUtils.java,uploadFile.	9.8	More Details
CVE-2024-48112	A deserialization vulnerability in the component \controller\Index.php of Thinkphp v6.1.3 to v8.0.4 allows attackers to execute arbitrary code.	9.8	More Details
CVE-2024-51424	An issue in the PepeGxng smart contract (which can be run on the Ethereum blockchain) allows remote attackers to have an unspecified impact via the Owned.setOwner function. NOTE: this is disputed by third parties because the impact is limited to function calls.	9.8	More Details
CVE-2024-51427	An issue in the PepeGxng smart contract (which can be run on the Ethereum blockchain) allows remote attackers to have an unspecified impact via the mint function. NOTE: this is disputed by third parties because the impact is limited to function calls.	9.8	More Details
CVE-2024-10392	The AI Power: Complete AI Pack plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'handle_image_upload' function in all versions up to, and including, 1.8.89. This makes it possible for unauthenticated attackers to upload arbitrary files on the affected site's server which may make remote code execution possible.	9.8	More Details
CVE-2024-42835	langflow v1.0.12 was discovered to contain a remote code execution (RCE) vulnerability via the PythonCodeTool component.	9.8	More Details
CVE-2024-48307	JeecgBoot v3.7.1 was discovered to contain a SQL injection vulnerability via the component /onlDragDatasetHead/getTotalData.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51358	An issue in Linux Server Heimdall v.2.6.1 allows a remote attacker to execute arbitrary code via a crafted script to the Add new application.	9.8	More Details
CVE-2024-39332	Webswing 23.2.2 allows remote attackers to modify client-side JavaScript code to achieve path traversal, likely leading to remote code execution via modification of shell scripts on the server.	9.8	More Details
CVE-2024-51260	DrayTek Vigor3900 1.5.1.3 allows attackers to inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the acme_process function.	9.8	More Details
CVE-2024-51255	DrayTek Vigor3900 1.5.1.3 allows attackers to inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the ruequest_certificate function.	9.8	More Details
CVE-2023-52044	Studio-42 eLfinder 2.1.62 is vulnerable to Remote Code Execution (RCE) as there is no restriction for uploading files with the .php8 extension.	9.8	More Details
CVE-2023-29121	Waybox Enel TCF Agent service could be used to get administrator’s privileges over the Waybox system.	9.6	More Details
CVE-2023-29120	Waybox Enel X web management application could be used to execute arbitrary OS commands and provide administrator’s privileges over the Waybox system.	9.6	More Details
CVE-2023-29118	Waybox Enel X web management application could execute arbitrary requests on the internal database via /admin/versions.php.	9.6	More Details
CVE-2023-29119	Waybox Enel X web management application could execute arbitrary requests on the internal database via /admin/dbstore.php.	9.6	More Details
CVE-2024-43984	Cross-Site Request Forgery (CSRF) vulnerability in Podlove Podlove Podcast Publisher allows Code Injection.This issue affects Podlove Podcast Publisher: from n/a through 4.1.13.	9.6	More Details
CVE-2024-49674	Cross-Site Request Forgery (CSRF) vulnerability in Lukas Huser EKC Tournament Manager allows Upload a Web Shell to a Web Server.This issue affects EKC Tournament Manager: from n/a through 2.2.1.	9.6	More Details
CVE-2024-23590	Session Fixation vulnerability in Apache Kylin. This issue affects Apache Kylin: from 2.0.0 through 4.x. Users are recommended to upgrade to version 5.0.0 or above, which fixes the issue.	9.1	More Details
CVE-2024-51661	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in David Lingren Media Library Assistant allows Command Injection.This issue affects Media Library Assistant: from n/a through 3.19.	9.1	More Details
CVE-2024-51063	Phpgurukul Teachers Record Management System v2.1 is vulnerable to SQL Injection in add-teacher.php via the mobile number or email parameter.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51060	Projectworlds Online Admission System v1 is vulnerable to SQL Injection in index.php via the 'a_id' parameter.	9.1	More Details
CVE-2024-28265	IBOS v4.5.5 has an arbitrary file deletion vulnerability via \system\modules\dashboard\controllers\LoginController.php.	9.1	More Details
CVE-2024-10525	In Eclipse Mosquitto, from version 1.3.2 through 2.0.18, if a malicious broker sends a crafted SUBACK packet with no reason codes, a client using libmosquitto may make out of bounds memory access when acting in its on_subscribe callback. This affects the mosquitto_sub and mosquitto_rr clients.	9.1	More Details
CVE-2024-8512	The W3SPEEDSTER plugin for WordPress is vulnerable to Remote Code Execution in all versions up to, and including, 7.26 via the 'script' parameter of the hookBeforeStartOptimization() function. This is due to the plugin passing user supplied input to eval(). This makes it possible for authenticated attackers, with Administrator-level access and above, to execute code on the server.	9.1	More Details
CVE-2024-48910	DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTML, MathML and SVG. DOMPurify was vulnerable to prototype pollution. This vulnerability is fixed in 2.4.2.	9.1	More Details
CVE-2023-29125	A heap buffer overflow could be triggered by sending a specific packet to TCP port 7700.	9.0	More Details
CVE-2024-47460	Command injection vulnerability in the underlying CLI service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of this vulnerability results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	9.0	More Details
CVE-2024-23309	The LevelOne WBR-6012 router with firmware R0.40e6 has an authentication bypass vulnerability in its web application due to reliance on client IP addresses for authentication. Attackers could spoof an IP address to gain unauthorized access without needing a session token.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-0105	NVIDIA ConnectX Firmware contains a vulnerability where an attacker may cause an improper handling of insufficient privileges issue. A successful exploit of this vulnerability may lead to denial of service, data tampering, and limited information disclosure.	8.9	More Details
CVE-2024-10698	A vulnerability was found in Tenda AC6 15.03.05.19 and classified as critical. Affected by this issue is the function formSetDeviceName of the file /goform/SetOnlineDevName. The manipulation of the argument devName leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48271	D-Link DSL6740C v6.TR069.20211230 was discovered to use insecure default credentials for Administrator access, possibly allowing attackers to bypass authentication and escalate privileges on the device via a bruteforce attack.	8.8	More Details
CVE-2024-51425	An issue in the WaterToken smart contract (which can be run on the Ethereum blockchain) allows remote attackers to have an unspecified impact. NOTE: this is disputed by third parties because the impact is limited to function calls.	8.8	More Details
CVE-2024-51247	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the doPPPo function.	8.8	More Details
CVE-2024-51245	In DrayTek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the rename_table function.	8.8	More Details
CVE-2024-48734	Unrestricted file upload in /SASStudio/SASStudio/sasexec/{sessionID}/{InternalPath} in SAS Studio 9.4 allows remote attacker to upload malicious files. NOTE: this is disputed by the vendor because file upload is allowed for authorized users.	8.8	More Details
CVE-2024-48733	SQL injection vulnerability in /SASStudio/sasexec/sessions/{sessionID}/sql in SAS Studio 9.4 allows remote attacker to execute arbitrary SQL commands via the POST body request. NOTE: this is disputed by the vendor because SQL statement execution is allowed for authorized users.	8.8	More Details
CVE-2024-51244	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the doIPSec function.	8.8	More Details
CVE-2024-36060	EnGenius EnStation5-AC A8J-ENS500AC 1.0.0 devices allow blind OS command injection via shell metacharacters in the Ping and Speed Test parameters.	8.8	More Details
CVE-2024-30616	Chamilo LMS 1.11.26 is vulnerable to Incorrect Access Control via main/auth/profile. Non-admin users can manipulate sensitive profiles information, posing a significant risk to data integrity.	8.8	More Details
CVE-2024-51258	DrayTek Vigor3900 1.5.1.3 allows attackers to inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the doSSLTunnel function.	8.8	More Details
CVE-2024-51301	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the packet_monitor function.	8.8	More Details
CVE-2024-51300	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the get_rrd function.	8.8	More Details
CVE-2024-51299	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the dumpSyslog function.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51296	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the pingtrace function.	8.8	More Details
CVE-2024-51426	An issue in the PepeGxng smart contract (which can be run on the Ethereum blockchain) allows remote attackers to have an unspecified impact via the _transfer function. NOTE: this is disputed by third parties because the impact is limited to function calls.	8.8	More Details
CVE-2023-29117	Waybox Enel X web management API authentication could be bypassed and provide administrator's privileges over the Waybox system.	8.8	More Details
CVE-2024-49772	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. In SuiteCRM versions 7.14.4, poor input validation allows authenticated user do a SQL injection attack. Authenticated user with low pivilege can leak all data in database. This issue has been addressed in releases 7.14.6 and 8.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2024-48311	Piwigo v14.5.0 was discovered to contain a Cross-Site Request Forgery (CSRF) via the Edit album function.	8.8	More Details
CVE-2024-51492	Zusam is a free and open-source way to self-host private forums. Prior to version 0.5.6, specially crafted SVG files uploaded to the service as images allow for unrestricted script execution on (raw) image load. With certain payloads, theft of the target user's long-lived session token is possible. Note that Zusam, at the time of writing, uses a user's static API key as a long-lived session token, and these terms can be used interchangeably on the platform. This session token/API key remains valid indefinitely, so long as the user doesn't expressly request a new one via their Settings page. Version 0.5.6 fixes the cross-site scripting vulnerability.	8.8	More Details
CVE-2024-21537	Versions of the package lilconfig from 3.1.0 and before 3.1.1 are vulnerable to Arbitrary Code Execution due to the insecure usage of eval in the dynamicImport function. An attacker can exploit this vulnerability by passing a malicious input through the defaultLoaders function.	8.8	More Details
CVE-2024-51023	D-Link DIR_823G 1.0.2B05 was discovered to contain a command injection vulnerability via the Address parameter in the SetNetworkTomographySettings function. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	8.8	More Details
CVE-2024-51254	DrayTek Vigor3900 1.5.1.3 allows attackers to inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the sign_cacertificate function.	8.8	More Details
CVE-2024-37232	Missing Authorization vulnerability in Hercules Design Hercules Core allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Hercules Core: from n/a through 6.5.	8.8	More Details
CVE-2024-10711	The WooCommerce Report plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.5.1. This is due to missing or incorrect nonce validation on the settings update functionality. This makes it possible for unauthenticated attackers to update arbitrary options that can be leveraged for 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 Number	Description	Base Score	Reference
CVE-2024-31998	Combodo iTop is a simple, web based IT Service Management tool. A CSRF can be performed on CSV import simulation. This issue has been fixed in versions 3.1.2 and 3.2.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2024-31448	Combodo iTop is a simple, web based IT Service Management tool. By filling malicious code in a CSV content, an Cross-site Scripting (XSS) attack can be performed when importing this content. This issue has been fixed in versions 3.1.2 and 3.2.0. All users are advised to upgrade. Users unable to upgrade should validate CSV content before importing it.	8.8	More Details
CVE-2023-34445	Combodo iTop is a simple, web based IT Service Management tool. When displaying pages/ajax.render.php XSS are possible for scripts outside of script tags. This issue has been fixed in versions 2.7.9, 3.0.4, 3.1.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2023-34444	Combodo iTop is a simple, web based IT Service Management tool. When displaying pages/ajax.searchform.php XSS are possible for scripts outside of script tags. This issue has been fixed in versions 2.7.9, 3.0.4, 3.1.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2023-34443	Combodo iTop is a simple, web based IT Service Management tool. When displaying page Run queries Cross-site Scripting (XSS) are possible for scripts outside of script tags. This has been fixed in versions 2.7.9, 3.0.4, 3.1.0. All users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2024-51329	A Host header injection vulnerability in Agile-Board 1.0 allows attackers to obtain the password reset token via user interaction with a crafted password reset link.	8.8	More Details
CVE-2024-51257	DrayTek Vigor3900 1.5.1.3 allows attackers to inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the doCertificate function.	8.8	More Details
CVE-2024-51248	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the modifyrow function.	8.8	More Details
CVE-2024-51304	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the ldap_search_dn function.	8.8	More Details
CVE-2024-43982	Missing Authorization vulnerability in Geek Code Lab Login As Users allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Login As Users: from n/a through 1.4.3.	8.8	More Details
CVE-2024-48217	An Insecure Direct Object Reference (IDOR) in the dashboard of SiSMART v7.4.0 allows attackers to execute a horizontal-privilege escalation.	8.8	More Details
CVE-2024-50506	Incorrect Privilege Assignment vulnerability in Azexo Marketing Automation by AZEXO allows Privilege Escalation.This issue affects Marketing Automation by AZEXO: from n/a through 1.27.80.	8.8	More Details
CVE-2024-51116	Tenda AC6 v2.0 V15.03.06.50 was discovered to contain a buffer overflow in the function 'formSetPPTPServer'.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-24777	A cross-site request forgery (CSRF) vulnerability exists in the Web Application functionality of the LevelOne WBR-6012 R0.40e6. A specially crafted HTTP request can lead to unauthorized access. An attacker can stage a malicious web page to trigger this vulnerability.	8.8	More Details
CVE-2024-50504	Incorrect Privilege Assignment vulnerability in Matt Whiteman Bulk Change Role allows Privilege Escalation.This issue affects Bulk Change Role: from n/a through 1.1.	8.8	More Details
CVE-2024-10662	A vulnerability was found in Tenda AC15 15.03.05.19 and classified as critical. This issue affects the function formSetDeviceName of the file /goform/SetOnlineDevName. The manipulation of the argument devName leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-50332	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Insufficient input value validation causes Blind SQL injection in DeleteRelationShip. This issue has been addressed in versions 7.14.6 and 8.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2024-10661	A vulnerability has been found in Tenda AC15 15.03.05.19 and classified as critical. This vulnerability affects the function SetDlnaCfg of the file /goform/SetDlnaCfg. The manipulation of the argument scanList leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-0106	NVIDIA ConnectX Host Firmware for the BlueField Data Processing Unit (DPU) contains a vulnerability where an attacker may cause an improper handling of insufficient privileges issue. A successful exploit of this vulnerability may lead to denial of service, data tampering, and limited information disclosure.	8.7	More Details
CVE-2024-50509	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Chetan Khandla Woocommerce Product Design allows Path Traversal.This issue affects Woocommerce Product Design: from n/a through 1.0.0.	8.6	More Details
CVE-2024-51626	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mansur Ahamed Woocommerce Quote Calculator allows Blind SQL Injection.This issue affects Woocommerce Quote Calculator: from n/a through 1.1.	8.5	More Details
CVE-2024-37423	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Automattic Newspack Blocks allows Path Traversal.This issue affects Newspack Blocks: from n/a through 3.0.8.	8.5	More Details
CVE-2024-51408	AppSmith Community 1.8.3 before 1.46 allows SSRF via New DataSource for application/json requests to 169.254.169.254 to retrieve AWS metadata credentials.	8.5	More Details
CVE-2024-48336	The install() function of ProviderInstaller.java in Magisk App before canary version 27007 does not verify the GMS app before loading it, which allows a local untrusted app with no additional privileges to silently execute arbitrary code in the Magisk app and escalate privileges to root via a crafted package, aka Bug #8279. User interaction is not needed for exploitation.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48214	KERUI HD 3MP 1080P Tuya Camera 1.0.4 has a command injection vulnerability in the module that connects to the local network via a QR code. This vulnerability allows an attacker to create a custom, unauthenticated QR code and abuse one of the parameters, either SSID or PASSWORD, in the JSON data contained within the QR code. By that, the attacker can execute arbitrary code on the camera.	8.4	More Details
CVE-2024-48200	An issue in MobaXterm v24.2 allows a local attacker to escalate privileges and execute arbitrary code via the remove function of the MobaXterm MSI is spawning one Administrative cmd (conhost.exe)	8.4	More Details
CVE-2024-47797	in OpenHarmony v4.1.0 and prior versions allow a local attacker cause the common permission is upgraded to root and sensitive information leak through out-of-bounds write.	8.4	More Details
CVE-2024-47404	in OpenHarmony v4.1.0 and prior versions allow a local attacker cause the common permission is upgraded to root and sensitive information leak through double free.	8.4	More Details
CVE-2024-47137	in OpenHarmony v4.1.0 and prior versions allow a local attacker cause the common permission is upgraded to root and sensitive information leak through out-of-bounds write.	8.4	More Details
CVE-2024-20104	In da, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09073261; Issue ID: MSV-1772.	8.4	More Details
CVE-2024-51379	Stored Cross-Site Scripting (XSS) vulnerability discovered in JATOS v3.9.3. The vulnerability exists in the description component of the study section, where an attacker can inject JavaScript into the description field. This allows for the execution of malicious scripts when an admin views the description, potentially leading to account takeover and unauthorized actions.	8.4	More Details
CVE-2024-37573	The Talkatone com.talkatone.android application 8.4.6 for Android enables any installed application (with no permissions) to place phone calls without user interaction by sending a crafted intent via the com.talkatone.vedroid.ui.launcher.OutgoingCallInterceptor component.	8.4	More Details
CVE-2024-51380	Stored Cross-Site Scripting (XSS) vulnerability discovered in the Properties Component of JATOS v3.9.3. This flaw allows an attacker to inject malicious JavaScript into the properties section of a study, specifically within the UUID field. When an admin user accesses the study's properties, the injected script is executed in the admin's browser, which could lead to unauthorized actions, including account compromise and privilege escalation.	8.4	More Details
CVE-2024-51381	Cross-Site Request Forgery (CSRF) vulnerability in JATOS v3.9.3 that allows attackers to perform actions reserved for administrators, including creating admin accounts. This critical flaw can lead to unauthorized activities, compromising the security and integrity of the platform, especially if an attacker gains administrative control.	8.4	More Details
CVE-2024-51382	Cross-Site Request Forgery (CSRF) vulnerability in JATOS v3.9.3 allows an attacker to reset the administrator's password. This critical security flaw can result in unauthorized access to the platform, enabling attackers to hijack admin accounts and compromise the integrity and security of the system.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9459	Zohocorp ManageEngine Exchange Reporter Plus versions 5718 and prior are vulnerable to authenticated SQL Injection in reports module.	8.3	More Details
CVE-2024-10006	A vulnerability was identified in Consul and Consul Enterprise (“Consul”) such that using Headers in L7 traffic intentions could bypass HTTP header based access rules.	8.3	More Details
CVE-2024-48878	Zohocorp ManageEngine ADManager Plus versions 7241 and prior are vulnerable to SQL Injection in Archived Audit Report.	8.3	More Details
CVE-2024-36485	Zohocorp ManageEngine ADAudit Plus versions below 8121 are vulnerable to SQL Injection in Technician reports option.	8.3	More Details
CVE-2024-38744	Missing Authorization vulnerability in Upqode Plum: Spin Wheel & Email Pop-up allows Accessing Functionality Not Properly Constrained by ACLs, Stored XSS.This issue affects Plum: Spin Wheel & Email Pop-up: from n/a through 2.0.	8.3	More Details
CVE-2024-39720	An issue was discovered in Ollama before 0.1.46. An attacker can use two HTTP requests to upload a malformed GGUF file containing just 4 bytes starting with the GGUF custom magic header. By leveraging a custom Modelfile that includes a FROM statement pointing to the attacker-controlled blob file, the attacker can crash the application through the CreateModel route, leading to a segmentation fault (signal SIGSEGV: segmentation violation).	8.2	More Details
CVE-2024-38408	Cryptographic issue when a controller receives an LMP start encryption command under unexpected conditions.	8.2	More Details
CVE-2024-37470	Missing Authorization vulnerability in WofficeIO Woffice Core allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Woffice Core: from n/a through 5.4.8.	8.2	More Details
CVE-2024-37094	Missing Authorization vulnerability in StylemixThemes MasterStudy LMS allows Exploiting Incorrectly Configured Access Control Security Levels. This issue affects MasterStudy LMS: from n/a through 3.2.12.	8.2	More Details
CVE-2024-37106	Missing Authorization vulnerability in WishList Products WishList Member X allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WishList Member X: from n/a through 3.26.6	8.2	More Details
CVE-2024-51526	Permission control vulnerability in the hidebug module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	8.2	More Details
CVE-2024-10097	The Loginizer Security and Loginizer plugins for WordPress are vulnerable to authentication bypass in all versions up to, and including, 1.9.2. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email and the user does not have an already-existing account for the service returning the token.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28875	A security flaw involving hard-coded credentials in LevelOne WBR-6012's web services allows attackers to gain unauthorized access during the first 30 seconds post-boot. Other vulnerabilities can force a reboot, circumventing the initial time restriction for exploitation.The backdoor string can be found at address 0x80100910 80100910 40 6d 21 74 ds "@m!t2K1" 32 4b 31 00 It is referenced by the function located at 0x800b78b0 and is used as shown in the pseudocode below: if ((SECOND_FROM_BOOT_TIME < 300) && (is_equal = strcmp(password,"@m!t2K1")) { return 1;} Where 1 is the return value to admin-level access (0 being fail and 3 being user).	8.1	More Details
CVE-2024-51774	qBittorrent before 5.0.1 proceeds with use of https URLs even after certificate validation errors.	8.1	More Details
CVE-2024-10114	The WooCommerce - Social Login plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 2.7.7. This is due to insufficient verification on the user being returned by the social login token. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if they have access to the email and the user does not have an already-existing account for the service returning the token.	8.1	More Details
CVE-2024-48646	An Unrestricted File Upload vulnerability exists in Sage 1000 v7.0.0, which allows authorized users to upload files without proper validation. An attacker could exploit this vulnerability by uploading malicious files, such as HTML, scripts, or other executable content, that may be executed on the server, leading to further system compromise.	8.1	More Details
CVE-2024-42041	The com.videodownload.browser.videodownloader (aka AppTool-Browser-Video All Video Downloader) application 20-30.05.24 for Android allows an attacker to execute arbitrary JavaScript code via the acr.browser.lightning.DefaultBrowserActivity component.	8.1	More Details
CVE-2024-31151	A security flaw involving hard-coded credentials in LevelOne WBR-6012's web services allows attackers to gain unauthorized access during the first 30 seconds post-boot. Other vulnerabilities can force a reboot, circumventing the initial time restriction for exploitation.The password string can be found at addresses 0x 803cdd0f and 0x803da3e6: 803cdd0f 41 72 69 65 ds "AriesSerenaCairryNativitaMegan" 73 53 65 72 65 6e 61 43 ... It is referenced by the function at 0x800b78b0 and simplified in the pseudocode below: if (is_equal = strcmp(password,"AriesSerenaCairryNativitaMegan"){ ret = 3;} Where 3 is the return value to user-level access (0 being fail and 1 being admin/backdoor). While there's no legitimate functionality to change this password, once authenticated it is possible manually make a change by taking advantage of TALOS-2024-XXXXX using HTTP POST paramater "Pu" (new user password) in place of "Pa" (new admin password).	8.1	More Details
CVE-2024-10005	A vulnerability was identified in Consul and Consul Enterprise (“Consul”) such that using URL paths in L7 traffic intentions could bypass HTTP request path-based access rules.	8.1	More Details
CVE-2024-7059	A high-severity vulnerability that can lead to arbitrary code execution on the system hosting the Web SDK role was found in the Genetec Security Center product line.	8.0	More Details
CVE-2024-51009	Netgear R8500 v1.0.2.160 was discovered to contain a command injection vulnerability in the wan_gateway parameter at ether.cgi. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51021	Netgear XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 was discovered to contain a command injection vulnerability via the wan_gateway parameter at genie_fix2.cgi. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	8.0	More Details
CVE-2024-51024	D-Link DIR_823G 1.0.2B05 was discovered to contain a command injection vulnerability via the HostName parameter in the SetWanSettings function. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	8.0	More Details
CVE-2024-51251	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the backup function.	8.0	More Details
CVE-2024-50993	Netgear R8500 v1.0.2.160 was discovered to contain a command injection vulnerability in the sysNewPasswd parameter at admin_account.cgi. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	8.0	More Details
CVE-2024-51246	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the doPPTP function.	8.0	More Details
CVE-2024-51008	Netgear XR300 v1.0.3.78 was discovered to contain a command injection vulnerability in the system_name parameter at wiz_dyn.cgi. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	8.0	More Details
CVE-2024-51005	Netgear R8500 v1.0.2.160 was discovered to contain a command injection vulnerability in the share_name parameter at usb_remote_smb_conf.cgi. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	8.0	More Details
CVE-2024-45890	DrayTek Vigor3900 1.5.1.3 contains a post-authentication command injection vulnerability This vulnerability occurs when the `action` parameter in `cgi-bin/mainfunction.cgi` is set to `download_ovpn.`	8.0	More Details
CVE-2024-45891	DrayTek Vigor3900 1.5.1.3 contains a post-authentication command injection vulnerability. This vulnerability occurs when the `action` parameter in `cgi-bin/mainfunction.cgi` is set to `delete_wlan_profile.`	8.0	More Details
CVE-2024-45893	DrayTek Vigor3900 1.5.1.3 contains a post-authentication command injection vulnerability. This vulnerability occurs when the `action` parameter in `cgi-bin/mainfunction.cgi` is set to `setSWMOption.`	8.0	More Details
CVE-2024-51249	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the reboot function.	8.0	More Details
CVE-2024-52018	Netgear XR300 v1.0.3.78 was discovered to contain a command injection vulnerability in the system_name parameter at genie_dyn.cgi. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	8.0	More Details
CVE-2024-43383	Deserialization of Untrusted Data vulnerability in Apache Lucene.Net.Replicator. This issue affects Apache Lucene.NET's Replicator library: from 4.8.0-beta00005 through 4.8.0-beta00016. An attacker that can intercept traffic between a replication client and server, or control the target replication node URL, can provide a specially-crafted JSON response that is deserialized as an attacker-provided exception type. This can result in remote code execution or other potential unauthorized access. Users are recommended to upgrade to version 4.8.0-beta00017, which fixes the issue.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51010	Netgear R8500 v1.0.2.160, XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 were discovered to contain a command injection vulnerability in the component ap_mode.cgi via the apmode_gateway parameter. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	8.0	More Details
CVE-2024-45884	DrayTek Vigor3900 1.5.1.3 contains a post-authentication command injection vulnerability. This vulnerability occurs when the `action` parameter in `cgi-bin/mainfunction.cgi` is set to `setSWMGroup.`	8.0	More Details
CVE-2024-51253	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the doL2TP function.	8.0	More Details
CVE-2024-51240	An issue in the luci-mod-rpc package in OpenWRT Luci LTS allows for privilege escalation from an admin account to root via the JSON-RPC-API, which is exposed by the luci-mod-rpc package	8.0	More Details
CVE-2024-52019	Netgear R8500 v1.0.2.160 was discovered to contain a command injection vulnerability in the wan_gateway parameter at genie_fix2.cgi. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	8.0	More Details
CVE-2024-48093	Unrestricted File Upload in the Discussions tab in Operately v.0.1.0 allows a privileged user to achieve Remote Code Execution via uploading and executing malicious files without validating file extensions or content types.	8.0	More Details
CVE-2024-45887	DrayTek Vigor3900 1.5.1.3 contains a post-authentication command injection vulnerability. This vulnerability occurs when the `action` parameter in `cgi-bin/mainfunction.cgi` is set to `doOpenVPN.`	8.0	More Details
CVE-2024-45888	DrayTek Vigor3900 1.5.1.3 contains a command injection vulnerability. This vulnerability occurs when the `action` parameter in `cgi-bin/mainfunction.cgi` is set to `set_ap_map_config.'	8.0	More Details
CVE-2024-45882	DrayTek Vigor3900 1.5.1.3 contains a command injection vulnerability. This vulnerability occurs when the `action` parameter in `cgi-bin/mainfunction.cgi` is set to `delete_map_profile.`	8.0	More Details
CVE-2024-45885	DrayTek Vigor3900 1.5.1.3 contains a post-authentication command injection vulnerability. This vulnerability occurs when the `action` parameter in `cgi-bin/mainfunction.cgi` is set to `autodiscovery_clear.`	8.0	More Details
CVE-2024-52021	Netgear R8500 v1.0.2.160 was discovered to contain a command injection vulnerability in the wan_gateway parameter at bsw_fix.cgi. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	8.0	More Details
CVE-2024-45889	DrayTek Vigor3900 1.5.1.3 contains a post-authentication command injection vulnerability. This vulnerability occurs when the `action` parameter in `cgi-bin/mainfunction.cgi` is set to `commandTable.`	8.0	More Details
CVE-2024-52020	Netgear R8500 v1.0.2.160 was discovered to contain a command injection vulnerability in the wan_gateway parameter at wiz_fix2.cgi. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-52022	Netgear R8500 v1.0.2.160, XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 were discovered to contain a command injection vulnerability in the component wlg_adv.cgi via the apmode_gateway parameter. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	8.0	More Details
CVE-2024-50126	In the Linux kernel, the following vulnerability has been resolved: net: sched: use RCU read-side critical section in taprio_dump() Fix possible use-after-free in 'taprio_dump()' by adding RCU read-side critical section there. Never seen on x86 but found on a KASAN-enabled arm64 system when investigating https://syzkaller.appspot.com/bug?extid=b65e0af58423fc8a73aa: [T15862] BUG: KASAN: slab-use-after-free in taprio_dump+0xa0c/0xbb0 [T15862] Read of size 4 at addr ffff0000d4bb88f8 by task repro/15862 [T15862] [T15862] CPU: 0 UID: 0 PID: 15862 Comm: repro Not tainted 6.11.0-rc1-00293-gdefaf1a2113a-dirty #2 [T15862] Hardware name: QEMU QEMU Virtual Machine, BIOS edk2-20240524-5.fc40 05/24/2024 [T15862] Call trace: [T15862] dump_backtrace+0x20c/0x220 [T15862] show_stack+0x2c/0x40 [T15862] dump_stack_lvl+0xf8/0x174 [T15862] print_report+0x170/0x4d8 [T15862] kasan_report+0xb8/0x1d4 [T15862] __asan_report_load4_noabort+0x20/0x2c [T15862] taprio_dump+0xa0c/0xbb0 [T15862] tc_fill_qdisc+0x540/0x1020 [T15862] qdisc_notify.isra.0+0x330/0x3a0 [T15862] tc_modify_qdisc+0x7b8/0x1838 [T15862] rtnetlink_rcv_msg+0x3c8/0xc20 [T15862] netlink_rcv_skb+0x1f8/0x3d4 [T15862] rtnetlink_rcv+0x28/0x40 [T15862] netlink_unicast+0x51c/0x790 [T15862] netlink_sendmsg+0x79c/0xc20 [T15862] __sock_sendmsg+0xe0/0x1a0 [T15862] ____sys_sendmsg+0x6c0/0x840 [T15862] ___sys_sendmsg+0x1ac/0x1f0 [T15862] __sys_sendmsg+0x110/0x1d0 [T15862] __arm64_sys_sendmsg+0x74/0xb0 [T15862] invoke_syscall+0x88/0x2e0 [T15862] el0_svc_common.constprop.0+0xe4/0x2a0 [T15862] do_el0_svc+0x44/0x60 [T15862] el0_svc+0x50/0x184 [T15862] el0t_64_sync_handler+0x120/0x12c [T15862] el0t_64_sync+0x190/0x194 [T15862] [T15862] Allocated by task 15857: [T15862] kasan_save_stack+0x3c/0x70 [T15862] kasan_save_track+0x20/0x3c [T15862] kasan_save_alloc_info+0x40/0x60 [T15862] __kasan_kmalloc+0xd4/0xe0 [T15862] __kmalloc_cache_noprof+0x194/0x334 [T15862] taprio_change+0x45c/0x2fe0 [T15862] tc_modify_qdisc+0x6a8/0x1838 [T15862] rtnetlink_rcv_msg+0x3c8/0xc20 [T15862] netlink_rcv_skb+0x1f8/0x3d4 [T15862] rtnetlink_rcv+0x28/0x40 [T15862] netlink_unicast+0x51c/0x790 [T15862] netlink_sendmsg+0x79c/0xc20 [T15862] __sock_sendmsg+0xe0/0x1a0 [T15862] ____sys_sendmsg+0x6c0/0x840 [T15862] ___sys_sendmsg+0x1ac/0x1f0 [T15862] __sys_sendmsg+0x110/0x1d0 [T15862] __arm64_sys_sendmsg+0x74/0xb0 [T15862] invoke_syscall+0x88/0x2e0 [T15862] el0_svc_common.constprop.0+0xe4/0x2a0 [T15862] do_el0_svc+0x44/0x60 [T15862] el0_svc+0x50/0x184 [T15862] el0t_64_sync_handler+0x120/0x12c [T15862] el0t_64_sync+0x190/0x194 [T15862] [T15862] Freed by task 6192: [T15862] kasan_save_stack+0x3c/0x70 [T15862] kasan_save_track+0x20/0x3c [T15862] kasan_save_free_info+0x4c/0x80 [T15862] poison_slab_object+0x110/0x160 [T15862] __kasan_slab_free+0x3c/0x74 [T15862] kfree+0x134/0x3c0 [T15862] taprio_free_sched_cb+0x18c/0x220 [T15862] rcu_core+0x920/0x1b7c [T15862] rcu_core_si+0x10/0x1c [T15862] handle_softirqs+0x2e8/0xd64 [T15862] __do_softirq+0x14/0x20	7.8	More Details
CVE-2024-38421	Memory corruption while processing GPU commands.	7.8	More Details
CVE-2024-38419	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38415	Memory corruption while handling session errors from firmware.	7.8	More Details
CVE-2024-38410	Memory corruption while IOCLT is called when device is in invalid state and the WMI command buffer may be freed twice.	7.8	More Details
CVE-2024-50130	In the Linux kernel, the following vulnerability has been resolved: netfilter: bpf: must hold reference on net namespace BUG: KASAN: slab-use-after-free in __nf_unregister_net_hook+0x640/0x6b0 Read of size 8 at addr ffff8880106fe400 by task repro/72= bpf_nf_link_release+0xda/0x1e0 bpf_link_free+0x139/0x2d0 bpf_link_release+0x68/0x80 __fput+0x414/0xb60 Eric says: It seems that bpf was able to defer the __nf_unregister_net_hook() after exit()/close() time. Perhaps a netns reference is missing, because the netns has been dismantled/freed already. bpf_nf_link_attach() does : link->net = net; But I do not see a reference being taken on net. Add such a reference and release it after hook unreg. Note that I was unable to get syzbot reproducer to work, so I do not know if this resolves this splat.	7.8	More Details
CVE-2024-50124	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: Fix UAF on iso_sock_timeout conn->sk maybe have been unlinked/freed while waiting for iso_conn_lock so this checks if the conn->sk is still valid by checking if it part of iso_sk_list.	7.8	More Details
CVE-2024-50129	In the Linux kernel, the following vulnerability has been resolved: net: pse-pd: Fix out of bound for loop Adjust the loop limit to prevent out-of-bounds access when iterating over PI structures. The loop should not reach the index pcdev->nr_lines since we allocate exactly pcdev->nr_lines number of PI structures. This fix ensures proper bounds are maintained during iterations.	7.8	More Details
CVE-2024-50125	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: SCO: Fix UAF on sco_sock_timeout conn->sk maybe have been unlinked/freed while waiting for sco_conn_lock so this checks if the conn->sk is still valid by checking if it part of sco_sk_list.	7.8	More Details
CVE-2024-9632	A flaw was found in the X.org server. Due to improperly tracked allocation size in _XkbSetCompatMap, a local attacker may be able to trigger a buffer overflow condition via a specially crafted payload, leading to denial of service or local privilege escalation in distributions where the X.org server is run with root privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50114	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Unregister redistributor for failed vCPU creation Alex reports that syzkaller has managed to trigger a use-after-free when tearing down a VM: BUG: KASAN: slab-use-after-free in kvm_put_kvm+0x300/0xe68 virt/kvm/kvm_main.c:5769 Read of size 8 at addr ffffff801c6890d0 by task syz.3.2219/10758 CPU: 3 UID: 0 PID: 10758 Comm: syz.3.2219 Not tainted 6.11.0-rc6-dirty #64 Hardware name: linux,dummy-virt (DT) Call trace: dump_backtrace+0x17c/0x1a8 arch/arm64/kernel/stacktrace.c:317 show_stack+0x2c/0x3c arch/arm64/kernel/stacktrace.c:324 __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x94/0xc0 lib/dump_stack.c:119 print_report+0x144/0x7a4 mm/kasan/report.c:377 kasan_report+0xcc/0x128 mm/kasan/report.c:601 __asan_report_load8_noabort+0x20/0x2c mm/kasan/report_generic.c:381 kvm_put_kvm+0x300/0xe68 virt/kvm/kvm_main.c:5769 kvm_vm_release+0x4c/0x60 virt/kvm/kvm_main.c:1409 __fput+0x198/0x71c fs/file_table.c:422 ____fput+0x20/0x30 fs/file_table.c:450 task_work_run+0x1cc/0x23c kernel/task_work.c:228 do_notify_resume+0x144/0x1a0 include/linux/resume_user_mode.h:50 el0_svc+0x64/0x68 arch/arm64/kernel/entry-common.c:169 el0t_64_sync_handler+0x90/0xfc arch/arm64/kernel/entry-common.c:730 el0t_64_sync+0x190/0x194 arch/arm64/kernel/entry.S:598 Upon closer inspection, it appears that we do not properly tear down the MMIO registration for a vCPU that fails creation late in the game, e.g. a vCPU w/ the same ID already exists in the VM. It is important to consider the context of commit that introduced this bug by moving the unregistration out of __kvm_vgic_vcpu_destroy(). That change correctly sought to avoid an srcu v. config_lock inversion by breaking up the vCPU teardown into two parts, one guarded by the config_lock. Fix the use-after-free while avoiding lock inversion by adding a special-cased unregistration to __kvm_vgic_vcpu_destroy(). This is safe because failed vCPUs are torn down outside of the config_lock.	7.8	More Details
CVE-2024-38422	Memory corruption while processing voice packet with arbitrary data received from ADSP.	7.8	More Details
CVE-2024-9419	Client / Server PCs with the HP Smart Universal Printing Driver installed are potentially vulnerable to Remote Code Execution and/or Elevation of Privilege. A client using the HP Smart Universal Printing Driver that sends a print job comprised of a malicious XPS file could potentially lead to Remote Code Execution and/or Elevation of Privilege on the PC.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50121	In the Linux kernel, the following vulnerability has been resolved: nfsd: cancel nfsd_shrinker_work using sync mode in nfs4_state_shutdown_net In the normal case, when we excute `echo 0 > /proc/fs/nfsd/threads`, the function `nfs4_state_destroy_net` in `nfs4_state_shutdown_net` will release all resources related to the hashed `nfs4_client`. If the `nfsd_client_shrinker` is running concurrently, the `expire_client` function will first unhash this client and then destroy it. This can lead to the following warning. Additionally, numerous use-after-free errors may occur as well. nfsd_client_shrinker echo 0 > /proc/fs/nfsd/threads expire_client nfsd_shutdown_net unhash_client ... nfs4_state_shutdown_net /* won't wait shrinker exit */ /* cancel_work(&nn->nfsd_shrinker_work) * nfsd_file for this /* won't destroy unhashed client1 */ * client1 still alive nfs4_state_destroy_net */ nfsd_file_cache_shutdown /* trigger warning */ kmem_cache_destroy(nfsd_file_slab) kmem_cache_destroy(nfsd_file_mark_slab) /* release nfsd_file and mark */ __destroy_client ======== BUG nfsd_file (Not tainted): Objects remaining in nfsd_file on __kmem_cache_shutdown() ---------- CPU: 4 UID: 0 PID: 764 Comm: sh Not tainted 6.12.0-rc3+ #1 dump_stack_lvl+0x53/0x70 slab_err+0xb0/0xf0 __kmem_cache_shutdown+0x15c/0x310 kmem_cache_destroy+0x66/0x160 nfsd_file_cache_shutdown+0xac/0x210 [nfsd] nfsd_destroy_serv+0x251/0x2a0 [nfsd] nfsd_svc+0x125/0x1e0 [nfsd] write_threads+0x16a/0x2a0 [nfsd] nfsctl_transaction_write+0x74/0xa0 [nfsd] vfs_write+0x1a5/0x6d0 ksys_write+0xc1/0x160 do_syscall_64+0x5f/0x170 entry_SYSCALL_64_after_hwframe+0x76/0x7e ======== BUG nfsd_file_mark (Tainted: G B W): Objects remaining nfsd_file_mark on __kmem_cache_shutdown() ---------- dump_stack_lvl+0x53/0x70 slab_err+0xb0/0xf0 __kmem_cache_shutdown+0x15c/0x310 kmem_cache_destroy+0x66/0x160 nfsd_file_cache_shutdown+0xc8/0x210 [nfsd] nfsd_destroy_serv+0x251/0x2a0 [nfsd] nfsd_svc+0x125/0x1e0 [nfsd] write_threads+0x16a/0x2a0 [nfsd] nfsctl_transaction_write+0x74/0xa0 [nfsd] vfs_write+0x1a5/0x6d0 ksys_write+0xc1/0x160 do_syscall_64+0x5f/0x170 entry_SYSCALL_64_after_hwframe+0x76/0x7e To resolve this issue, cancel `nfsd_shrinker_work` using synchronous mode in nfs4_state_shutdown_net.	7.8	More Details
CVE-2024-38409	Memory corruption while station LL statistic handling.	7.8	More Details
CVE-2024-38423	Memory corruption while processing GPU page table switch.	7.8	More Details
CVE-2024-7995	A maliciously crafted binary file when downloaded could lead to escalation of privileges to NT AUTHORITY/SYSTEM due to an untrusted search path being utilized in the VRED Design application. Exploitation of this vulnerability may lead to code execution.	7.8	More Details
CVE-2024-38424	Memory corruption during GNSS HAL process initialization.	7.8	More Details
CVE-2024-38407	Memory corruption while processing input parameters for any IOCTL call in the JPEG Encoder driver.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38406	Memory corruption while handling IOCTL calls in JPEG Encoder driver.	7.8	More Details
CVE-2024-49522	Substance3D - Painter versions 10.0.1 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-2024-50131	In the Linux kernel, the following vulnerability has been resolved: tracing: Consider the NULL character when validating the event length strlen() returns a string length excluding the null byte. If the string length equals to the maximum buffer length, the buffer will have no space for the NULL terminating character. This commit checks this condition and returns failure for it.	7.8	More Details
CVE-2024-50127	In the Linux kernel, the following vulnerability has been resolved: net: sched: fix use-after-free in taprio_change() In 'taprio_change()', 'admin' pointer may become dangling due to sched switch / removal caused by 'advance_sched()', and critical section protected by 'q->current_entry_lock' is too small to prevent from such a scenario (which causes use-after-free detected by KASAN). Fix this by prefer 'rcu_replace_pointer()' over 'rcu_assign_pointer()' to update 'admin' immediately before an attempt to schedule freeing.	7.8	More Details
CVE-2024-50112	In the Linux kernel, the following vulnerability has been resolved: x86/lam: Disable ADDRESS_MASKING in most cases Linear Address Masking (LAM) has a weakness related to transient execution as described in the SLAM paper[1]. Unless Linear Address Space Separation (LASS) is enabled this weakness may be exploitable. Until kernel adds support for LASS[2], only allow LAM for COMPILE_TEST, or when speculation mitigations have been disabled at compile time, otherwise keep LAM disabled. There are no processors in market that support LAM yet, so currently nobody is affected by this issue. [1] SLAM: https://download.vusec.net/papers/slam_sp24.pdf [2] LASS: https://lore.kernel.org/lkml/20230609183632.48706-1-alexander.shishkin@linux.intel.com/ [dhansen: update SPECULATION_MITIGATIONS -> CPU_MITIGATIONS]	7.8	More Details
CVE-2024-37108	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WishList Products WishList Member X allows Path Traversal.This issue affects WishList Member X: from n/a through 3.26.6.	7.7	More Details
CVE-2024-48735	Directory Traversal in /SASStudio/sasexec/sessions/{sessionID}/workspace/{InternalPath} in SAS Studio 9.4 allows remote attacker to access internal files by manipulating default path during file download. NOTE: this is disputed by the vendor because these filesystem paths are allowed for authorized users.	7.7	More Details
CVE-2024-51510	Out-of-bounds access vulnerability in the logo module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	7.6	More Details
CVE-2024-51672	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPDeveloper BetterLinks allows SQL Injection.This issue affects BetterLinks: from n/a through 2.1.7.	7.6	More Details
CVE-2024-23385	Transient DOS as modem reset occurs when an unexpected MAC RAR (with invalid PDU length) is seen at UE.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3935	In Eclipse Mosquito, versions from 2.0.0 through 2.0.18, if a Mosquitto broker is configured to create an outgoing bridge connection, and that bridge connection has an incoming topic configured that makes use of topic remapping, then if the remote connection sends a crafted PUBLISH packet to the broker a double free will occur with a subsequent crash of the broker.	7.5	More Details
CVE-2024-51582	Path Traversal: '.../...//' vulnerability in ThimPress WP Hotel Booking allows PHP Local File Inclusion.This issue affects WP Hotel Booking: from n/a through 2.1.4.	7.5	More Details
CVE-2024-33700	The LevelOne WBR-6012 router firmware R0.40e6 suffers from an input validation vulnerability within its FTP functionality, enabling attackers to cause a denial of service through a series of malformed FTP commands. This can lead to device reboots and service disruption.	7.5	More Details
CVE-2024-33068	Transient DOS while parsing fragments of MBSSID IE from beacon frame.	7.5	More Details
CVE-2024-38405	Transient DOS while processing the CU information from RNR IE.	7.5	More Details
CVE-2024-50528	Exposure of Sensitive System Information to an Unauthorized Control Sphere vulnerability in Stacks Stacks Mobile App Builder allows Retrieve Embedded Sensitive Data.This issue affects Stacks Mobile App Builder: from n/a through 5.2.3.	7.5	More Details
CVE-2024-51739	Combodo iTop is a simple, web based IT Service Management tool. Unauthenticated user can perform users enumeration, which can make it easier to bruteforce a valid account. As a fix the sentence displayed after resetting password no longer shows if the user exists or not. This fix is included in versions 2.7.11, 3.0.5, 3.1.2, and 3.2.0. Users are advised to upgrade. Users unable to upgrade may overload the dictionary entry `"UI:ResetPwd-Error-WrongLogin"` through an extension and replace it with a generic message.	7.5	More Details
CVE-2024-51326	SQL Injection vulnerability in projectworlds Travel management System v.1.0 allows a remote attacker to execute arbitrary code via the 't2' parameter in deletesubcategory.php.	7.5	More Details
CVE-2024-38403	Transient DOS while parsing BTM ML IE when per STA profile is not included.	7.5	More Details
CVE-2024-48270	An issue in the component /logins of oasys v1.1 allows attackers to access sensitive information via a burst attack.	7.5	More Details
CVE-2024-37277	Authorization Bypass Through User-Controlled Key vulnerability in Paid Memberships Pro allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Paid Memberships Pro: from n/a through 3.0.4.	7.5	More Details
CVE-2024-48352	Yealink Meeting Server before V26.0.0.67 is vulnerable to sensitive data exposure in the server response via sending HTTP request with enterprise ID.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43158	Missing Authorization vulnerability in Masteriyo Masteriyo - LMS allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Masteriyo - LMS: from n/a through 1.11.4.	7.5	More Details
CVE-2024-48353	Yealink Meeting Server before V26.0.0.67 allows attackers to obtain static key information from a front-end JS file and decrypt the plaintext passwords based on the obtained key information.	7.5	More Details
CVE-2024-22733	TP Link MR200 V4 Firmware version 210201 was discovered to contain a null-pointer-dereference in the web administration panel on /cgi/login via the sign, Action or LoginStatus query parameters which could lead to a denial of service by a local or remote unauthenticated attacker.	7.5	More Details
CVE-2024-8185	Vault Community and Vault Enterprise (“Vault”) clusters using Vault’s Integrated Storage backend are vulnerable to a denial-of-service (DoS) attack through memory exhaustion through a Raft cluster join API endpoint . An attacker may send a large volume of requests to the endpoint which may cause Vault to consume excessive system memory resources, potentially leading to a crash of the underlying system and the Vault process itself. This vulnerability, CVE-2024-8185, is fixed in Vault Community 1.18.1 and Vault Enterprise 1.18.1, 1.17.8, and 1.16.12.	7.5	More Details
CVE-2024-51561	This vulnerability exists in Aero due to improper implementation of OTP validation mechanism in certain API endpoints. An authenticated remote attacker could exploit this vulnerability by intercepting and manipulating the responses exchanged during the second factor authentication process. Successful exploitation of this vulnerability could allow the attacker to bypass OTP verification for accessing other user accounts.	7.5	More Details
CVE-2024-40490	An issue in Sourcebans++ before v.1.8.0 allows a remote attacker to obtain sensitive information via a crafted XAJAX call to the Forgot Password function.	7.5	More Details
CVE-2024-9579	A potential vulnerability was discovered in certain Poly video conferencing devices. The firmware flaw does not properly sanitize user input. The exploitation of this vulnerability is dependent on a layered attack and cannot be exploited by itself.	7.5	More Details
CVE-2024-50508	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Chetan Khandla Woocommerce Product Design allows Path Traversal.This issue affects Woocommerce Product Design: from n/a through 1.0.0.	7.5	More Details
CVE-2024-51066	An Insecure Direct Object Reference (IDOR) vulnerability in appointment-detail.php in Phpgurukul's Beauty Parlour Management System v1.1 allows unauthorized access to the Personally Identifiable Information (PII) of other customers.	7.5	More Details
CVE-2024-39719	An issue was discovered in Ollama through 0.3.14. File existence disclosure can occur via api/create. When calling the CreateModel route with a path parameter that does not exist, it reflects the "File does not exist" error message to the attacker, providing a primitive for file existence on the server.	7.5	More Details
CVE-2024-39721	An issue was discovered in Ollama before 0.1.34. The CreateModelHandler function uses os.Open to read a file until completion. The req.Path parameter is user-controlled and can be set to /dev/random, which is blocking, causing the goroutine to run infinitely (even after the HTTP request is aborted by the client).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39722	An issue was discovered in Ollama before 0.1.46. It exposes which files exist on the server on which it is deployed via path traversal in the api/push route.	7.5	More Details
CVE-2024-48360	Qualitor v8.24 was discovered to contain a Server-Side Request Forgery (SSRF) via the component /request/viewValidacao.php.	7.5	More Details
CVE-2024-38726	Missing Authorization vulnerability in PickPlugins Product Designer allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Product Designer: from n/a through 1.0.33.	7.5	More Details
CVE-2024-48809	An issue in Open Networking Foundations sdran-in-a-box v.1.4.3 and onos-a1t v.0.2.3 allows a remote attacker to cause a denial of service via the onos-a1t component of the sdran-in-a-box, specifically the DeleteWatcher function.	7.5	More Details
CVE-2024-43212	Missing Authorization vulnerability in MagePeople Team WpTravelly allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WpTravelly: from n/a through 1.7.7.	7.5	More Details
CVE-2024-30619	Chamilo LMS Version 1.11.26 is vulnerable to Incorrect Access Control. A non-authenticated attacker can request the number of messages and the number of online users via "/main/inc/ajax/message.ajax.php?a=get_count_message" AND "/main/inc/ajax/online.ajax.php?a=get_users_online."	7.5	More Details
CVE-2024-10791	A vulnerability, which was classified as critical, has been found in Codezips Hospital Appointment System 1.0. This issue affects some unknown processing of the file /doctorAction.php. The manipulation of the argument Name leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions contradicting file and parameter names to be affected.	7.3	More Details
CVE-2024-10844	A vulnerability, which was classified as critical, was found in 1000 Projects Bookstore Management System 1.0. This affects an unknown part of the file search.php. The manipulation of the argument s 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-2024-10739	A vulnerability, which was classified as critical, has been found in code-projects E-Health Care System 1.0. Affected by this issue is some unknown functionality of the file /Admin/adminlogin.php. The manipulation of the argument email/admin_pswd as part of String leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "email" to be affected. But it must be assumed that parameter "admin_pswd" is affected as well.	7.3	More Details
CVE-2024-9846	The The Enable Shortcodes inside Widgets,Comments and Experts plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.0.0. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10556	A vulnerability, which was classified as critical, was found in Codezips Pet Shop Management System 1.0. Affected is an unknown function of the file birdsadd.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.	7.3	More Details
CVE-2024-10561	A vulnerability was found in Codezips Pet Shop Management System 1.0. It has been classified as critical. This affects an unknown part of the file birdsupdate.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10509	A vulnerability, which was classified as critical, has been found in Codezips Online Institute Management System 1.0. This issue affects some unknown processing of the file /login.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10845	A vulnerability has been found in 1000 Projects Bookstore Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file book_detail.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10699	A vulnerability was found in code-projects Wazifa System 1.0. It has been classified as critical. This affects an unknown part of the file /controllers/logincontrol.php. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10702	A vulnerability classified as critical has been found in code-projects Simple Car Rental System 1.0. Affected is an unknown function of the file /signup.php. The manipulation of the argument fname leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10263	The Tickera – WordPress Event Ticketing plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 3.5.4.4. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-10733	A vulnerability was found in code-projects Restaurant Order System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /login.php. The manipulation of the argument uid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10736	A vulnerability was found in Codezips Free Exam Hall Seating Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /student.php. The manipulation of the argument email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10507	A vulnerability classified as critical was found in Codezips Free Exam Hall Seating Management System 1.0. This vulnerability affects unknown code of the file /login.php. The manipulation of the argument email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10737	A vulnerability classified as critical has been found in Codezips Free Exam Hall Seating Management System 1.0. Affected is an unknown function of the file /teacher.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10741	A vulnerability has been found in code-projects E-Health Care System 1.0 and classified as critical. This vulnerability affects unknown code of the file /Users/registration.php. The manipulation of the argument f_name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	7.3	More Details
CVE-2024-10752	A vulnerability was found in Codezips Pet Shop Management System 1.0. It has been classified as critical. This affects an unknown part of the file /productsadd.php. The manipulation of the argument id/name leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions contradicting file names to be affected.	7.3	More Details
CVE-2024-39650	Missing Authorization vulnerability in WPWeb Elite WooCommerce PDF Vouchers allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WooCommerce PDF Vouchers: from n/a through 4.9.4.	7.3	More Details
CVE-2024-39664	Missing Authorization vulnerability in YMC Filter & Grids allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Filter & Grids: from n/a through 2.8.33.	7.3	More Details
CVE-2024-10758	A vulnerability, which was classified as critical, was found in code-projects/anirbandutta9 Content Management System and News-Buzz 1.0. This affects an unknown part of the file /index.php. The manipulation of the argument user_name leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. This product is distributed under two entirely different names.	7.3	More Details
CVE-2024-10607	A vulnerability was found in code-projects Courier Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /track-result.php. The manipulation of the argument Consignment leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10608	A vulnerability was found in code-projects Courier Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /login.php. The manipulation of the argument txtusername leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-10600	A vulnerability, which was classified as critical, was found in Tongda OA 2017 up to 11.6. Affected is an unknown function of the file pda/appcenter/submenu.php. The manipulation of the argument appid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-47253	In 2N Access Commander versions 3.1.1.2 and prior, a Path Traversal vulnerability could allow an attacker with administrative privileges to write files on the filesystem and potentially achieve arbitrary remote code execution. This vulnerability cannot be exploited by users with lower privilege roles.	7.2	More Details
CVE-2024-10653	IDExpert from CHANGING Information Technology does not properly validate a specific parameter in the administrator interface, allowing remote attackers with administrative privileges to inject and execute OS commands on the server.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47461	An authenticated command injection vulnerability exists in the Instant AOS-8 and AOS-10 command line interface. A successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying host operating system.	7.2	More Details
CVE-2024-47462	An arbitrary file creation vulnerability exists in the Instant AOS-8 and AOS-10 command line interface. Successful exploitation of this vulnerability could allow an authenticated remote attacker to create arbitrary files, which could lead to a remote command execution (RCE) on the underlying operating system.	7.2	More Details
CVE-2024-47463	An arbitrary file creation vulnerability exists in the Instant AOS-8 and AOS-10 command line interface. Successful exploitation of this vulnerability could allow an authenticated remote attacker to create arbitrary files, which could lead to a remote command execution (RCE) on the underlying operating system.	7.2	More Details
CVE-2024-51243	The eladmin v2.7 and before contains a remote code execution (RCE) vulnerability that can control all application deployment servers of this management system via DeployController.java.	7.2	More Details
CVE-2023-52066	http.zig commit 76cf5 was discovered to contain a CRLF injection vulnerability via the url parameter.	7.2	More Details
CVE-2024-49774	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. SuiteCRM relies on the blacklist of functions/methods to prevent installation of malicious MLPs. But this checks can be bypassed with some syntax constructions. SuiteCRM uses token_get_all to parse PHP scripts and check the resulted AST against blacklists. But it doesn't take into account all scenarios. This issue has been addressed in versions 7.14.6 and 8.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.2	More Details
CVE-2024-48647	A file disclosure vulnerability exists in Sage 1000 v7.0.0. This vulnerability allows remote attackers to retrieve arbitrary files from the server's file system by manipulating the URL parameter in HTTP requests. The attacker can exploit this flaw to access sensitive information, including configuration files that may contain credentials and system settings, which could lead to further compromise of the server.	7.2	More Details
CVE-2024-10108	The WPAdverts – Classifieds Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's adverts_add shortcode in all versions up to, and including, 2.1.6 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2024-47314	Missing Authorization vulnerability in WP Sunshine Sunshine Photo Cart allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sunshine Photo Cart: from n/a through 3.2.8.	7.1	More Details
CVE-2024-27524	Cross Site Scripting vulnerability in Chamilo LMS v.1.11.26 allows a remote attacker to escalate privileges via a crafted script to the filename parameter of the new_ticket.php component.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50128	In the Linux kernel, the following vulnerability has been resolved: net: wwan: fix global oob in wwan_rtnl_policy The variable wwan_rtnl_link_ops assign a *bigger* maxtype which leads to a global out-of-bounds read when parsing the netlink attributes. Exactly same bug cause as the oob fixed in commit b33fb5b801c6 ("net: qualcomm: rmnet: fix global oob in rmnet_policy"). == BUG: KASAN: global-out-of-bounds in validate_nla lib/nlattr.c:388 [inline] BUG: KASAN: global-out-of-bounds in __nla_validate_parse+0x19d7/0x29a0 lib/nlattr.c:603 Read of size 1 at addr ffffffff8b09cb60 by task syz.1.66276/323862 CPU: 0 PID: 323862 Comm: syz.1.66276 Not tainted 6.1.70 #1 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.13.0-1ubuntu1.1 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x177/0x231 lib/dump_stack.c:106 print_address_description mm/kasan/report.c:284 [inline] print_report+0x14f/0x750 mm/kasan/report.c:395 kasan_report+0x139/0x170 mm/kasan/report.c:495 validate_nla lib/nlattr.c:388 [inline] __nla_validate_parse+0x19d7/0x29a0 lib/nlattr.c:603 __nla_parse+0x3c/0x50 lib/nlattr.c:700 nla_parse_nested_deprecated include/net/netlink.h:1269 [inline] __rtnl_newlink net/core/rtnetlink.c:3514 [inline] rtnl_newlink+0x7bc/0x1fd0 net/core/rtnetlink.c:3623 rtnetlink_rcv_msg+0x794/0xef0 net/core/rtnetlink.c:6122 netlink_rcv_skb+0x1de/0x420 net/netlink/af_netlink.c:2508 netlink_unicast_kernel net/netlink/af_netlink.c:1326 [inline] netlink_unicast+0x74b/0x8c0 net/netlink/af_netlink.c:1352 netlink_sendmsg+0x882/0xb90 net/netlink/af_netlink.c:1874 sock_sendmsg_nosec net/socket.c:716 [inline] __sock_sendmsg net/socket.c:728 [inline] ____sys_sendmsg+0x5cc/0x8f0 net/socket.c:2499 ___sys_sendmsg+0x21c/0x290 net/socket.c:2553 __sys_sendmsg net/socket.c:2582 [inline] __do_sys_sendmsg net/socket.c:2591 [inline] __se_sys_sendmsg+0x19e/0x270 net/socket.c:2589 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x45/0x90 arch/x86/entry/common.c:81 entry_SYSCALL_64_after_hwframe+0x63/0xcd RIP: 0033:0x7f67b19a24ad RSP: 002b:00007f67b17febb8 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f67b1b45f80 RCX: 00007f67b19a24ad RDX: 0000000000000000 RSI: 0000000020005e40 RDI: 0000000000000004 RBP: 00007f67b1a1e01d R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007ffd2513764f R14: 00007ffd251376e0 R15: 00007f67b17fed40 </TASK> The buggy address belongs to the variable: wwan_rtnl_policy+0x20/0x40 The buggy address belongs to the physical page: page:ffffea00002c2700 refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0xb09c flags: 0xfff00000001000(reservedlnode=0lzone=1llastcpupid=0x7ff) raw: 00fff00000001000 ffffea00002c2708 ffffea00002c2708 0000000000000000 raw: 0000000000000000 0000000000000000 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected page_owner info is not present (never set?) Memory state around the buggy address: ffffffff8b09ca00: 05 f9 f9 f9 05 f9 f9 f9 00 01 f9 f9 00 01 f9 f9 ffffffff8b09ca80: 00 00 00 05 f9 f9 f9 f9 00 00 03 f9 f9 f9 f9 f9 >ffffffff8b09cb00: 00 00 00 00 05 f9 f9 f9 00 00 00 00 f9 f9 f9 f9 ^ ffffffff8b09cb80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 == According to the comment of `nla_parse_nested_deprecated`, use correct size `IFLA_WWAN_MAX` here to fix this issue.	7.1	More Details
CVE-2024-50123	In the Linux kernel, the following vulnerability has been resolved: bpf: Add the missing BPF_LINK_TYPE invocation for sockmap There is an out-of-bounds read in bpf_link_show_fdinfo() for the sockmap link fd. Fix it by adding the missing BPF_LINK_TYPE invocation for sockmap link Also add comments for bpf_link_type to prevent missing updates in the future.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50115	In the Linux kernel, the following vulnerability has been resolved: KVM: nSVM: Ignore nCR3[4:0] when loading PDPTEs from memory Ignore nCR3[4:0] when loading PDPTEs from memory for nested SVM, as bits 4:0 of CR3 are ignored when PAE paging is used, and thus VMRUN doesn't enforce 32-byte alignment of nCR3. In the absolute worst case scenario, failure to ignore bits 4:0 can result in an out-of-bounds read, e.g. if the target page is at the end of a memslot, and the VMM isn't using guard pages. Per the APM: The CR3 register points to the base address of the page-directory-pointer table. The page-directory-pointer table is aligned on a 32-byte boundary, with the low 5 address bits 4:0 assumed to be 0. And the SDM's much more explicit: 4:0 Ignored Note, KVM gets this right when loading PDPTRs, it's only the nSVM flow that is broken.	7.1	More Details
CVE-2024-9191	The Okta Device Access features, provided by the Okta Verify agent for Windows, provides access to the OktaDeviceAccessPipe, which enables attackers in a compromised device to retrieve passwords associated with Desktop MFA passwordless logins. The vulnerability was discovered via routine penetration testing. Note: A precondition of this vulnerability is that the user must be using the Okta Device Access passwordless feature. Okta Device Access users not using passwordless are not affected, and customers only using Okta Verify on platforms other than Windows, or only using FastPass are not affected.	7.1	More Details
CVE-2024-51523	Information management vulnerability in the Gallery module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	7.1	More Details
CVE-2024-43235	Missing Authorization vulnerability in MetaBox.Io Meta Box – WordPress Custom Fields Framework allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Meta Box – WordPress Custom Fields Framework: from n/a through 5.9.10.	7.1	More Details
CVE-2024-38721	Missing Authorization vulnerability in spider-themes EazyDocs allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects EazyDocs: from n/a through 2.5.0.	7.1	More Details
CVE-2024-51127	An issue in the createTempFile method of hornetq v2.4.9 allows attackers to arbitrarily overwrite files or access sensitive information.	7.1	More Details
CVE-2024-45164	Akamai SIA (Secure Internet Access Enterprise) ThreatAvert, in SPS (Security and Personalization Services) before the latest 19.2.0 patch and Apps Portal before 19.2.0.3 or 19.2.0.20240814, has incorrect authorization controls for the Admin functionality on the ThreatAvert Policy page. An authenticated user can navigate directly to the /#app/intelligence/threatAvertPolicies URI and disable policy enforcement.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50106	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix race between laundromat and free_stateid There is a race between laundromat handling of revoked delegations and a client sending free_stateid operation. Laundromat thread finds that delegation has expired and needs to be revoked so it marks the delegation stid revoked and it puts it on a reaper list but then it unlock the state lock and the actual delegation revocation happens without the lock. Once the stid is marked revoked a racing free_stateid processing thread does the following (1) it calls list_del_init() which removes it from the reaper list and (2) frees the delegation stid structure. The laundromat thread ends up not calling the revoke_delegation() function for this particular delegation but that means it will no release the lock lease that exists on the file. Now, a new open for this file comes in and ends up finding that lease list isn't empty and calls nfsd_breaker_owns_lease() which ends up trying to derefence a freed delegation stateid. Leading to the followint use-after-free KASAN warning: kernel: == kernel: BUG: KASAN: slab-use-after-free in nfsd_breaker_owns_lease+0x140/0x160 [nfsd] kernel: Read of size 8 at addr ffff0000e73cd0c8 by task nfsd/6205 kernel: kernel: CPU: 2 UID: 0 PID: 6205 Comm: nfsd Kdump: loaded Not tainted 6.11.0-rc7+ #9 kernel: Hardware name: Apple Inc. Apple Virtualization Generic Platform, BIOS 2069.0.0.0.0 08/03/2024 kernel: Call trace: kernel: dump_backtrace+0x98/0x120 kernel: show_stack+0x1c/0x30 kernel: dump_stack_lvl+0x80/0xe8 kernel: print_address_description.constprop.0+0x84/0x390 kernel: print_report+0xa4/0x268 kernel: kasan_report+0xb4/0xf8 kernel: __asan_report_load8_noabort+0x1c/0x28 kernel: nfsd_breaker_owns_lease+0x140/0x160 [nfsd] kernel: nfsd_file_do_acquire+0xb3c/0x11d0 [nfsd] kernel: nfsd_file_acquire_opened+0x84/0x110 [nfsd] kernel: nfs4_get_vfs_file+0x634/0x958 [nfsd] kernel: nfsd4_process_open2+0xa40/0x1a40 [nfsd] kernel: nfsd4_open+0xa08/0xe80 [nfsd] kernel: nfsd4_proc_compound+0xb8c/0x2130 [nfsd] kernel: nfsd_dispatch+0x22c/0x718 [nfsd] kernel: svc_process_common+0x8e8/0x1960 [sunrpc] kernel: svc_process+0x3d4/0x7e0 [sunrpc] kernel: svc_handle_xprt+0x828/0xe10 [sunrpc] kernel: svc_recv+0x2cc/0x6a8 [sunrpc] kernel: nfsd+0x270/0x400 [nfsd] kernel: kthread+0x288/0x310 kernel: ret_from_fork+0x10/0x20 This patch proposes a fixed that's based on adding 2 new additional stid's sc_status values that help coordinate between the laundromat and other operations (nfsd4_free_stateid() and nfsd4_delegreturn()). First to make sure, that once the stid is marked revoked, it is not removed by the nfsd4_free_stateid(), the laundromat take a reference on the stateid. Then, coordinating whether the stid has been put on the cl_revoked list or we are processing FREE_STATEID and need to make sure to remove it from the list, each check that state and act accordingly. If laundromat has added to the cl_revoke list before the arrival of FREE_STATEID, then nfsd4_free_stateid() knows to remove it from the list. If nfsd4_free_stateid() finds that operations arrived before laundromat has placed it on cl_revoke list, it marks the state freed and then laundromat will no longer add it to the list. Also, for nfsd4_delegreturn() when looking for the specified stid, we need to access stid that are marked removed or freeable, it means the laundromat has started processing it but hasn't finished and this delegreturn needs to return nfserr_deleg_revoked and not nfserr_bad_stateid. The latter will not trigger a FREE_STATEID and the lack of it will leave this stid on the cl_revoked list indefinitely.	7.0	More Details
CVE-2024-47464	An authenticated Path Traversal vulnerability exists in Instant AOS-8 and AOS-10. Successful exploitation of this vulnerability allows an attacker to copy arbitrary files to a user readable location from the command line interface of the underlying operating system, which could lead to a remote unauthorized access to files.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-34891	Insufficiently protected credentials in DAV server settings in 1C-Bitrix Bitrix24 23.300.100 allows remote administrators to read Exchange account passwords via HTTP GET request.	6.8	More Details
CVE-2024-34885	Insufficiently protected credentials in SMTP server settings in 1C-Bitrix Bitrix24 23.300.100 allows remote administrators to read SMTP accounts passwords via HTTP GET request.	6.8	More Details
CVE-2024-20113	In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09036814; Issue ID: MSV-1715.	6.7	More Details
CVE-2024-33029	Memory corruption while handling the PDR in driver for getting the remote heap maps.	6.7	More Details
CVE-2024-33031	Memory corruption while processing the update SIM PB records request.	6.7	More Details
CVE-2024-10573	An out-of-bounds write flaw was found in mpg123 when handling crafted streams. When decoding PCM, the libmpg123 may write past the end of a heap-located buffer. Consequently, heap corruption may happen, and arbitrary code execution is not discarded. The complexity required to exploit this flaw is considered high as the payload must be validated by the MPEG decoder and the PCM synth before execution. Additionally, to successfully execute the attack, the user must scan through the stream, making web live stream content (such as web radios) a very unlikely attack vector.	6.7	More Details
CVE-2024-33032	Memory corruption when the user application modifies the same shared memory asynchronously when kernel is accessing it.	6.7	More Details
CVE-2024-20110	In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09065887; Issue ID: MSV-1762.	6.7	More Details
CVE-2024-33033	Memory corruption while processing IOCTL calls to unmap the buffers.	6.7	More Details
CVE-2024-23386	memory corruption when WiFi display APIs are invoked with large random inputs.	6.7	More Details
CVE-2024-23377	Memory corruption while invoking IOCTL command from user-space, when a user modifies the original packet size of the command after system properties have been already sent to the EVA driver.	6.7	More Details
CVE-2023-29122	Under certain conditions, access to service libraries is granted to account they should not have access to.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-33030	Memory corruption while parsing IPC frequency table parameters for LPLH that has size greater than expected size.	6.7	More Details
CVE-2024-20106	In m4u, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08960505; Issue ID: MSV-1590.	6.7	More Details
CVE-2024-20121	In KeyInstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08956986; Issue ID: MSV-1574.	6.7	More Details
CVE-2024-20108	In atci, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09082988; Issue ID: MSV-1774.	6.7	More Details
CVE-2024-20120	In KeyInstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08956986; Issue ID: MSV-1575.	6.7	More Details
CVE-2024-20119	In mms, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09062301; Issue ID: MSV-1620.	6.7	More Details
CVE-2024-20118	In mms, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09062392; Issue ID: MSV-1621.	6.7	More Details
CVE-2024-20109	In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09065928; Issue ID: MSV-1763.	6.7	More Details
CVE-2024-20115	In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09036695; Issue ID: MSV-1713.	6.7	More Details
CVE-2024-20114	In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09037038; Issue ID: MSV-1714.	6.7	More Details
CVE-2024-51530	LaunchAnywhere vulnerability in the account module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.6	More Details
CVE-2024-50333	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. User input is not validated and is written to the filesystem. The ParserLabel::addLabels() function can be used to write attacker-controlled data into the custom language file that will be included at the runtime. This issue has been addressed in versions 7.14.6 and 8.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.6	More Details
CVE-2024-37510	Missing Authorization vulnerability in Charitable Donations & Fundraising Team Charitable allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Charitable: from n/a through 1.8.1.7.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6479	The SIP Reviews Shortcode for WooCommerce plugin for WordPress is vulnerable to SQL Injection via the 'no_of_reviews' attribute in the woocommerce_reviews shortcode in all versions up to, and including, 1.2.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	6.5	More Details
CVE-2024-43209	Missing Authorization vulnerability in Bitly allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Bitly: from n/a through 2.7.2.	6.5	More Details
CVE-2024-9657	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tooltip' parameter in all versions up to, and including, 5.10.2 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.	6.5	More Details
CVE-2024-10750	A vulnerability has been found in Tenda i22 1.0.0.3(4687) and classified as problematic. Affected by this vulnerability is the function websReadEvent of the file /goform/GetIPTV?fgHPOST/goform/SysToo. The manipulation of the argument Content-Length leads to null pointer dereference. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.5	More Details
CVE-2024-51559	This vulnerability exists in the Wave 2.0 due to improper authorization checks on certain API endpoints. An authenticated remote attacker could exploit this vulnerability by manipulating API input parameters to gain unauthorized access and perform malicious activities on other user accounts.	6.5	More Details
CVE-2023-29115	In certain conditions a request directed to the Waybox Enel X Web management application could cause a denial-of-service (e.g. reboot).	6.5	More Details
CVE-2024-8934	A local user with administrative access rights can enter specialy crafted values for settings at the user interface (UI) of the TwinCAT Package Manager which then causes arbitrary OS commands to be executed.	6.5	More Details
CVE-2024-48289	An issue in the Bluetooth Low Energy implementation of Cypress Bluetooth SDK v3.66 allows attackers to cause a Denial of Service (DoS) via supplying a crafted LL_PAUSE_ENC_REQ packet.	6.5	More Details
CVE-2024-47308	Missing Authorization vulnerability in Templately allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Templately: from n/a through 3.1.2.	6.5	More Details
CVE-2024-51398	Altai Technologies Ltd Altai X500 Indoor 22 802.11ac Wave 2 AP web Management Weak password leakage in the background may lead to unauthorized access, data theft, and network attacks, seriously threatening network security.	6.5	More Details
CVE-2024-41744	IBM CICS TX Standard 11.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43998	Missing Authorization vulnerability in WebsiteinWP Blogpoet allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Blogpoet: from n/a through 1.0.3.	6.5	More Details
CVE-2024-43980	Missing Authorization vulnerability in CozyThemes Fota WP allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fota WP: from n/a through 1.4.1.	6.5	More Details
CVE-2024-43979	Missing Authorization vulnerability in CozyThemes Blockbooster allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Blockbooster: from n/a through 1.0.10.	6.5	More Details
CVE-2024-43974	Missing Authorization vulnerability in CozyThemes ReviveNews allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects ReviveNews: from n/a through 1.0.2.	6.5	More Details
CVE-2024-48272	D-Link DSL6740C v6.TR069.20211230 was discovered to use an insecure default Wifi password, possibly allowing attackers to connect to the device via a bruteforce attack.	6.5	More Details
CVE-2024-51242	A Server-Side Request Forgery (SSRF) vulnerability has been identified in eladmin 2.7 and earlier in ServerDeployController.java. The manipulation of the HTTP Body ip parameter leads to SSRF.	6.5	More Details
CVE-2024-51362	The LSC Smart Connect Indoor IP Camera V7.6.32 is vulnerable to an information disclosure issue where live camera footage can be accessed through the RTSP protocol on port 8554 without requiring authentication. This allows unauthorized users with network access to view the camera's feed, potentially compromising user privacy and security. No credentials or special permissions are required, and access can be gained remotely over the network.	6.5	More Details
CVE-2024-43956	Missing Authorization vulnerability in Caseproof, LLC Memberpress allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Memberpress: from n/a through 1.11.34.	6.5	More Details
CVE-2024-43932	Missing Authorization vulnerability in POSIMYTH The Plus Addons for Elementor Page Builder Lite allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Plus Addons for Elementor Page Builder Lite: from n/a through 5.6.2.	6.5	More Details
CVE-2024-43929	Missing Authorization vulnerability in eyecix JobSearch allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects JobSearch: from n/a through 2.5.4.	6.5	More Details
CVE-2024-43341	Missing Authorization vulnerability in CozyThemes Hello Agency allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Hello Agency: from n/a through 1.0.5.	6.5	More Details
CVE-2024-43310	Missing Authorization vulnerability in UkrSolution Print Barcode Labels for your WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Print Barcode Labels for your WooCommerce products/orders: from n/a through 3.4.9.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47361	Missing Authorization vulnerability in WPVibes Elementor Addon Elements allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Elementor Addon Elements: from n/a through 1.13.6.	6.5	More Details
CVE-2024-51680	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CrestaProject – Rizzo Andrea Cresta Addons for Elementor allows Stored XSS.This issue affects Cresta Addons for Elementor: from n/a through 1.0.9.	6.5	More Details
CVE-2024-51677	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WebberZone Knowledge Base allows Stored XSS.This issue affects Knowledge Base: from n/a through 2.2.0.	6.5	More Details
CVE-2024-47321	Missing Authorization vulnerability in Fahad Mahmood WP Datepicker allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WP Datepicker: from n/a through 2.1.1.	6.5	More Details
CVE-2024-38771	Missing Authorization vulnerability in Atarim allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Atarim: from n/a through 4.0.	6.5	More Details
CVE-2024-38777	Missing Authorization vulnerability in CreativeMotion Titan Anti-spam & Security allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Titan Anti-spam & Security: from n/a through 7.3.6.	6.5	More Details
CVE-2024-51683	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Michael Gangolf Custom post type templates for Elementor allows Stored XSS.This issue affects Custom post type templates for Elementor: from n/a through 1.10.1.	6.5	More Details
CVE-2024-37209	Access Control vulnerability in Prism IT Systems User Rights Access Manager allows . This issue affects User Rights Access Manager: from n/a through 1.1.2.	6.5	More Details
CVE-2024-37214	Missing Authorization vulnerability in Dropshipping Guru Ali2Woo Lite Exploiting Incorrectly Configured Access Control Security Levels, Stored XSS.This issue affects Ali2Woo Lite: from n/a through 3.3.5.	6.5	More Details
CVE-2024-48052	In gradio <=4.42.0, the gr.DownloadButton function has a hidden server-side request forgery (SSRF) vulnerability. The reason is that within the save_url_to_cache function, there are no restrictions on the URL, which allows access to local target resources. This can lead to the download of local resources and sensitive information.	6.5	More Details
CVE-2024-51682	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in HasThemes HT Builder – WordPress Theme Builder for Elementor allows Stored XSS.This issue affects HT Builder – WordPress Theme Builder for Elementor: from n/a through 1.3.0.	6.5	More Details
CVE-2024-51681	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CodeRevolution WP Pocket URLs allows Stored XSS.This issue affects WP Pocket URLs: from n/a through 1.0.3.	6.5	More Details
CVE-2024-39640	Missing Authorization vulnerability in QuadLayers WP Social Feed Gallery allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Social Feed Gallery: from n/a through 4.3.9.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51678	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Marcel Pol Elo Rating Shortcode allows Stored XSS.This issue affects Elo Rating Shortcode: from n/a through 1.0.3.	6.5	More Details
CVE-2024-48463	Bruno before 1.29.1 uses Electron shell.openExternal without validation (of http or https) for opening windows within the Markdown docs viewer.	6.5	More Details
CVE-2024-51556	This vulnerability exists in the Wave 2.0 due to insufficient encryption of sensitive data received at the API response. An authenticated remote attacker could exploit this vulnerability by manipulating API input parameters through API request URL/payload leading to unauthorized access to sensitive information belonging to other users.	6.5	More Details
CVE-2024-37477	Missing Authorization vulnerability in Automattic Newspack Content Converter allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Newspack Content Converter: from n/a through 0.1.5.	6.5	More Details
CVE-2024-37481	Missing Authorization vulnerability in Post Grid Team by RadiusTheme The Post Grid allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects The Post Grid: from n/a through 7.7.4.	6.5	More Details
CVE-2024-43122	Missing Authorization vulnerability in Creative Motion Robin image optimizer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Robin image optimizer: from n/a through 1.6.9.	6.5	More Details
CVE-2024-51557	This vulnerability exists in the Wave 2.0 due to missing rate limiting on OTP requests in an API endpoint. An authenticated remote attacker could exploit this vulnerability by sending multiple OTP request through vulnerable API endpoint which could lead to the OTP bombing/flooding on the targeted system.	6.5	More Details
CVE-2024-8627	The Ultimate TinyMCE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'field' shortcode in all versions up to, and including, 5.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9446	The WP Simple Anchors Links plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpanchor shortcode in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9165	The Gift Cards (Gift Vouchers and Packages) (WooCommerce Supported) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 4.4.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-9708	The Easy SVG Upload plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43937	Missing Authorization vulnerability in Themeum WP Crowdfunding allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Crowdfunding: from n/a through 2.1.10.	6.4	More Details
CVE-2024-9388	The Black Widgets For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.3.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-9110	A medium severity vulnerability has been identified within Privileged Identity which can allow an attacker to perform reflected cross-site scripting attacks.	6.4	More Details
CVE-2024-9884	The T(-) Countdown plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'tminus' shortcode in all versions up to, and including, 2.4.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9885	The Widget or Sidebar Shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'sidebar' shortcode in all versions up to, and including, 0.6.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9886	The WP Baidu Map plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'baidu_map' shortcode in all versions up to, and including, 1.2.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-10223	The WP Team – WordPress Team Member Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's htteamember shortcode in all versions up to, and including, 1.1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-43143	Missing Authorization vulnerability in Roundup WP Registrations for the Events Calendar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Registrations for the Events Calendar: from n/a through 2.12.1.	6.4	More Details
CVE-2024-10310	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Custom Gallery Widget 'image_title' parameter in all versions up to, and including, 5.10.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9443	The Basticom Framework plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.5.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-10232	The Group Chat & Video Chat by AtomChat plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's atomchat shortcode in all versions up to, and including, 1.1.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9655	The Gutenberg Blocks with AI by Kadence WP – Page Builder Features plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Icon widget in all versions up to, and including, 6.6.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-10340	The Shortcodes Blocks Creator Ultimate plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'scu' shortcode in versions up to, and including, 2.1.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-51430	Cross Site Scripting vulnerability in online diagnostic lab management system using php v.1.0 allows a remote attacker to execute arbitrary code via the Test Name parameter on the diagnostic/add-test.php component.	6.4	More Details
CVE-2024-10367	The Otter Blocks – Gutenberg Blocks, Page Builder for Gutenberg Editor & FSE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via REST API SVG File uploads in all versions up to, and including, 3.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-9178	The XT Floating Cart for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 2.8.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-6480	The SIP Reviews Shortcode for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'no_of_reviews' attribute in the woocommerce_reviews shortcode in all versions up to, and including, 1.2.3 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-2024-10742	A vulnerability was found in code-projects Wazifa System 1.0 and classified as critical. This issue affects some unknown processing of the file /controllers/control.php. The manipulation of the argument to leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10760	A vulnerability was found in code-projects University Event Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /dodelete.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10751	A vulnerability was found in Codezips ISP Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file pay.php. The manipulation of the argument customer 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-2024-10805	A vulnerability was found in code-projects University Event Management System 1.0. It has been classified as critical. This affects an unknown part of the file doedit.php. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions a confusing product name to be affected. Other parameters might be affected as well.	6.3	More Details
CVE-2024-10810	A vulnerability was found in code-projects E-Health Care System 1.0. It has been classified as critical. Affected is an unknown function of the file Doctor/app_request.php. The manipulation of the argument app_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-2024-10740	A vulnerability, which was classified as critical, was found in code-projects E-Health Care System up to 1.0. This affects an unknown part of the file /Admin/consulting_detail.php. The manipulation of the argument consulting_id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10809	A vulnerability was found in code-projects E-Health Care System 1.0 and classified as critical. This issue affects some unknown processing of the file /Doctor/chat.php. The manipulation of the argument name/message leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "name" to be affected. But it must be assumed that the parameter "message" is affected as well.	6.3	More Details
CVE-2024-10659	A vulnerability, which was classified as critical, has been found in ESAFENET CDG 5. Affected by this issue is the function delSystemEncryptPolicy of the file /com/esafenet/servlet/document/CDGAuthoriseTempletService.java. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10759	A vulnerability has been found in itsourcecode Farm Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /edit-pig.php. The manipulation of the argument pigno/weight/arrived/breed/remark/status leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "pigno" to be affected. But it must be assumed that other parameters are affected as well.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10660	A vulnerability, which was classified as critical, was found in ESAFENET CDG 5. This affects the function deleteHook of the file /com/esafenet/servlet/policy/HookService.java. The manipulation of the argument hookId 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-2024-10738	A vulnerability classified as critical was found in itsourcecode Farm Management System 1.0. Affected by this vulnerability is an unknown functionality of the file manage-breed.php. The manipulation of the argument breed 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-2024-47254	In 2N Access Commander versions 3.1.1.2 and prior, an Insufficient Verification of Data Authenticity vulnerability could allow an attacker to escalate their privileges and gain root access to the system.	6.3	More Details
CVE-2024-10501	A vulnerability, which was classified as critical, was found in ESAFENET CDG 5. This affects the function findById of the file /com/esafenet/servlet/document/ExamCDGDocService.java. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-10735	A vulnerability was found in Project Worlds Life Insurance Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /editNominee.php. The manipulation of the argument nominee_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10734	A vulnerability was found in Project Worlds Life Insurance Management System 1.0. It has been classified as critical. This affects an unknown part of the file /editPayment.php. The manipulation of the argument recipt_no 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-2024-10732	A vulnerability has been found in Tongda OA 2017 up to 11.10 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /module/word_model/view/index.php. The manipulation of the argument query_str 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-2024-10731	A vulnerability, which was classified as critical, was found in Tongda OA up to 11.10. Affected is an unknown function of the file /pda/appcenter/check_seal.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-2024-10730	A vulnerability, which was classified as critical, has been found in Tongda OA up to 11.6. This issue affects some unknown processing of the file /pda/appcenter/web_show.php. The manipulation of the argument ID leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10764	A vulnerability classified as critical has been found in Codezips Online Institute Management System 1.0. This affects an unknown part of the file /pages/save_user.php. The manipulation of the argument image leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10700	A vulnerability was found in code-projects University Event Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file submit.php. The manipulation of the argument name/email/title/Year/gender/fromdate/todate/people leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "name" to be affected. But it must be assumed that a variety of other parameters is affected too.	6.3	More Details
CVE-2024-10765	A vulnerability classified as critical was found in Codezips Online Institute Management System up to 1.0. This vulnerability affects unknown code of the file /profile.php. The manipulation of the argument old_image leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10766	A vulnerability, which was classified as critical, has been found in Codezips Free Exam Hall Seating Management System 1.0. This issue affects some unknown processing of the file /pages/save_user.php. The manipulation of the argument image leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher disclosure contains confusing vulnerability classes and file names.	6.3	More Details
CVE-2024-10697	A vulnerability has been found in Tenda AC6 15.03.05.19 and classified as critical. Affected by this vulnerability is the function formWriteFacMac of the file /goform/WriteFacMac of the component API Endpoint. The manipulation of the argument The leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10808	A vulnerability has been found in code-projects E-Health Care System 1.0 and classified as critical. This vulnerability affects unknown code of the file Admin/req_detail.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10500	A vulnerability, which was classified as critical, has been found in ESAFENET CDG 5. Affected by this issue is some unknown functionality of the file /com/esafenet/servlet/policy/HookWhiteListService.java. The manipulation of the argument policyId leads to sql injection. The attack may be launched remotely. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-10619	A vulnerability, which was classified as critical, was found in Tongda OA 2017 up to 11.10. Affected is an unknown function of the file /pda/reportshop/next_detail.php. The manipulation of the argument repid 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-2024-10655	A vulnerability was found in Tongda OA 2017 up to 11.9. It has been declared as critical. This vulnerability affects unknown code of the file /pda/reportshop/new.php. The manipulation of the argument repid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10657	A vulnerability classified as critical has been found in Tongda OA up to 11.10. Affected is an unknown function of the file /pda/approve_center/prcs_info.php. The manipulation of the argument RUN_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 Number	Description	Base Score	Reference
CVE-2024-10658	A vulnerability classified as critical was found in Tongda OA up to 11.10. Affected by this vulnerability is an unknown functionality of the file /pda/approve_center/check_seal.php. The manipulation of the argument ID leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10602	A vulnerability was found in Tongda OA 2017 up to 11.9 and classified as critical. Affected by this issue is some unknown functionality of the file /general/approve_center/list/input_form/data_picker_link.php. The manipulation of the argument dataSrc 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-2024-10601	A vulnerability has been found in Tongda OA 2017 up to 11.10 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /general/address/private/address/query/delete.php. The manipulation of the argument where_repeat 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-2024-10597	A vulnerability classified as critical has been found in ESAFENET CDG 5. This affects the function delPolicyAction of the file /com/esafenet/servlet/system/PolicyActionService.java. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-10596	A vulnerability was found in ESAFENET CDG 5. It has been rated as critical. Affected by this issue is the function delEntryptPolicySort of the file /com/esafenet/servlet/system/EncryptPolicyTypeService.java. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-10595	A vulnerability was found in ESAFENET CDG 5. It has been declared as critical. Affected by this vulnerability is the function delFile/delDifferCourseList of the file /com/esafenet/servlet/ajax/PublicDocInfoAjax.java. The manipulation leads to sql injection. 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.	6.3	More Details
CVE-2024-46531	phpgurukul Vehicle Record Management System v1.0 was discovered to contain a SQL injection vulnerability via the searchinputdata parameter at /index.php.	6.3	More Details
CVE-2024-10546	A vulnerability classified as critical was found in open-scratch Teaching 在线教学平台 up to 2.7. This vulnerability affects unknown code of the file /api/sys/ng-alain/getDictItemsByTable/ of the component URL Handler. The manipulation leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-43285	Missing Authorization vulnerability in Presto Made, Inc Presto Player allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Presto Player: from n/a through 3.0.2.	6.3	More Details
CVE-2024-37516	Missing Authorization vulnerability in fifu.App Featured Image from URL allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Featured Image from URL: from n/a through 4.8.2.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8553	A vulnerability was found in Foreman's loader macros introduced with report templates. These macros may allow an authenticated user with permissions to view and create templates to read any field from Foreman's database. By using specific strings in the loader macros, users can bypass permissions and access sensitive information.	6.3	More Details
CVE-2024-37929	Missing Authorization vulnerability in solwin User Activity Log Pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects User Activity Log Pro: from n/a through 2.3.4.	6.3	More Details
CVE-2024-38707	Missing Authorization vulnerability in WPDeveloper EmbedPress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects EmbedPress: from n/a through 4.0.4.	6.3	More Details
CVE-2024-43146	Missing Authorization vulnerability in Ahmed Kaludi, Mohammed Kaludi AMP for WP allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects AMP for WP: from n/a through 1.0.96.1.	6.3	More Details
CVE-2024-10656	A vulnerability was found in Tongda OA 2017 up to 11.9. It has been rated as critical. This issue affects some unknown processing of the file /pda/meeting/apply.php. The manipulation of the argument mr_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10594	A vulnerability was found in ESAFENET CDG 5. It has been classified as critical. Affected is the function docHistory of the file /com/esafenet/servlet/fileManagement/FileDirectoryService.java. The manipulation of the argument fileId leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-10610	A vulnerability has been found in ESAFENET CDG 5 and classified as critical. This vulnerability affects the function delProtocol of the file /com/esafenet/servlet/system/ProtocolService.java. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-10617	A vulnerability classified as critical was found in Tongda OA up to 11.10. This vulnerability affects unknown code of the file /pda/workflow/check_seal.php. The manipulation of the argument ID leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10505	A vulnerability was found in wuzhicms 4.1.0. It has been classified as critical. Affected is the function add/edit of the file www/coreframe/app/content/admin/block.php. The manipulation leads to code injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. Initially two separate issues were created by the researcher for the different function calls. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-10615	A vulnerability was found in Tongda OA 2017 up to 11.10. It has been rated as critical. Affected by this issue is some unknown functionality of the file /general/approve_center/query/list/input_form/delete_data_attach.php. The manipulation of the argument RUN_ID leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10616	A vulnerability classified as critical has been found in Tongda OA up to 11.9. This affects an unknown part of the file /pda/workflow/webSignSubmit.php. The manipulation of the argument saleId 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-2024-10502	A vulnerability has been found in ESAFENET CDG 5 and classified as critical. This vulnerability affects the function getOneFileDirectory of the file /com/esafenet/servlet/fileManagement/FileDirectoryService.java. The manipulation of the argument directoryId leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-10612	A vulnerability was found in ESAFENET CDG 5. It has been classified as critical. Affected is the function removeHookInvalidCourse of the file /com/esafenet/servlet/system/HookInvalidCourseService.java. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-10506	A vulnerability classified as critical has been found in code-projects Blood Bank System 1.0. This affects an unknown part of the file /admin/blood/update/B-.php. The manipulation of the argument Bloodname 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-2024-10611	A vulnerability was found in ESAFENET CDG 5 and classified as critical. This issue affects the function delProtocol of the file /com/esafenet/servlet/system/PrintScreenListService.java. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-10609	A vulnerability, which was classified as critical, was found in itsourcecode Tailoring Management System Project 1.0. This affects an unknown part of the file typeadd.php. The manipulation of the argument sex 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-2024-10618	A vulnerability, which was classified as critical, has been found in Tongda OA 2017 up to 11.10. This issue affects some unknown processing of the file /pda/reportshop/record_detail.php. The manipulation of the argument repid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-10613	A vulnerability was found in ESAFENET CDG 5. It has been declared as critical. Affected by this vulnerability is the function delSystemEncryptPolicy of the file /com/esafenet/servlet/system/SystemEncryptPolicyService.java. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-51515	Race condition vulnerability in the kernel network module Impact:Successful exploitation of this vulnerability may affect availability.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51516	Permission control vulnerability in the ability module Impact: Successful exploitation of this vulnerability may cause features to function abnormally.	6.2	More Details
CVE-2024-51522	Vulnerability of improper device information processing in the device management module Impact: Successful exploitation of this vulnerability may affect availability.	6.2	More Details
CVE-2024-20107	In da, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09124360; Issue ID: MSV-1823.	6.2	More Details
CVE-2024-51407	Floodlight SDN OpenFlow Controller v.1.2 has an issue that allows local hosts to construct false broadcast ports causing inter-host communication anomalies.	6.2	More Details
CVE-2024-51406	Floodlight SDN Open Flow Controller v.1.2 has an issue that allows local hosts to build fake LLDP packets that allow specific clusters to be missed by Floodlight, which in turn leads to missed hosts inside and outside the cluster.	6.2	More Details
CVE-2024-51512	Vulnerability of parameter type not being verified in the WantAgent module Impact: Successful exploitation of this vulnerability may affect availability.	6.2	More Details
CVE-2024-51511	Vulnerability of parameter type not being verified in the WantAgent module Impact: Successful exploitation of this vulnerability may affect availability.	6.2	More Details
CVE-2024-51525	Permission control vulnerability in the clipboard module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	6.2	More Details
CVE-2024-8792	The Subscribe to Comments plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.3. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2023-52045	Studio-42 eLfinder 2.1.62 contains a filename restriction bypass leading to a persistent Cross-site Scripting (XSS) vulnerability.	6.1	More Details
CVE-2024-48057	localai <=2.20.1 is vulnerable to Cross Site Scripting (XSS). When calling the delete model API and passing inappropriate parameters, it can cause a one-time storage XSS, which will trigger the payload when a user accesses the homepage.	6.1	More Details
CVE-2024-8871	The Pricing Tables WordPress Plugin – Easy Pricing Tables plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.2.5. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-10454	Clickjacking vulnerability in Clibo Manager v1.1.9.12 in the '/public/login' directory, a login panel. This vulnerability occurs due to the absence of an X-Frame-Options server-side header. An attacker could overlay a transparent iframe to perform click hijacking on victims.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51419	Cross Site Scripting vulnerability in Shenzhen Interconnection Harbor Network Technology Co., Ltd Ofweek Online Exhibition v.1.0.0 allows a remote attacker to execute arbitrary code.	6.1	More Details
CVE-2024-9434	The WPGlobus Translate Options plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.2.0. This is due to missing or incorrect nonce validation on the on__translate_options_page() function. This makes it possible for unauthenticated attackers to inject malicious web scripts and update plugin settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9896	The BBP Core – Expand bbPress powered forums with useful features 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, 1.2.5. 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-2024-48648	A Reflected Cross-Site Scripting (XSS) vulnerability exists in the Sage 1000 v 7.0.0. This vulnerability allows attackers to inject malicious scripts into URLs, which are reflected back by the server in the response without proper sanitization or encoding.	6.1	More Details
CVE-2024-48346	xtreme1 <= v0.9.1 contains a Server-Side Request Forgery (SSRF) vulnerability in the /api/data/upload path. The vulnerability is triggered through the fileUrl parameter, which allows an attacker to make arbitrary requests to internal or external systems.	6.1	More Details
CVE-2024-8739	The ReCaptcha Integration for WordPress 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, 1.2.5. 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-2024-9667	The Seriously Simple Podcasting plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.5.0. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-51328	Cross Site Scripting vulnerability in addcategory.php in projectworld's Travel Management System v1.0 allows remote attacker to inject arbitrary code via the t2 parameter.	6.1	More Details
CVE-2024-30618	A Stored Cross-Site Scripting (XSS) Vulnerability in Chamilo LMS 1.11.26 allows a remote attacker to execute arbitrary JavaScript in a web browser by including a malicious payload in the 'content' parameter of 'group_topics.php'.	6.1	More Details
CVE-2024-10086	A vulnerability was identified in Consul and Consul Enterprise such that the server response did not explicitly set a Content-Type HTTP header, allowing user-provided inputs to be misinterpreted and lead to reflected XSS.	6.1	More Details
CVE-2024-48059	gaizhenbiao/chuanhuchatgpt project, version <=20240802 is vulnerable to stored Cross-Site Scripting (XSS) in WebSocket session transmission. An attacker can inject malicious content into a WebSocket message. When a victim accesses this session, the malicious JavaScript is executed in the victim's browser.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48410	Cross Site Scripting vulnerability in Camtrace v.9.16.2.1 allows a remote attacker to execute arbitrary code via the login.php.	6.1	More Details
CVE-2024-41745	IBM CICS TX Standard is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	6.1	More Details
CVE-2024-10652	IDExpert from CHANGING Information Technology does not properly validate a parameter for a specific functionality, allowing unauthenticated remote attackers to inject JavsScript code and perform Reflected Cross-site scripting attacks.	6.1	More Details
CVE-2024-9147	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Bna Informatics PosPratik allows XSS Through HTTP Query Strings.This issue affects PosPratik: before v3.2.1.	6.1	More Details
CVE-2024-50802	A SQL Injection vulnerability was discovered in AbanteCart 1.4.0 in the update() function in public_html/admin/controller/responses/listing_grid/email_templates.php. The vulnerability is exploitable via the id parameter.	6.0	More Details
CVE-2024-50801	A SQL Injection vulnerability was discovered in AbanteCart 1.4.0 in the update() function in public_html/admin/controller/responses/listing_grid/collections.php. The vulnerability is exploitable via the id parameter.	6.0	More Details
CVE-2024-43211	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PluginOps MailChimp Subscribe Forms allows Stored XSS.This issue affects MailChimp Subscribe Forms : from n/a through 4.0.9.9.	5.9	More Details
CVE-2024-41738	IBM TXSeries for Multiplatforms 10.1 could allow an attacker to obtain sensitive information from the query string of an HTTP GET method to process a request which could be obtained using man in the middle techniques.	5.9	More Details
CVE-2024-32946	A vulnerability in the LevelOne WBR-6012 router's firmware version R0.40e6 allows sensitive information to be transmitted in cleartext via Web and FTP services, exposing it to network sniffing attacks.	5.9	More Details
CVE-2024-43382	Snowflake JDBC driver versions >= 3.2.6 and <= 3.19.1 have an Incorrect Security Setting that can result in data being uploaded to an encrypted stage without the additional layer of protection provided by client side encryption.	5.9	More Details
CVE-2024-51685	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Michael Gangolf Accordion title for Elementor allows Stored XSS.This issue affects Accordion title for Elementor: from n/a through 1.2.1.	5.9	More Details
CVE-2024-32870	Combodo iTop is a simple, web based IT Service Management tool. Server, OS, DBMS, PHP, and iTop info (name, version and parameters) can be read by anyone having access to iTop URI. This issue has been patched in versions 2.7.11, 3.0.5, 3.1.2, and 3.2.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.8	More Details
CVE-2024-43274	Missing Authorization vulnerability in JS Help Desk JS Help Desk – Best Help Desk & Support Plugin allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects JS Help Desk – Best Help Desk & Support Plugin: from n/a through 2.8.6.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50998	Netgear R8500 v1.0.2.160 was discovered to contain multiple stack overflow vulnerabilities in the component openvpn.cgi via the openvpn_service_port and openvpn_service_port_tun parameters. These vulnerabilities allow attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51016	Netgear XR300 v1.0.3.78 was discovered to contain a stack overflow via the addName%d parameter in usb_approve.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51013	Netgear R7000P v1.3.3.154 was discovered to contain a stack overflow via the RADIUSAddr%d_wla parameter at wireless.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51014	Netgear XR300 v1.0.3.78 was discovered to contain a stack overflow via the ssid_an parameter in bridge_wireless_main.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51015	Netgear R7000P v1.3.3.154 was discovered to contain a command injection vulnerability via the device_name2 parameter at operation_mode.cgi. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	5.7	More Details
CVE-2024-51017	Netgear R7000P v1.3.3.154 was discovered to contain a stack overflow via the l2tp_user_netmask parameter at l2tp.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51018	Netgear R7000P v1.3.3.154 was discovered to contain a stack overflow via the pptp_user_netmask parameter at pptp.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51019	Netgear R7000P v1.3.3.154 was discovered to contain a stack overflow via the pppoe_localnetmask parameter at pppoe.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51020	Netgear R7000P v1.3.3.154 was discovered to contain a stack overflow via the apn parameter at usbISP_detail_edit.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51022	Netgear XR300 v1.0.3.78 was discovered to contain a stack overflow via the ssid parameter in bridge_wireless_main.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-52013	Netgear R8500 v1.0.2.160, XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 were discovered to contain a stack overflow via the pptp_user_ip parameter at wiz_pptp.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-52014	Netgear R8500 v1.0.2.160, XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 were discovered to contain a stack overflow via the pptp_user_ip parameter at genie_pptp.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-52016	Netgear R8500 v1.0.2.160, XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 were discovered to multiple stack overflow vulnerabilities in the component wlg_adv.cgi via the apmode_dns1_pri and apmode_dns1_sec parameters. These vulnerabilities allow attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51521	Input parameter verification vulnerability in the background service module Impact: Successful exploitation of this vulnerability may affect availability.	5.7	More Details
CVE-2024-51011	Netgear XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 was discovered to contain a stack overflow via the pppoe_localip parameter at pppoe.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51012	Netgear R8500 v1.0.2.160 was discovered to contain a stack overflow via the ipv6_pri_dns parameter at ipv6_fix.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-50999	Netgear R8500 v1.0.2.160 was discovered to contain a command injection vulnerability in the sysNewPasswd parameter at password.cgi. This vulnerability allows attackers to execute arbitrary OS commands via a crafted request.	5.7	More Details
CVE-2024-52017	Netgear XR300 v1.0.3.78 was discovered to contain a stack overflow via the passphrase parameter at bridge_wireless_main.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51007	Netgear XR300 v1.0.3.78 was discovered to contain a stack overflow via the passphrase parameter at wireless.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2023-29114	System logs could be accessed through web management application due to a lack of access control. An attacker can obtain the following sensitive information: • Wi-Fi access point credentials to which the EV charger can connect. • APN web address and credentials. • IPSEC credentials. • Web interface access credentials for user and admin accounts. • JuiceBox system components (software installed, model, firmware version, etc.). • C2G configuration details. • Internal IP addresses. • OTA firmware update configurations (DNS servers). All the credentials are stored in logs in an unencrypted plaintext format.	5.7	More Details
CVE-2024-50995	Netgear R8500 v1.0.2.160 was discovered to contain a stack overflow via the share_name parameter at usb_remote_smb_conf.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51006	Netgear R8500 v1.0.2.160 was discovered to contain a stack overflow via the ipv6_static_ip parameter in the ipv6_tunnel function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51004	Netgear R8500 v1.0.2.160 and R7000P v1.3.3.154 were discovered to multiple stack overflow vulnerabilities in the component usb_device.cgi via the cifs_user, read_access, and write_access parameters. These vulnerabilities allow attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-50996	Netgear R8500 v1.0.2.160, XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 were discovered to contain a stack overflow via the bpa_server parameter at genie_bpa.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51003	Netgear R8500 v1.0.2.160, XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 were discovered to multiple stack overflow vulnerabilities in the component ap_mode.cgi via the apmode_dns1_pri and apmode_dns1_sec parameters. These vulnerabilities allow attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51002	Netgear R8500 v1.0.2.160, XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 were discovered to contain a stack overflow via the l2tp_user_ip parameter at l2tp.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51001	Netgear R8500 v1.0.2.160 was discovered to contain a stack overflow via the sysDNSHost parameter at ddns.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-50997	Netgear R8500 v1.0.2.160, XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 were discovered to contain a stack overflow via the pptp_user_ip parameter at pptp.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51000	Netgear R8500 v1.0.2.160 was discovered to contain multiple stack overflow vulnerabilities in the component wireless.cgi via the opmode, opmode_an, and opmode_an_2 parameters. These vulnerabilities allow attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-50994	Netgear R8500 v1.0.2.160 was discovered to contain multiple stack overflow vulnerabilities in the component ipv6_fix.cgi via the ipv6_wan_ipaddr, ipv6_lan_ipaddr, ipv6_wan_length, and ipv6_lan_length parameters. These vulnerabilities allow attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-52015	Netgear R8500 v1.0.2.160, XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 were discovered to contain a stack overflow via the pptp_user_ip parameter at bsw_pptp.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-52028	Netgear R7000P v1.3.3.154 was discovered to contain a stack overflow via the pptp_user_netmask parameter at wiz_pptp.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-51399	Altai Technologies Ltd Altai IX500 Indoor 22 802.11ac Wave 2 AP After login, there are file reads in the background, and attackers can obtain sensitive information such as user credentials, system configuration, and database connection strings, which can lead to data breaches and identity theft.	5.7	More Details
CVE-2024-52023	Netgear XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 was discovered to contain a stack overflow via the pppoe_localip parameter at pppoe2.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-52024	Netgear XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 was discovered to contain a stack overflow via the pppoe_localip parameter at wizpppoe.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-52025	Netgear XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 was discovered to contain a stack overflow via the pppoe_localip parameter at geniepppoe.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-52026	Netgear XR300 v1.0.3.78, R7000P v1.3.3.154, and R6400 v2 1.0.4.128 was discovered to contain a stack overflow via the pppoe_localip parameter at bsw_pppoe.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-52030	Netgear R7000P v1.3.3.154 was discovered to contain a stack overflow via the pptp_user_netmask parameter at ru_wan_flow.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-52029	Netgear R7000P v1.3.3.154 was discovered to contain a stack overflow via the pptp_user_netmask parameter at genie_pptp.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted POST request.	5.7	More Details
CVE-2024-50117	In the Linux kernel, the following vulnerability has been resolved: drm/amd: Guard against bad data for ATIF ACPI method If a BIOS provides bad data in response to an ATIF method call this causes a NULL pointer dereference in the caller. ``` ? show_regs (arch/x86/kernel/dumpstack.c:478 (discriminator 1)) ? __die (arch/x86/kernel/dumpstack.c:423 arch/x86/kernel/dumpstack.c:434) ? page_fault_oops (arch/x86/mm/fault.c:544 (discriminator 2) arch/x86/mm/fault.c:705 (discriminator 2)) ? do_user_addr_fault (arch/x86/mm/fault.c:440 (discriminator 1) arch/x86/mm/fault.c:1232 (discriminator 1)) ? acpi_ut_update_object_reference (drivers/acpi/acpica/utdelete.c:642) ? exc_page_fault (arch/x86/mm/fault.c:1542) ? asm_exc_page_fault (./arch/x86/include/asm/idtentry.h:623) ? amdgpu_atif_query_backlight_caps.constprop.0 (drivers/gpu/drm/amd/amdgpu/amdgpu_acpi.c:387 (discriminator 2)) amdgpu ? amdgpu_atif_query_backlight_caps.constprop.0 (drivers/gpu/drm/amd/amdgpu/amdgpu_acpi.c:386 (discriminator 1)) amdgpu ``` It has been encountered on at least one system, so guard for it. (cherry picked from commit c9b7c809b89f24e9372a4e7f02d64c950b07fdee)	5.5	More Details
CVE-2024-50122	In the Linux kernel, the following vulnerability has been resolved: PCI: Hold rescan lock while adding devices during host probe Since adding the PCI power control code, we may end up with a race between the pwrctl platform device rescanning the bus and host controller probe functions. The latter need to take the rescan lock when adding devices or we may end up in an undefined state having two incompletely added devices and hit the following crash when trying to remove the device over sysfs: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Internal error: Oops: 0000000096000004 [#1] SMP Call trace: __pi_strlen+0x14/0x150 kernfs_find_ns+0x80/0x13c kernfs_remove_by_name_ns+0x54/0xf0 sysfs_remove_bin_file+0x24/0x34 pci_remove_resource_files+0x3c/0x84 pci_remove_sysfs_dev_files+0x28/0x38 pci_stop_bus_device+0x8c/0xd8 pci_stop_bus_device+0x40/0xd8 pci_stop_and_remove_bus_device_locked+0x28/0x48 remove_store+0x70/0xb0 dev_attr_store+0x20/0x38 sysfs_kf_write+0x58/0x78 kernfs_fop_write_iter+0xe8/0x184 vfs_write+0x2dc/0x308 ksys_write+0x7c/0xec	5.5	More Details
CVE-2024-50120	In the Linux kernel, the following vulnerability has been resolved: smb: client: Handle kstrdup failures for passwords In smb3_reconfigure(), after duplicating ctx->password and ctx->password2 with kstrdup(), we need to check for allocation failures. If ses->password allocation fails, return -ENOMEM. If ses->password2 allocation fails, free ses->password, set it to NULL, and return -ENOMEM.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50119	In the Linux kernel, the following vulnerability has been resolved: cifs: fix warning when destroy 'cifs_io_request_pool' There's a issue as follows: WARNING: CPU: 1 PID: 27826 at mm/slub.c:4698 free_large_kmalloc+0xac/0xe0 RIP: 0010:free_large_kmalloc+0xac/0xe0 Call Trace: <TASK> ? __warn+0xea/0x330 mempool_destroy+0x13f/0x1d0 init_cifs+0xa50/0xff0 [cifs] do_one_initcall+0xdc/0x550 do_init_module+0x22d/0x6b0 load_module+0x4e96/0x5ff0 init_module_from_file+0xcd/0x130 idempotent_init_module+0x330/0x620 __x64_sys_finit_module+0xb3/0x110 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Obviously, 'cifs_io_request_pool' is not created by mempool_create(). So just use mempool_exit() to revert 'cifs_io_request_pool'.	5.5	More Details
CVE-2024-50118	In the Linux kernel, the following vulnerability has been resolved: btrfs: reject ro->rw reconfiguration if there are hard ro requirements [BUG] Syzbot reports the following crash: BTRFS info (device loop0 state MCS): disabling free space tree BTRFS info (device loop0 state MCS): clearing compat-ro feature flag for FREE_SPACE_TREE (0x1) BTRFS info (device loop0 state MCS): clearing compat-ro feature flag for FREE_SPACE_TREE_VALID (0x2) Oops: general protection fault, probably for non-canonical address 0xdffffc0000000003: 0000 [#1] PREEMPT SMP KASAN NOPTI KASAN: null-ptr-deref in range [0x0000000000000018-0x000000000000001f] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2~bpo12+1 04/01/2014 RIP: 0010:backup_super_roots fs/btrfs/disk-io.c:1691 [inline] RIP: 0010:write_all_supers+0x97a/0x40f0 fs/btrfs/disk-io.c:4041 Call Trace: <TASK> btrfs_commit_transaction+0x1eae/0x3740 fs/btrfs/transaction.c:2530 btrfs_delete_free_space_tree+0x383/0x730 fs/btrfs/free-space-tree.c:1312 btrfs_start_pre_rw_mount+0xf28/0x1300 fs/btrfs/disk-io.c:3012 btrfs_remount_rw fs/btrfs/super.c:1309 [inline] btrfs_reconfigure+0xae6/0x2d40 fs/btrfs/super.c:1534 btrfs_reconfigure_for_mount fs/btrfs/super.c:2020 [inline] btrfs_get_tree_subvol fs/btrfs/super.c:2079 [inline] btrfs_get_tree+0x918/0x1920 fs/btrfs/super.c:2115 vfs_get_tree+0x90/0x2b0 fs/super.c:1800 do_new_mount+0x2be/0xb40 fs/namespace.c:3472 do_mount fs/namespace.c:3812 [inline] __do_sys_mount fs/namespace.c:4020 [inline] __se_sys_mount+0x2d6/0x3c0 fs/namespace.c:3997 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f [CAUSE] To support mounting different subvolume with different RO/RW flags for the new mount APIs, btrfs introduced two workaround to support this feature: - Skip mount option/feature checks if we are mounting a different subvolume - Reconfigure the fs to RW if the initial mount is RO Combining these two, we can have the following sequence: - Mount the fs ro,rescue=all,clear_cache,space_cache=v1 rescue=all will mark the fs as hard read-only, so no v2 cache clearing will happen. - Mount a subvolume rw of the same fs. We go into btrfs_get_tree_subvol(), but fc_mount() returns EBUSY because our new fc is RW, different from the original fs. Now we enter btrfs_reconfigure_for_mount(), which switches the RO flag first so that we can grab the existing fs_info. Then we reconfigure the fs to RW. - During reconfiguration, option/features check is skipped This means we will restart the v2 cache clearing, and convert back to v1 cache. This will trigger fs writes, and since the original fs has "rescue=all" option, it skips the csum tree read. And eventually causing NULL pointer dereference in super block writeback. [FIX] For reconfiguration caused by different subvolume RO/RW flags, ensure we always run btrfs_check_options() to ensure we have proper hard RO requirements met. In fact the function btrfs_check_options() doesn't really do many complex checks, but hard RO requirement and some feature dependency checks, thus there is no special reason not to do the check for mount reconfiguration.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51529	Data verification vulnerability in the battery module Impact: Successful exploitation of this vulnerability may affect function stability.	5.5	More Details
CVE-2024-50116	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix kernel bug due to missing clearing of buffer delay flag Syzbot reported that after nilfs2 reads a corrupted file system image and degrades to read-only, the BUG_ON check for the buffer delay flag in submit_bh_wbc() may fail, causing a kernel bug. This is because the buffer delay flag is not cleared when clearing the buffer state flags to discard a page/folio or a buffer head. So, fix this. This became necessary when the use of nilfs2's own page clear routine was expanded. This state inconsistency does not occur if the buffer is written normally by log writing.	5.5	More Details
CVE-2024-50113	In the Linux kernel, the following vulnerability has been resolved: firewire: core: fix invalid port index for parent device In a commit 24b7f8e5cd65 ("firewire: core: use helper functions for self ID sequence"), the enumeration over self ID sequence was refactored with some helper functions with KUnit tests. These helper functions are guaranteed to work expectedly by the KUnit tests, however their application includes a mistake to assign invalid value to the index of port connected to parent device. This bug affects the case that any extra node devices which has three or more ports are connected to 1394 OHCI controller. In the case, the path to update the tree cache could hits WARN_ON(), and gets general protection fault due to the access to invalid address computed by the invalid value. This commit fixes the bug to assign correct port index.	5.5	More Details
CVE-2023-52920	In the Linux kernel, the following vulnerability has been resolved: bpf: support non-r10 register spill/fill to/from stack in precision tracking Use instruction (jump) history to record instructions that performed register spill/fill to/from stack, regardless if this was done through read-only r10 register, or any other register after copying r10 into it *and* potentially adjusting offset. To make this work reliably, we push extra per-instruction flags into instruction history, encoding stack slot index (spi) and stack frame number in extra 10 bit flags we take away from prev_idx in instruction history. We don't touch idx field for maximum performance, as it's checked most frequently during backtracking. This change removes basically the last remaining practical limitation of precision backtracking logic in BPF verifier. It fixes known deficiencies, but also opens up new opportunities to reduce number of verified states, explored in the subsequent patches. There are only three differences in selftests' BPF object files according to veristat, all in the positive direction (less states). File Program Insns (A) Insns (B) Insns (DIFF) States (A) States (B) States (DIFF) ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- test_cls_redirect_dynptr.bpf.linked3.o cls_redirect 2987 2864 -123 (-4.12%) 240 231 -9 (-3.75%) xdp_synproxy_kern.bpf.linked3.o syncookie_tc 82848 82661 -187 (-0.23%) 5107 5073 -34 (-0.67%) xdp_synproxy_kern.bpf.linked3.o syncookie_xdp 85116 84964 -152 (-0.18%) 5162 5130 -32 (-0.62%) Note, I avoided renaming jmp_history to more generic insn_hist to minimize number of lines changed and potential merge conflicts between bpf and bpf-next trees. Notice also cur_hist_entry pointer reset to NULL at the beginning of instruction verification loop. This pointer avoids the problem of relying on last jump history entry's insn_idx to determine whether we already have entry for current instruction or not. It can happen that we added jump history entry because current instruction is_jmp_point(), but also we need to add instruction flags for stack access. In this case, we don't want to entries, so we need to reuse last added entry, if it is present. Relying on insn_idx comparison has the same ambiguity problem as the one that was fixed recently in [0], so we avoid that. [0] https://patchwork.kernel.org/project/netdevbpf/patch/20231110002638.4168352-3-andrii@kernel.org/	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50111	In the Linux kernel, the following vulnerability has been resolved: LoongArch: Enable IRQ if do_ale() triggered in irq-enabled context Unaligned access exception can be triggered in irq-enabled context such as user mode, in this case do_ale() may call get_user() which may cause sleep. Then we will get: BUG: sleeping function called from invalid context at arch/loongarch/kernel/access-helper.h:7 in_atomic(): 0, irqs_disabled(): 1, non_block: 0, pid: 129, name: modprobe preempt_count: 0, expected: 0 RCU nest depth: 0, expected: 0 CPU: 0 UID: 0 PID: 129 Comm: modprobe Tainted: G W 6.12.0-rc1+ #1723 Tainted: [W]=WARN Stack : 9000000105e0bd48 0000000000000000 9000000003803944 9000000105e08000 9000000105e0bc70 9000000105e0bc78 0000000000000000 0000000000000000 9000000105e0bc78 0000000000000001 9000000185e0ba07 9000000105e0b890 ffffffffffffffff 9000000105e0bc78 73924b81763be05b 9000000100194500 000000000000020c 000000000000000a 0000000000000000 0000000000000003 00000000000023f0 00000000000e1401 00000000072f8000 0000007ffbb0e260 0000000000000000 0000000000000000 9000000005437650 90000000055d5000 0000000000000000 0000000000000003 0000007ffbb0e1f0 0000000000000000 0000005567b00490 0000000000000000 9000000003803964 0000007ffbb0dfec 00000000000000b0 0000000000000007 0000000000000003 0000000000071c1d ... Call Trace: [<9000000003803964>] show_stack+0x64/0x1a0 [<9000000004c57464>] dump_stack_lvl+0x74/0xb0 [<9000000003861ab4>] __might_resched+0x154/0x1a0 [<900000000380c96c>] emulate_load_store_insn+0x6c/0xf60 [<9000000004c58118>] do_ale+0x78/0x180 [<9000000003801bc8>] handle_ale+0x128/0x1e0 So enable IRQ if unaligned access exception is triggered in irq-enabled context to fix it.	5.5	More Details
CVE-2024-10841	A vulnerability classified as critical was found in romadebrian WEB-Sekolah 1.0. Affected by this vulnerability is an unknown functionality of the file /Proses_Kirim.php of the component Mail Handler. The manipulation of the argument Name leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50110	In the Linux kernel, the following vulnerability has been resolved: xfrm: fix one more kernel-infoleak in algo dumping During fuzz testing, the following issue was discovered: BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x598/0x2a30 _copy_to_iter+0x598/0x2a30 __skb_datagram_iter+0x168/0x1060 skb_copy_datagram_iter+0x5b/0x220 netlink_recvmsg+0x362/0x1700 sock_recvmsg+0x2dc/0x390 __sys_recvfrom+0x381/0x6d0 __x64_sys_recvfrom+0x130/0x200 x64_sys_call+0x32c8/0x3cc0 do_syscall_64+0xd8/0x1c0 entry_SYSCALL_64_after_hwframe+0x79/0x81 Uninit was stored to memory at: copy_to_user_state_extra+0xcc1/0x1e00 dump_one_state+0x28c/0x5f0 xfrm_state_walk+0x548/0x11e0 xfrm_dump_sa+0x1e0/0x840 netlink_dump+0x943/0x1c40 __netlink_dump_start+0x746/0xdb0 xfrm_user_rcv_msg+0x429/0xc00 netlink_rcv_skb+0x613/0x780 xfrm_netlink_rcv+0x77/0xc0 netlink_unicast+0xe90/0x1280 netlink_sendmsg+0x126d/0x1490 __sock_sendmsg+0x332/0x3d0 ____sys_sendmsg+0x863/0xc30 ___sys_sendmsg+0x285/0x3e0 __x64_sys_sendmsg+0x2d6/0x560 x64_sys_call+0x1316/0x3cc0 do_syscall_64+0xd8/0x1c0 entry_SYSCALL_64_after_hwframe+0x79/0x81 Uninit was created at: __kmalloc+0x571/0xd30 attach_auth+0x106/0x3e0 xfrm_add_sa+0x2aa0/0x4230 xfrm_user_rcv_msg+0x832/0xc00 netlink_rcv_skb+0x613/0x780 xfrm_netlink_rcv+0x77/0xc0 netlink_unicast+0xe90/0x1280 netlink_sendmsg+0x126d/0x1490 __sock_sendmsg+0x332/0x3d0 ____sys_sendmsg+0x863/0xc30 ___sys_sendmsg+0x285/0x3e0 __x64_sys_sendmsg+0x2d6/0x560 x64_sys_call+0x1316/0x3cc0 do_syscall_64+0xd8/0x1c0 entry_SYSCALL_64_after_hwframe+0x79/0x81 Bytes 328-379 of 732 are uninitialized Memory access of size 732 starts at ffff88800e18e000 Data copied to user address 00007ff30f48aff0 CPU: 2 PID: 18167 Comm: syz-executor.0 Not tainted 6.8.11 #1 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 Fixes copying of xfrm algorithms where some random data of the structure fields can end up in userspace. Padding in structures may be filled with random (possibly sensitve) data and should never be given directly to user-space. A similar issue was resolved in the commit 8222d5910dae ("xfrm: Zero padding when dumping algos and encap") Found by Linux Verification Center (linuxtesting.org) with Syzkaller.	5.5	More Details
CVE-2024-50109	In the Linux kernel, the following vulnerability has been resolved: md/raid10: fix null ptr dereference in raid10_size() In raid10_run() if raid10_set_queue_limits() succeed, the return value is set to zero, and if following procedures failed raid10_run() will return zero while mddev->private is still NULL, causing null ptr dereference in raid10_size(). Fix the problem by only overwrite the return value if raid10_set_queue_limits() failed.	5.5	More Details
CVE-2024-51520	Vulnerability of input parameters not being verified in the HDC module Impact: Successful exploitation of this vulnerability may affect availability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50132	In the Linux kernel, the following vulnerability has been resolved: tracing/probes: Fix MAX_TRACE_ARGS limit handling When creating a trace_probe we would set nr_args prior to truncating the arguments to MAX_TRACE_ARGS. However, we would only initialize arguments up to the limit. This caused invalid memory access when attempting to set up probes with more than 128 fetchargs. BUG: kernel NULL pointer dereference, address: 0000000000000020 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: Oops: 0000 [#1] PREEMPT SMP PTI CPU: 0 UID: 0 PID: 1769 Comm: cat Not tainted 6.11.0-rc7+ #8 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-1.fc39 04/01/2014 RIP: 0010:__set_print_fmt+0x134/0x330 Resolve the issue by applying the MAX_TRACE_ARGS limit earlier. Return an error when there are too many arguments instead of silently truncating.	5.5	More Details
CVE-2024-48241	An issue in radare2 v5.8.0 through v5.9.4 allows a local attacker to cause a denial of service via the __bf_div function.	5.5	More Details
CVE-2024-44233	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14.7.1, macOS Ventura 13.7.1, visionOS 2.1, watchOS 11.1, tvOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, iOS 18.1 and iPadOS 18.1. Parsing a maliciously crafted video file may lead to unexpected system termination.	5.5	More Details
CVE-2024-44232	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14.7.1, macOS Ventura 13.7.1, visionOS 2.1, watchOS 11.1, tvOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, iOS 18.1 and iPadOS 18.1. Parsing a maliciously crafted video file may lead to unexpected system termination.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50107	In the Linux kernel, the following vulnerability has been resolved: platform/x86/intel/pmc: Fix pmc_core_iounmap to call iounmap for valid addresses Commit 50c6dbdfd16e ("x86/ioremap: Improve iounmap() address range checks") introduces a WARN when adrress ranges of iounmap are invalid. On Thinkpad P1 Gen 7 (Meteor Lake-P) this caused the following warning to appear: WARNING: CPU: 7 PID: 713 at arch/x86/mm/ioremap.c:461 iounmap+0x58/0x1f0 Modules linked in: rfkill(+) snd_timer(+) fjes(+) snd soundcore intel_pmc_core(+) int3403_thermal(+) int340x_thermal_zone intel_vsec pmt_telemetry acpi_pad pmt_class acpi_tad int3400_thermal acpi_thermal_rel joydev loop nfnetlink zram xe drm_suballoc_helper nouveau i915 mxm_wmi drm_ttm_helper gpu_sched drm_gpuvm drm_exec drm_buddy i2c_algo_bit crct10dif_pclmul crc32_pclmul ttm crc32c_intel polyval_clmulni rtsx_pci_sdmmc ucsi_acpi polyval_generic mmc_core hid_multitouch drm_display_helper ghash_clmulni_intel typec_ucsi nvme sha512_ssse3 video sha256_ssse3 nvme_core intel_vpu sha1_ssse3 rtsx_pci cec typec nvme_auth i2c_hid_acpi i2c_hid wmi pinctrl_meteorlake serio_raw ip6_tables ip_tables fuse CPU: 7 UID: 0 PID: 713 Comm: (udev-worker) Not tainted 6.12.0-rc2iounmap+ #42 Hardware name: LENOVO 21KWCTO1WW/21KWCTO1WW, BIOS N48ET19W (1.06) 07/18/2024 RIP: 0010:iounmap+0x58/0x1f0 Code: 85 6a 01 00 00 48 8b 05 e6 e2 28 04 48 39 c5 72 19 eb 26 cc cc cc 48 ba 00 00 00 00 00 00 32 00 48 8d 44 02 ff 48 39 c5 72 23 <0f> 0b 48 83 c4 08 5b 5d 41 5c c3 cc cc cc cc 48 ba 00 00 00 00 00 RSP: 0018:ffff888131eff038 EFLAGS: 00010207 RAX: ffffc90000000000 RBX: 0000000000000000 RCX: ffff888e33b80000 RDX: dfffffc0000000000 RSI: ffff888e33bc29c0 RDI: 0000000000000000 RBP: 0000000000000000 R08: ffff8881598a8000 R09: ffff888e2ccedc10 R10: 0000000000000003 R11: ffffffffb3367634 R12: 00000000fe000000 R13: ffff888101d0da28 R14: ffffffffc2e437e0 R15: ffff888110b03b28 FS: 00007f3c1d4b3980(0000) GS:ffff888e33b80000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00005651cfc93578 CR3: 0000000124e4c002 CR4: 0000000000f70ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000ffff07f0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? __warn.cold+0xb6/0x176 ? iounmap+0x58/0x1f0 ? report_bug+0x1f4/0x2b0 ? handle_bug+0x58/0x90 ? exc_invalid_op+0x17/0x40 ? asm_exc_invalid_op+0x1a/0x20 ? iounmap+0x58/0x1f0 pmc_core_ssram_get_pmc+0x477/0x6c0 [intel_pmc_core] ? __pfx_pmc_core_ssram_get_pmc+0x10/0x10 [intel_pmc_core] ? __pfx_do_pci_enable_device+0x10/0x10 ? pci_wait_for_pending+0x60/0x110 ? pci_enable_device_flags+0x1e3/0x2e0 ? __pfx_mtl_core_init+0x10/0x10 [intel_pmc_core] pmc_core_ssram_init+0x7f/0x110 [intel_pmc_core] mtl_core_init+0xda/0x130 [intel_pmc_core] ? __mutex_init+0xb9/0x130 pmc_core_probe+0x27e/0x10b0 [intel_pmc_core] ? _raw_spin_lock_irqsave+0x96/0xf0 ? __pfx_pmc_core_probe+0x10/0x10 [intel_pmc_core] ? __pfx_mutex_unlock+0x10/0x10 ? __pfx_mutex_lock+0x10/0x10 ? device_pm_check_callbacks+0x82/0x370 ? acpi_dev_pm_attach+0x234/0x2b0 platform_probe+0x9f/0x150 really_probe+0x1e0/0x8a0 __driver_probe_device+0x18c/0x370 ? __pfx___driver_attach+0x10/0x10 driver_probe_device+0x4a/0x120 __driver_attach+0x190/0x4a0 ? __pfx___driver_attach+0x10/0x10 bus_for_each_dev+0x103/0x180 ? __pfx_bus_for_each_dev+0x10/0x10 ? klist_add_tail+0x136/0x270 bus_add_driver+0x2fc/0x540 driver_register+0x1a5/0x360 ? __pfx_pmc_core_driver_init+0x10/0x10 [intel_pmc_core] do_one_initcall+0xa4/0x380 ? __pfx_do_one_initcall+0x10/0x10 ? kasan_unpoison+0x44/0x70 do_init_module+0x296/0x800 load_module+0x5090/0x6ce0 ? __pfx_load_module+0x10/0x10 ? ima_post_read_file+0x193/0x200 ? __pfx_ima_post_read_file+0x10/0x10 ? rw_verify_area+0x152/0x4c0 ? kernel_read_file+0x257/0x750 ? __pfx_kernel_read_file+0x10/0x10 ? __pfx_filemap_get_read_batch+0x10/0x10 ? init_module_from_file+0xd1/0x130	5.5	More Details

CVE Number	Description	Base Score	Reference
	init_module_from_file+0xd1/0x130 ? __pfx_init_module_from_file+0x10/0 ---truncated---		
	In the Linux kernel, the following vulnerability has been resolved: LoongArch: Don't crash in stack_top() for tasks without vDSO Not all tasks have a vDSO mapped, for example		
CVE-2024-50133	kthreads never do. If such a task ever ends up calling stack_top(), it will derefence the NULL vdso pointer and crash. This can for example happen when using kunit: [<9000000000203874>] stack_top+0x58/0xa8 [<90000000002956cc>] arch_pick_mmap_layout+0x164/0x220 [<90000000003c284c>] kunit_vm_mmap_init+0x108/0x12c [<90000000003c1fbc>] __kunit_add_resource+0x38/0x8c [<90000000003c2704>] kunit_vm_mmap+0x88/0xc8 [<9000000000410b14>] usercopy_test_init+0xbc/0x25c [<90000000003c1db4>] kunit_try_run_case+0x5c/0x184 [<90000000003c3d54>] kunit_generic_run_threadfn_adapter+0x24/0x48 [<900000000022e4bc>] kthread+0xc8/0xd4 [<9000000000200ce8>] ret_from_kernel_thread+0xc/0xa4	5.5	More Details
CVE-2024-50134	In the Linux kernel, the following vulnerability has been resolved: drm/vboxvideo: Replace fake VLA at end of vbva_mouse_pointer_shape with real VLA Replace the fake VLA at end of the vbva_mouse_pointer_shape shape with a real VLA to fix a "memcpy: detected field-spanning write error" warning: [13.319813] memcpy: detected field-spanning write (size 16896) of single field "p->data" at drivers/gpu/drm/vboxvideo/hgsmi_base.c:154 (size 4) [13.319841] WARNING: CPU: 0 PID: 1105 at drivers/gpu/drm/vboxvideo/hgsmi_base.c:154 hgsmi_update_pointer_shape+0x192/0x1c0 [vboxvideo] [13.320038] Call Trace: [13.320173] hgsmi_update_pointer_shape [vboxvideo] [13.320184] vbox_cursor_atomic_update [vboxvideo] Note as mentioned in the added comment it seems the original length calculation for the allocated and send hgsmi buffer is 4 bytes too large. Changing this is not the goal of this patch, so this behavior is kept.	5.5	More Details
CVE-2024-45086	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A privileged user could exploit this vulnerability to expose sensitive information or consume memory resources.	5.5	More Details
CVE-2024-51513	Vulnerability of processes not being fully terminated in the VPN module Impact: Successful exploitation of this vulnerability will affect power consumption.	5.5	More Details
CVE-2024-50136	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Unregister notifier on eswitch init failure It otherwise remains registered and a subsequent attempt at eswitch enabling might trigger warnings of the sort: [682.589148] ------------[cut here]------------ [682.590204] notifier callback eswitch_vport_event [mlx5_core] already registered [682.590256] WARNING: CPU: 13 PID: 2660 at kernel/notifier.c:31 notifier_chain_register+0x3e/0x90 [...snipped] [682.610052] Call Trace: [682.610369] <TASK> [682.610663] ? __warn+0x7c/0x110 [682.611050] ? notifier_chain_register+0x3e/0x90 [682.611556] ? report_bug+0x148/0x170 [682.611977] ? handle_bug+0x36/0x70 [682.612384] ? exc_invalid_op+0x13/0x60 [682.612817] ? asm_exc_invalid_op+0x16/0x20 [682.613284] ? notifier_chain_register+0x3e/0x90 [682.613789] atomic_notifier_chain_register+0x25/0x40 [682.614322] mlx5_eswitch_enable_locked+0x1d4/0x3b0 [mlx5_core] [682.614965] mlx5_eswitch_enable+0xc9/0x100 [mlx5_core] [682.615551] mlx5_device_enable_sriov+0x25/0x340 [mlx5_core] [682.616170] mlx5_core_sriov_configure+0x50/0x170 [mlx5_core] [682.616789] sriov_numvfs_store+0xb0/0x1b0 [682.617248] kernfs_fop_write_iter+0x117/0x1a0 [682.617734] vfs_write+0x231/0x3f0 [682.618138] ksys_write+0x63/0xe0 [682.618536] do_syscall_64+0x4c/0x100 [682.618958] entry_SYSCALL_64_after_hwframe+0x4b/0x53	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50137	In the Linux kernel, the following vulnerability has been resolved: reset: starfive: jh71x0: Fix accessing the empty member on JH7110 SoC data->asserted will be NULL on JH7110 SoC since commit 82327b127d41 ("reset: starfive: Add StarFive JH7110 reset driver") was added. Add the judgment condition to avoid errors when calling reset_control_status on JH7110 SoC.	5.5	More Details
CVE-2024-50138	In the Linux kernel, the following vulnerability has been resolved: bpf: Use raw_spinlock_t in ringbuf The function __bpf_ringbuf_reserve is invoked from a tracepoint, which disables preemption. Using spinlock_t in this context can lead to a "sleep in atomic" warning in the RT variant. This issue is illustrated in the example below: BUG: sleeping function called from invalid context at kernel/locking/spinlock_rt.c:48 in_atomic(): 1, irqs_disabled(): 0, non_block: 0, pid: 556208, name: test_progs preempt_count: 1, expected: 0 RCU nest depth: 1, expected: 1 INFO: lockdep is turned off. Preemption disabled at: [<ffffd33a5c88ea44>] migrate_enable+0xc0/0x39c CPU: 7 PID: 556208 Comm: test_progs Tainted: G Hardware name: Qualcomm SA8775P Ride (DT) Call trace: dump_backtrace+0xac/0x130 show_stack+0x1c/0x30 dump_stack_lvl+0xac/0xe8 dump_stack+0x18/0x30 __might_resched+0x3bc/0x4fc rt_spin_lock+0x8c/0x1a4 __bpf_ringbuf_reserve+0xc4/0x254 bpf_ringbuf_reserve_dynptr+0x5c/0xdc bpf_prog_ac3d15160d62622a_test_read_write+0x104/0x238 trace_call_bpf+0x238/0x774 perf_call_bpf_enter.isra.0+0x104/0x194 perf_syscall_enter+0x2f8/0x510 trace_sys_enter+0x39c/0x564 syscall_trace_enter+0x220/0x3c0 do_el0_svc+0x138/0x1dc el0_svc+0x54/0x130 el0t_64_sync_handler+0x134/0x150 el0t_64_sync+0x17c/0x180 Switch the spinlock to raw_spinlock_t to avoid this error.	5.5	More Details
CVE-2024-49377	OctoPrint provides a web interface for controlling consumer 3D printers. OctoPrint versions up until and including 1.10.2 contain reflected XSS vulnerabilities in the login dialog and the standalone application key confirmation dialog. An attacker who successfully talked a victim into clicking on a specially crafted login link, or a malicious app running on a victim's computer triggering the application key workflow with specially crafted parameters and then redirecting the victim to the related standalone confirmation dialog could use this to retrieve or modify sensitive configuration settings, interrupt prints or otherwise interact with the OctoPrint instance in a malicious way. The above mentioned specific vulnerabilities of the login dialog and the standalone application key confirmation dialog have been patched in the bugfix release 1.10.3 by individual escaping of the detected locations. A global change throughout all of OctoPrint's templating system with the upcoming 1.11.0 release will handle this further, switching to globally enforced automatic escaping and thus reducing the attack surface in general. The latter will also improve the security of third party plugins. During a transition period, third party plugins will be able to opt into the automatic escaping. With OctoPrint 1.13.0, automatic escaping will be switched over to be enforced even for third party plugins, unless they explicitly opt-out.	5.5	More Details
CVE-2024-50108	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Disable PSR-SU on Parade 08-01 TCON too Stuart Hayhurst has found that both at bootup and fullscreen VA-API video is leading to black screens for around 1 second and kernel WARNING [1] traces when calling dmub_psr_enable() with Parade 08-01 TCON. These symptoms all go away with PSR-SU disabled for this TCON, so disable it for now while DMUB traces [2] from the failure can be analyzed and the failure state properly root caused. (cherry picked from commit afb634a6823d8d9db23c5fb04f79c5549349628b)	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44234	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14.7.1, macOS Ventura 13.7.1, visionOS 2.1, watchOS 11.1, tvOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, iOS 18.1 and iPadOS 18.1. Parsing a maliciously crafted video file may lead to unexpected system termination.	5.5	More Details
CVE-2024-50105	In the Linux kernel, the following vulnerability has been resolved: ASoC: qcom: sc7280: Fix missing Soundwire runtime stream alloc Commit 15c7fab0e047 ("ASoC: qcom: Move Soundwire runtime stream alloc to soundcards") moved the allocation of Soundwire stream runtime from the Qualcomm Soundwire driver to each individual machine sound card driver, except that it forgot to update SC7280 card. Just like for other Qualcomm sound cards using Soundwire, the card driver should allocate and release the runtime. Otherwise sound playback will result in a NULL pointer dereference or other effect of uninitialized memory accesses (which was confirmed on SDM845 having similar issue).	5.5	More Details
CVE-2024-50100	In the Linux kernel, the following vulnerability has been resolved: USB: gadget: dummy-hcd: Fix "task hung" problem The syzbot fuzzer has been encountering "task hung" problems ever since the dummy-hcd driver was changed to use hrtimers instead of regular timers. It turns out that the problems are caused by a subtle difference between the timer_pending() and hrtimer_active() APIs. The changeover blindly replaced the first by the second. However, timer_pending() returns True when the timer is queued but not when its callback is running, whereas hrtimer_active() returns True when the hrtimer is queued _or_ its callback is running. This difference occasionally caused dummy_urb_enqueue() to think that the callback routine had not yet started when in fact it was almost finished. As a result the hrtimer was not restarted, which made it impossible for the driver to dequeue later the URB that was just enqueued. This caused usb_kill_urb() to hang, and things got worse from there. Since hrtimers have no API for telling when they are queued and the callback isn't running, the driver must keep track of this for itself. That's what this patch does, adding a new "timer_pending" flag and setting or clearing it at the appropriate times.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50093	In the Linux kernel, the following vulnerability has been resolved: thermal: intel: int340x: processor: Fix warning during module unload The processor_thermal driver uses pcim_device_enable() to enable a PCI device, which means the device will be automatically disabled on driver detach. Thus there is no need to call pci_disable_device() again on it. With recent PCI device resource management improvements, e.g. commit f748a07a0b64 ("PCI: Remove legacy pcim_release()"), this problem is exposed and triggers the warining below. [224.010735] proc_thermal_pci 0000:00:04.0: disabling already-disabled device [224.010747] WARNING: CPU: 8 PID: 4442 at drivers/pci/pci.c:2250 pci_disable_device+0xe5/0x100 ... [224.010844] Call Trace: [224.010845] <TASK> [224.010847] ? show_regs+0x6d/0x80 [224.010851] ? __warn+0x8c/0x140 [224.010854] ? pci_disable_device+0xe5/0x100 [224.010856] ? report_bug+0x1c9/0x1e0 [224.010859] ? handle_bug+0x46/0x80 [224.010862] ? exc_invalid_op+0x1d/0x80 [224.010863] ? asm_exc_invalid_op+0x1f/0x30 [224.010867] ? pci_disable_device+0xe5/0x100 [224.010869] ? pci_disable_device+0xe5/0x100 [224.010871] ? kfree+0x21a/0x2b0 [224.010873] pcim_disable_device+0x20/0x30 [224.010875] devm_action_release+0x16/0x20 [224.010878] release_nodes+0x47/0xc0 [224.010880] devres_release_all+0x9f/0xe0 [224.010883] device_unbind_cleanup+0x12/0x80 [224.010885] device_release_driver_internal+0x1ca/0x210 [224.010887] driver_detach+0x4e/0xa0 [224.010889] bus_remove_driver+0x6f/0xf0 [224.010890] driver_unregister+0x35/0x60 [224.010892] pci_unregister_driver+0x44/0x90 [224.010894] proc_thermal_pci_driver_exit+0x14/0x5f0 [processor_thermal_device_pci] ... [224.010921] ---[end trace 0000000000000000]--- Remove the excess pci_disable_device() calls. [rjw: Subject and changelog edits]	5.5	More Details
CVE-2024-50094	In the Linux kernel, the following vulnerability has been resolved: sfc: Don't invoke xdp_do_flush() from netpoll. Yury reported a crash in the sfc driver originated from netpoll_send_udp(). The netconsole sends a message and then netpoll invokes the driver's NAPI function with a budget of zero. It is dedicated to allow driver to free TX resources, that it may have used while sending the packet. In the netpoll case the driver invokes xdp_do_flush() unconditionally, leading to crash because bpf_net_context was never assigned. Invoke xdp_do_flush() only if budget is not zero.	5.5	More Details
CVE-2024-50090	In the Linux kernel, the following vulnerability has been resolved: drm/xe/oa: Fix overflow in oa batch buffer By default xe_bb_create_job() appends a MI_BATCH_BUFFER_END to batch buffer, this is not a problem if batch buffer is only used once but oa reuses the batch buffer for the same metric and at each call it appends a MI_BATCH_BUFFER_END, printing the warning below and then overflowing. [381.072016] ------------[cut here]------------ [381.072019] xe 0000:00:02.0: [drm] Assertion `bb->len * 4 + bb_prefetch(q->gt) <= size` failed! platform: LUNARLAKE subplatform: 1 graphics: Xe2_LPG / Xe2_HPG 20.04 step B0 media: Xe2_LPM / Xe2_HPM 20.00 step B0 tile: 0 VRAM 0 B GT: 0 type 1 So here checking if batch buffer already have MI_BATCH_BUFFER_END if not append it. v2: - simply fix, suggestion from Ashutosh (cherry picked from commit 9ba0e0f30ca42a98af3689460063edfb6315718a)	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50095	In the Linux kernel, the following vulnerability has been resolved: RDMA/mad: Improve handling of timed out WRs of mad agent Current timeout handler of mad agent acquires/releases mad_agent_priv lock for every timed out WRs. This causes heavy locking contention when higher no. of WRs are to be handled inside timeout handler. This leads to softlockup with below trace in some use cases where rdma-cm path is used to establish connection between peer nodes Trace: ----- BUG: soft lockup - CPU#4 stuck for 26s! [kworker/u128:3:19767] CPU: 4 PID: 19767 Comm: kworker/u128:3 Kdump: loaded Tainted: G OE ------- --- 5.14.0-427.13.1.el9_4.x86_64 #1 Hardware name: Dell Inc. PowerEdge R740/01YM03, BIOS 2.4.8 11/26/2019 Workqueue: ib_mad1 timeout_sends [ib_core] RIP: 0010:__do_softirq+0x78/0x2ac RSP: 0018:ffffb253449e4f98 EFLAGS: 00000246 RAX: 00000000ffffffff RBX: 0000000000000000 RCX: 000000000000001f RDX: 000000000000001d RSI: 000000003d1879ab RDI: fff363b66fd3a86b RBP: ffffb253604cbcd8 R08: 0000009065635f3b R09: 0000000000000000 R10: 0000000000000040 R11: ffffb253449e4ff8 R12: 0000000000000000 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000040 FS: 0000000000000000(0000) GS:ffff8caa1fc80000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007fd9ec9db900 CR3: 0000000891934006 CR4: 00000000007706e0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <IRQ> ? show_trace_log_lvl+0x1c4/0x2df ? show_trace_log_lvl+0x1c4/0x2df ? __irq_exit_rcu+0xa1/0xc0 ? watchdog_timer_fn+0x1b2/0x210 ? __pfx_watchdog_timer_fn+0x10/0x10 ? __hrtimer_run_queues+0x127/0x2c0 ? hrtimer_interrupt+0xfc/0x210 ? __sysvec_apic_timer_interrupt+0x5c/0x110 ? sysvec_apic_timer_interrupt+0x37/0x90 ? asm_sysvec_apic_timer_interrupt+0x16/0x20 ? __do_softirq+0x78/0x2ac ? __do_softirq+0x60/0x2ac __irq_exit_rcu+0xa1/0xc0 sysvec_call_function_single+0x72/0x90 </IRQ> <TASK> asm_sysvec_call_function_single+0x16/0x20 RIP: 0010:_raw_spin_unlock_irq+0x14/0x30 RSP: 0018:ffffb253604cbd88 EFLAGS: 00000247 RAX: 000000000001960d RBX: 0000000000000002 RCX: ffff8cad2a064800 RDX: 000000008020001b RSI: 0000000000000001 RDI: ffff8cad5d39f66c RBP: ffff8cad5d39f600 R08: 0000000000000001 R09: 0000000000000000 R10: ffff8caa443e0c00 R11: ffffb253604cbcd8 R12: ffff8cacb8682538 R13: 0000000000000005 R14: ffffb253604cbd90 R15: ffff8cad5d39f66c cm_process_send_error+0x122/0x1d0 [ib_cm] timeout_sends+0x1dd/0x270 [ib_core] process_one_work+0x1e2/0x3b0 ? __pfx_worker_thread+0x10/0x10 worker_thread+0x50/0x3a0 ? __pfx_worker_thread+0x10/0x10 kthread+0xdd/0x100 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x29/0x50 </TASK> Simplified timeout handler by creating local list of timed out WRs and invoke send handler post creating the list. The new method acquires/ releases lock once to fetch the list and hence helps to reduce locking contetiong when processing higher no. of WRs	5.5	More Details
CVE-2024-50096	In the Linux kernel, the following vulnerability has been resolved: nouveau/dmem: Fix vulnerability in migrate_to_ram upon copy error The `nouveau_dmem_copy_one` function ensures that the copy push command is sent to the device firmware but does not track whether it was executed successfully. In the case of a copy error (e.g., firmware or hardware failure), the copy push command will be sent via the firmware channel, and `nouveau_dmem_copy_one` will likely report success, leading to the `migrate_to_ram` function returning a dirty HIGH_USER page to the user. This can result in a security vulnerability, as a HIGH_USER page that may contain sensitive or corrupted data could be returned to the user. To prevent this vulnerability, we allocate a zero page. Thus, in case of an error, a non-dirty (zero) page will be returned to the user.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50354	gnark is a fast zk-SNARK library that offers a high-level API to design circuits. In gnark 0.11.0 and earlier, deserialization of Groth16 verification keys allocate excessive memory, consuming a lot of resources and triggering a crash with the error fatal error: runtime: out of memory.	5.5	More Details
CVE-2024-50097	In the Linux kernel, the following vulnerability has been resolved: net: fec: don't save PTP state if PTP is unsupported Some platforms (such as i.MX25 and i.MX27) do not support PTP, so on these platforms fec_ptp_init() is not called and the related members in fep are not initialized. However, fec_ptp_save_state() is called unconditionally, which causes the kernel to panic. Therefore, add a condition so that fec_ptp_save_state() is not called if PTP is not supported.	5.5	More Details
CVE-2024-50091	In the Linux kernel, the following vulnerability has been resolved: dm vdo: don't refer to dedupe_context after releasing it Clear the dedupe_context pointer in a data_vio whenever ownership of the context is lost, so that vdo can't examine it accidentally.	5.5	More Details
CVE-2024-50099	In the Linux kernel, the following vulnerability has been resolved: arm64: probes: Remove broken LDR (literal) uprobe support The simulate_ldr_literal() and simulate_ldrsw_literal() functions are unsafe to use for uprobes. Both functions were originally written for use with kprobes, and access memory with plain C accesses. When uprobes was added, these were reused unmodified even though they cannot safely access user memory. There are three key problems: 1) The plain C accesses do not have corresponding extable entries, and thus if they encounter a fault the kernel will treat these as unintentional accesses to user memory, resulting in a BUG() which will kill the kernel thread, and likely lead to further issues (e.g. lockup or panic()). 2) The plain C accesses are subject to HW PAN and SW PAN, and so when either is in use, any attempt to simulate an access to user memory will fault. Thus neither simulate_ldr_literal() nor simulate_ldrsw_literal() can do anything useful when simulating a user instruction on any system with HW PAN or SW PAN. 3) The plain C accesses are privileged, as they run in kernel context, and in practice can access a small range of kernel virtual addresses. The instructions they simulate have a range of +/-1MiB, and since the simulated instructions must itself be a user instructions in the TTBR0 address range, these can address the final 1MiB of the TTBR1 acddress range by wrapping downwards from an address in the first 1MiB of the TTBR0 address range. In contemporary kernels the last 8MiB of TTBR1 address range is reserved, and accesses to this will always fault, meaning this is no worse than (1). Historically, it was theoretically possible for the linear map or vmemmap to spill into the final 8MiB of the TTBR1 address range, but in practice this is extremely unlikely to occur as this would require either: * Having enough physical memory to fill the entire linear map all the way to the final 1MiB of the TTBR1 address range. * Getting unlucky with KASLR randomization of the linear map such that the populated region happens to overlap with the last 1MiB of the TTBR address range. ... and in either case if we were to spill into the final page there would be larger problems as the final page would alias with error pointers. Practically speaking, (1) and (2) are the big issues. Given there have been no reports of problems since the broken code was introduced, it appears that no-one is relying on probing these instructions with uprobes. Avoid these issues by not allowing uprobes on LDR (literal) and LDRSW (literal), limiting the use of simulate_ldr_literal() and simulate_ldrsw_literal() to kprobes. Attempts to place uprobes on LDR (literal) and LDRSW (literal) will be rejected as arm_probe_decode_insn() will return INSN_REJECTED. In future we can consider introducing working uprobes support for these instructions, but this will require more significant work.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50098	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Set SDEV_OFFLINE when UFS is shut down There is a history of deadlock if reboot is performed at the beginning of booting. SDEV_QUIESCE was set for all LU's scsi_devices by UFS shutdown, and at that time the audio driver was waiting on blk_mq_submit_bio() holding a mutex_lock while reading the fw binary. After that, a deadlock issue occurred while audio driver shutdown was waiting for mutex_unlock of blk_mq_submit_bio(). To solve this, set SDEV_OFFLINE for all LUs except WLUN, so that any I/O that comes down after a UFS shutdown will return an error. [31.907781]I[0: swapper/0: 0] 1 130705007 1651079834 11289729804 0 D(2) 3 ffffff882e208000 * init [device_shutdown] [31.907793]I[0: swapper/0: 0] Mutex: 0xffffff8849a2b8b0: owner[0xffffff882e28cb00 kworker/6:0 :49] [31.907806]I[0: swapper/0: 0] Call trace: [31.907810]I[0: swapper/0: 0] __switch_to+0x174/0x338 [31.907819]I[0: swapper/0: 0] __schedule+0x5ec/0x9cc [31.907826]I[0: swapper/0: 0] schedule+0x7c/0xe8 [31.907834]I[0: swapper/0: 0] schedule_preempt_disabled+0x24/0x40 [31.907842]I[0: swapper/0: 0] __mutex_lock+0x408/0xdac [31.907849]I[0: swapper/0: 0] __mutex_lock_slowpath+0x14/0x24 [31.907858]I[0: swapper/0: 0] mutex_lock+0x40/0xec [31.907866]I[0: swapper/0: 0] device_shutdown+0x108/0x280 [31.907875]I[0: swapper/0: 0] kernel_restart+0x4c/0x11c [31.907883]I[0: swapper/0: 0] __arm64_sys_reboot+0x15c/0x280 [31.907890]I[0: swapper/0: 0] invoke_syscall+0x70/0x158 [31.907899]I[0: swapper/0: 0] el0_svc_common+0xb4/0xf4 [31.907909]I[0: swapper/0: 0] do_el0_svc+0x2c/0xb0 [31.907918]I[0: swapper/0: 0] el0_svc+0x34/0xe0 [31.907928]I[0: swapper/0: 0] el0t_64_sync_handler+0x68/0xb4 [31.907937]I[0: swapper/0: 0] el0t_64_sync+0x1a0/0x1a4 [31.908774]I[0: swapper/0: 0] 49 0 11960702 11236868007 0 D(2) 6 ffffff882e28cb00 * kworker/6:0 [__bio_queue_enter] [31.908783]I[0: swapper/0: 0] Call trace: [31.908788]I[0: swapper/0: 0] __switch_to+0x174/0x338 [31.908796]I[0: swapper/0: 0] __schedule+0x5ec/0x9cc [31.908803]I[0: swapper/0: 0] schedule+0x7c/0xe8 [31.908811]I[0: swapper/0: 0] __bio_queue_enter+0xb8/0x178 [31.908818]I[0: swapper/0: 0] blk_mq_submit_bio+0x194/0x67c [31.908827]I[0: swapper/0: 0] __submit_bio+0xb8/0x19c	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50104	In the Linux kernel, the following vulnerability has been resolved: ASoC: qcom: sdm845: add missing soundwire runtime stream alloc During the migration of Soundwire runtime stream allocation from the Qualcomm Soundwire controller to SoC's soundcard drivers the sdm845 soundcard was forgotten. At this point any playback attempt or audio daemon startup, for instance on sdm845-db845c (Qualcomm RB3 board), will result in stream pointer NULL dereference: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000020 Mem abort info: ESR = 0x0000000096000004 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 user pgtable: 4k pages, 48-bit VAs, pgdp=0000000101ecf000 [0000000000000020] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP Modules linked in: ... CPU: 5 UID: 0 PID: 1198 Comm: aplay Not tainted 6.12.0-rc2-qcomlt-arm64-00059-g9d78f315a362-dirty #18 Hardware name: Thundercomm Dragonboard 845c (DT) pstate: 60400005 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : sdw_stream_add_slave+0x44/0x380 [soundwire_bus] lr : sdw_stream_add_slave+0x44/0x380 [soundwire_bus] sp : ffff80008a2035c0 x29: ffff80008a2035c0 x28: ffff80008a203978 x27: 0000000000000000 x26: 00000000000000c0 x25: 0000000000000000 x24: ffff1676025f4800 x23: ffff167600ff1cb8 x22: ffff167600ff1c98 x21: 0000000000000003 x20: ffff167607316000 x19: ffff167604e64e80 x18: 0000000000000000 x17: 0000000000000000 x16: ffffcec265074160 x15: 0000000000000000 x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : 0000000000000000 x8 : 0000000000000000 x7 : 0000000000000000 x6 : ffff167600ff1cec x5 : ffffcec22cfa2010 x4 : 0000000000000000 x3 : 0000000000000003 x2 : ffff167613f836c0 x1 : 0000000000000000 x0 : ffff16761feb60b8 Call trace: sdw_stream_add_slave+0x44/0x380 [soundwire_bus] wsa881x_hw_params+0x68/0x80 [snd_soc_wsa881x] snd_soc_dai_hw_params+0x3c/0xa4 __soc_pcm_hw_params+0x230/0x660 dpcm_be_dai_hw_params+0x1d0/0x3f8 dpcm_fe_dai_hw_params+0x98/0x268 snd_pcm_hw_params+0x124/0x460 snd_pcm_common_ioctl+0x998/0x16e8 snd_pcm_ioctl+0x34/0x58 __arm64_sys_ioctl+0xac/0xf8 invoke_syscall+0x48/0x104 el0_svc_common.constprop.0+0x40/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x34/0xe0 el0t_64_sync_handler+0x120/0x12c el0t_64_sync+0x190/0x194 Code: aa0403fb f9418400 9100e000 9400102f (f8420f22) ---[end trace 0000000000000000]--- 0000000000006108 <sdw_stream_add_slave>: 6108: d503233f paciasp 610c: a9b97bfd stp x29, x30, [sp, #-112]! 6110: 910003fd mov x29, sp 6114: a90153f3 stp x19, x20, [sp, #16] 6118: a9025bf5 stp x21, x22, [sp, #32] 611c: aa0103f6 mov x22, x1 6120: 2a0303f5 mov w21, w3 6124: a90363f7 stp x23, x24, [sp, #48] 6128: aa0003f8 mov x24, x0 612c: aa0203f7 mov x23, x2 6130: a9046bf9 stp x25, x26, [sp, #64] 6134: aa0403f9 mov x25, x4 <-- x4 copied to x25 6138: a90573fb stp x27, x28, [sp, #80] 613c: aa0403fb mov x27, x4 6140: f9418400 ldr x0, [x0, #776] 6144: 9100e000 add x0, x0, #0x38 6148: 94000000 bl 0 <mutex_lock> 614c: f8420f22 ldr x2, [x25, #32]! <-- offset 0x44 ^^^ This is 0x6108 + offset 0x44 from the beginning of sdw_stream_add_slave() where data abort happens. wsa881x_hw_params() is called with stream = NULL and passes it further in register x4 (5th argu ---truncated---	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50102	In the Linux kernel, the following vulnerability has been resolved: x86: fix user address masking non-canonical speculation issue It turns out that AMD has a "Meltdown Lite(tm)" issue with non-canonical accesses in kernel space. And so using just the high bit to decide whether an access is in user space or kernel space ends up with the good old "leak speculative data" if you have the right gadget using the result: CVE-2020-12965 “Transient Execution of Non-Canonical Accesses“ Now, the kernel surrounds the access with a STAC/CLAC pair, and those instructions end up serializing execution on older Zen architectures, which closes the speculation window. But that was true only up until Zen 5, which renames the AC bit [1]. That improves performance of STAC/CLAC a lot, but also means that the speculation window is now open. Note that this affects not just the new address masking, but also the regular valid_user_address() check used by access_ok(), and the asm version of the sign bit check in the get_user() helpers. It does not affect put_user() or clear_user() variants, since there's no speculative result to be used in a gadget for those operations.	5.5	More Details
CVE-2024-50101	In the Linux kernel, the following vulnerability has been resolved: iommu/vt-d: Fix incorrect pci_for_each_dma_alias() for non-PCI devices Previously, the domain_context_clear() function incorrectly called pci_for_each_dma_alias() to set up context entries for non-PCI devices. This could lead to kernel hangs or other unexpected behavior. Add a check to only call pci_for_each_dma_alias() for PCI devices. For non-PCI devices, domain_context_clear_one() is called directly.	5.5	More Details
CVE-2024-50103	In the Linux kernel, the following vulnerability has been resolved: ASoC: qcom: Fix NULL Dereference in asoc_qcom_lpass_cpu_platform_probe() A devm_kzalloc() in asoc_qcom_lpass_cpu_platform_probe() could possibly return NULL pointer. NULL Pointer Dereference may be triggerred without addtional check. Add a NULL check for the returned pointer.	5.5	More Details
CVE-2024-48044	Missing Authorization vulnerability in ShortPixel – Convert WebP/AVIF & Optimize Images ShortPixel Image Optimizer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ShortPixel Image Optimizer: from n/a through 5.6.3.	5.4	More Details
CVE-2024-49256	Incorrect Authorization vulnerability in WPChill Htaccess File Editor allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Htaccess File Editor: from n/a through 1.0.18.	5.4	More Details
CVE-2024-21510	Versions of the package sinatra from 0.0.0 are vulnerable to Reliance on Untrusted Inputs in a Security Decision via the X-Forwarded-Host (XFH) header. When making a request to a method with redirect applied, it is possible to trigger an Open Redirect Attack by inserting an arbitrary address into this header. If used for caching purposes, such as with servers like Nginx, or as a reverse proxy, without handling the X-Forwarded-Host header, attackers can potentially exploit Cache Poisoning or Routing-based SSRF.	5.4	More Details
CVE-2024-30617	A Cross-Site Request Forgery (CSRF) vulnerability in Chamilo LMS 1.11.26 "/main/social/home.php," allows attackers to initiate a request that posts a fake post onto the user's social wall without their consent or knowledge.	5.4	More Details
CVE-2024-48312	WebLaudos v20.8 (118) was discovered to contain a cross-site scripting (XSS) vulnerability via the login page.	5.4	More Details
CVE-2024-8444	The Download Manager WordPress plugin before 3.3.00 doesn't sanitize some of it's shortcode parameters, leading to cross site scripting.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43928	Missing Authorization vulnerability in eyecix JobSearch allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JobSearch: from n/a through 2.5.4.	5.4	More Details
CVE-2024-51377	An issue in Ladybird Web Solution Faveo Helpdesk & Servicedesk (On-Premise and Cloud) 9.2.0 allows a remote attacker to execute arbitrary code via the Subject and Identifier fields	5.4	More Details
CVE-2024-39635	Missing Authorization vulnerability in KaineLabs Youzify allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Youzify: from n/a through 1.2.6.	5.4	More Details
CVE-2024-38733	Missing Authorization vulnerability in Meks Meks Video Importer allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Meks Video Importer: from n/a through 1.0.12.	5.4	More Details
CVE-2024-7424	The Multiple Page Generator Plugin – MPG plugin for WordPress is vulnerable to unauthorized modification of and access to data due to a missing capability check on several functions in all versions up to, and including, 4.0.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to invoke those functions intended for admin use resulting in subscribers being able to upload csv files and view the contents of MPG projects.	5.4	More Details
CVE-2024-38737	Missing Authorization vulnerability in Reservation Diary ReDi Restaurant Reservation allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects ReDi Restaurant Reservation: from n/a through 24.0422.	5.4	More Details
CVE-2024-38740	Missing Authorization vulnerability in Packlink Shipping S.L. Packlink PRO shipping module allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Packlink PRO shipping module: from n/a through 3.4.6.	5.4	More Details
CVE-2024-38774	Missing Authorization vulnerability in SiteGround SiteGround Security allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects SiteGround Security: from n/a through 1.5.0.	5.4	More Details
CVE-2024-44021	Missing Authorization vulnerability in Truepush allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Truepush: from n/a through 1.0.8.	5.4	More Details
CVE-2024-49685	Cross-Site Request Forgery (CSRF) vulnerability in Smash Balloon Custom Twitter Feeds (Tweets Widget) allows Cross Site Request Forgery.This issue affects Custom Twitter Feeds (Tweets Widget): from n/a through 2.2.3.	5.4	More Details
CVE-2024-43962	Missing Authorization vulnerability in LWS LWS Affiliation allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects LWS Affiliation: from n/a through 2.3.4.	5.4	More Details
CVE-2024-50419	Incorrect Authorization vulnerability in Wpsoul Greenshift – animation and page builder blocks allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Greenshift – animation and page builder blocks: from n/a through 9.7.	5.4	More Details
CVE-2024-48569	Proactive Risk Manager version 9.1.1.0 is affected by multiple Cross-Site Scripting (XSS) vulnerabilities in the add/edit form fields, at the urls starting with the subpaths: /ar/config/configuation/ and /ar/config/risk-strategy-control/	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48807	Cross Site Scripting vulnerability in PHPGurukul Doctor Appointment Management System v.1.0 allows a local attacker to execute arbitrary code via the search parameter.	5.4	More Details
CVE-2024-37483	Missing Authorization vulnerability in Post Grid Team by RadiusTheme The Post Grid allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Post Grid: from n/a through 7.7.4.	5.4	More Details
CVE-2024-43260	Missing Authorization vulnerability in Creative Motion Clearfy Cache allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Clearfy Cache: from n/a through 2.2.4.	5.4	More Details
CVE-2024-43268	Access Control vulnerability in WPBackItUp Backup and Restore WordPress allows . This issue affects Backup and Restore WordPress: from n/a through 1.50.	5.4	More Details
CVE-2024-43273	Missing Authorization vulnerability in icegram Icegram Collect plugin allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Icegram Collect plugin: from n/a through 1.3.14.	5.4	More Details
CVE-2024-37439	Missing Authorization vulnerability in Uncanny Owl Uncanny Toolkit Pro for LearnDash allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Uncanny Toolkit Pro for LearnDash: from n/a through 4.1.4.0	5.4	More Details
CVE-2024-37425	Missing Authorization vulnerability in Automattic Newspack Blocks newspack-blocks allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Newspack Blocks: from n/a through 3.0.8.	5.4	More Details
CVE-2024-37415	Missing Authorization vulnerability in E2Pdf.Com allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects e2pdf: from n/a through 1.20.27.	5.4	More Details
CVE-2024-37250	Missing Authorization vulnerability in WPEngine Inc. Advanced Custom Fields PRO allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Advanced Custom Fields PRO: from n/a through 6.3.1.	5.4	More Details
CVE-2024-9867	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Open Map Widget' marker_content parameter in all versions up to, and including, 5.10.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2024-43312	Missing Authorization vulnerability in WPClever WPC Frequently Bought Together for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WPC Frequently Bought Together for WooCommerce: from n/a through 7.1.9.	5.4	More Details
CVE-2024-9868	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Age Gate Widget 'url' parameter in all versions up to, and including, 5.10.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37207	Missing Authorization vulnerability in Theme4Press Demo Awesome allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Demo Awesome: from n/a through 1.0.2.	5.4	More Details
CVE-2024-28052	The WBR-6012 is a wireless SOHO router. It is a low-cost device which functions as an internet gateway for homes and small offices while aiming to be easy to configure and operate. In addition to providing a WiFi access point, the device serves as a 4-port wired router and implements a variety of common SOHO router capabilities such as port forwarding, quality-of-service, web-based administration, a DHCP server, a basic DMZ, and UPnP capabilities.	5.3	More Details
CVE-2024-51514	Vulnerability of pop-up windows belonging to no app in the VPN module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.3	More Details
CVE-2024-51493	OctoPrint provides a web interface for controlling consumer 3D printers. OctoPrint versions up until and including 1.10.2 contain a vulnerability that allows an attacker that has gained temporary control over an authenticated victim's OctoPrint browser session to retrieve/recreate/delete the user's or - if the victim has admin permissions - the global API key without having to reauthenticate by re-entering the user account's password. An attacker could use a stolen API key to access OctoPrint through its API, or disrupt workflows depending on the API key they deleted. This vulnerability will be patched in version 1.10.3 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2024-33626	The LevelOne WBR-6012 router contains a vulnerability within its web application that allows unauthenticated disclosure of sensitive information, such as the WiFi WPS PIN, through a hidden page accessible by an HTTP request. Disclosure of this information could enable attackers to connect to the device's WiFi network.	5.3	More Details
CVE-2024-10599	A vulnerability, which was classified as problematic, has been found in Tongda OA 2017 up to 11.7. This issue affects some unknown processing of the file /inc/package_static_resources.php. The manipulation leads to resource consumption. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2024-51518	Vulnerability of message types not being verified in the advanced messaging modul Impact: Successful exploitation of this vulnerability may affect availability.	5.3	More Details
CVE-2024-50512	Generation of Error Message Containing Sensitive Information vulnerability in Posti Posti Shipping allows Retrieve Embedded Sensitive Data.This issue affects Posti Shipping: from n/a through 3.10.2.	5.3	More Details
CVE-2024-31152	The LevelOne WBR-6012 router with firmware R0.40e6 is vulnerable to improper resource allocation within its web application, where a series of crafted HTTP requests can cause a reboot. This could lead to network service interruptions.	5.3	More Details
CVE-2024-10598	A vulnerability classified as critical was found in Tongda OA 11.2/11.3/11.4/11.5/11.6. This vulnerability affects unknown code of the file general/hr/setting/attendance/leave/data.php of the component Annual Leave Handler. The manipulation leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10544	The Woo Manage Fraud Orders plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 6.1.7 through publicly exposed log files. This makes it possible for unauthenticated attackers to view potentially sensitive information about users contained in the exposed log files.	5.3	More Details
CVE-2024-9700	The Forminator Forms – Contact Form, Payment Form & Custom Form Builder plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.36.0 via the submit_quizzes() function due to missing validation on the 'entry_id' user controlled key. This makes it possible for unauthenticated attackers to modify other user's quiz submissions.	5.3	More Details
CVE-2024-49773	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. Poor input validation in export allows authenticated user do a SQL injection attack. User-controlled input is used to build SQL query. `current_post` parameter in `export` entry point can be abused to perform blind SQL injection via generateSearchWhere(). Allows for Information disclosure, including personally identifiable information. This issue has been addressed in versions 7.14.6 and 8.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2024-33603	The LevelOne WBR-6012 router has an information disclosure vulnerability in its web application, which allows unauthenticated users to access a verbose system log page and obtain sensitive data, such as memory addresses and IP addresses for login attempts. This flaw could lead to session hijacking due to the device's reliance on IP address for authentication.	5.3	More Details
CVE-2024-50353	ICG.AspNetCore.Utilities.CloudStorage is a collection of cloud storage utilities to assist with the management of files for cloud upload. Users of this library that set a duration for a SAS Uri with a value other than 1 hour may have generated a URL with a duration that is longer, or shorter than desired. Users not implemented SAS Uri's are unaffected. This issue was resolved in version 8.0.0 of the library.	5.3	More Details
CVE-2024-10559	A vulnerability was found in SourceCodester Airport Booking Management System 1.0 and classified as critical. Affected by this issue is the function details of the component Passport Number Handler. The manipulation leads to buffer overflow. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2024-10620	A vulnerability was found in knightliao Disconf 2.6.36. It has been classified as critical. This affects an unknown part of the file /api/config/list of the component Configuration Center. The manipulation leads to improper authentication. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	5.3	More Details
CVE-2024-9430	The Get Quote For Woocommerce – Request A Quote For Woocommerce plugin for WordPress is vulnerable to unauthorized access of Quote data due to a missing capability check on the ct_tepfw_wp_loaded function in all versions up to, and including, 1.0.0. This makes it possible for unauthenticated attackers to download Quote PDF and CSV documents.	5.3	More Details
CVE-2024-47358	Missing Authorization vulnerability in Popup Maker allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Popup Maker: from n/a through 1.19.2.	5.3	More Details
CVE-2024-38748	Access Control vulnerability in TheInnovs EleForms allows . This issue affects EleForms: from n/a through 2.9.9.9.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37506	Missing Authorization vulnerability in Charitable Donations & Fundraising Team Charitable allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Charitable: from n/a through 1.8.1.7.	5.3	More Details
CVE-2024-38743	Access Control vulnerability in Upqode Plum: Spin Wheel & Email Pop-up allows . This issue affects Plum: Spin Wheel & Email Pop-up: from n/a through 2.0.	5.3	More Details
CVE-2024-38702	Missing Authorization vulnerability in Tyche Softwares Product Delivery Date for WooCommerce – Lite allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Product Delivery Date for WooCommerce – Lite: from n/a through 2.7.2.	5.3	More Details
CVE-2024-38690	Missing Authorization vulnerability in Avirtum iPanorama 360 WordPress Virtual Tour Builder allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects iPanorama 360 WordPress Virtual Tour Builder: from n/a through 1.8.3.	5.3	More Details
CVE-2024-47302	Missing Authorization vulnerability in WPManageNinja LLC Fluent Support allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fluent Support: from n/a through 1.8.0.	5.3	More Details
CVE-2024-37926	Missing Authorization vulnerability in Alex Volkov WP Accessibility Helper (WAH) allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WP Accessibility Helper (WAH): from n/a through 0.6.2.9.	5.3	More Details
CVE-2024-37921	Missing Authorization vulnerability in Kiboko Labs Chained Quiz allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Chained Quiz: from n/a through 1.3.2.8.	5.3	More Details
CVE-2024-47311	Missing Authorization vulnerability in Kraft Plugins Wheel of Life allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Wheel of Life: from n/a through 1.1.8.	5.3	More Details
CVE-2024-37475	Missing Authorization vulnerability in Automattic Newspack Newsletters allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Newspack Newsletters: from n/a through 2.13.2.	5.3	More Details
CVE-2024-41741	IBM TXSeries for Multiplatforms 10.1 could allow an attacker to determine valid usernames due to an observable timing discrepancy which could be used in further attacks against the system.	5.3	More Details
CVE-2024-37468	Missing Authorization vulnerability in blazethemes Newsmatic allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Newsmatic: from n/a through 1.3.1.	5.3	More Details
CVE-2024-37463	Missing Authorization vulnerability in CRM Perks CRM Perks Forms allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects CRM Perks Forms: from n/a through 1.1.5.	5.3	More Details
CVE-2024-37456	Missing Authorization vulnerability in Noptin Newsletter Noptin allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Noptin: from n/a through 3.4.2.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37444	Missing Authorization vulnerability in WPMU DEV Defender Security allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Defender Security: from n/a through 4.7.1.	5.3	More Details
CVE-2024-37427	Missing Authorization vulnerability in Arraytics Timetics allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Timetics: from n/a through 1.0.21.	5.3	More Details
CVE-2024-37411	Missing Authorization vulnerability in Team Emilia Projects Progress Planner allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Progress Planner: from n/a through 0.9.1.	5.3	More Details
CVE-2024-37276	Missing Authorization vulnerability in fifu.App Featured Image from URL allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Featured Image from URL: from n/a through 4.8.1.	5.3	More Details
CVE-2024-38745	Missing Authorization vulnerability in Rymera Web Co Wholesale Suite allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Wholesale Suite: from n/a through 2.1.12.	5.3	More Details
CVE-2024-38769	Missing Authorization vulnerability in Tyche Softwares Arconix Shortcodes allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Arconix Shortcodes: from n/a through 2.1.11.	5.3	More Details
CVE-2024-37255	Missing Authorization vulnerability in Wpmet Elements kit Elementor addons allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Elements kit Elementor addons: from n/a through 3.1.4.	5.3	More Details
CVE-2024-43253	Missing Authorization vulnerability in Zaytech Smart Online Order for Clover allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Smart Online Order for Clover: from n/a through 1.5.6.	5.3	More Details
CVE-2024-43923	Missing Authorization vulnerability in Arraytics Timetics allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Timetics: from n/a through 1.0.23.	5.3	More Details
CVE-2024-43919	Access Control vulnerability in YARPP YARPP allows . This issue affects YARPP: from n/a through 5.30.10.	5.3	More Details
CVE-2024-10540	The Appointment Booking Calendar Plugin and Scheduling Plugin – BookingPress plugin for WordPress is vulnerable to SQL Injection via the 'service' parameter of the bookingpress_form shortcode in all versions up to, and including, 1.1.16 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Subscriber-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	5.3	More Details
CVE-2024-43323	Missing Authorization vulnerability in ReviewX ReviewX allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ReviewX: from n/a through 1.6.28.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43290	Missing Authorization vulnerability in Atarim allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Atarim: from n/a through 4.0.1.	5.3	More Details
CVE-2024-43277	Missing Authorization vulnerability in AyeCode Ltd UsersWP allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects UsersWP: from n/a through 1.2.15.	5.3	More Details
CVE-2024-43270	Missing Authorization vulnerability in WPBackItUp Backup and Restore WordPress allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Backup and Restore WordPress: from n/a through 1.50.	5.3	More Details
CVE-2024-43219	Missing Authorization vulnerability in ووکامرس فارسی Persian WooCommerce allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Persian WooCommerce: from n/a through 7.1.6.	5.3	More Details
CVE-2024-38783	Missing Authorization vulnerability in Tyche Softwares Arconix FAQ allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Arconix FAQ: from n/a through 1.9.4.	5.3	More Details
CVE-2024-43159	Missing Authorization vulnerability in Masteriyo Masteriyo - LMS allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Masteriyo - LMS: from n/a through 1.11.6.	5.3	More Details
CVE-2024-44038	Missing Authorization vulnerability in WP Sunshine Sunshine Photo Cart allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sunshine Photo Cart: from n/a through 3.2.9.	5.3	More Details
CVE-2024-43120	Missing Authorization vulnerability in XSERVER Inc. TypeSquare Webfonts allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects TypeSquare Webfonts: from n/a through 2.0.7.	5.3	More Details
CVE-2024-39654	Missing Authorization vulnerability in Fetch Designs Sign-up Sheets allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sign-up Sheets: from n/a through 2.2.12.	5.3	More Details
CVE-2024-39625	Missing Authorization vulnerability in icegram Icegram allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Icegram: from n/a through 3.1.24.	5.3	More Details
CVE-2024-38794	Missing Authorization vulnerability in MediaRon LLC Custom Query Blocks allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Custom Query Blocks: from n/a through 5.2.0.	5.3	More Details
CVE-2024-38792	Missing Authorization vulnerability in ConveyThis Translate Team Language Translate Widget for WordPress – ConveyThis allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Language Translate Widget for WordPress – ConveyThis: from n/a through 234.	5.3	More Details
CVE-2024-37269	Missing Authorization vulnerability in StylemixThemes Masterstudy Elementor Widgets allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Masterstudy Elementor Widgets: from n/a through 1.2.2.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44019	Missing Authorization vulnerability in Renzo Johnson Contact Form 7 Campaign Monitor Extension allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Contact Form 7 Campaign Monitor Extension: from n/a through 0.4.67.	5.3	More Details
CVE-2024-37220	Missing Authorization vulnerability in OptinlyHQ Optinly allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Optinly: from n/a through 1.0.18.	5.3	More Details
CVE-2024-10654	A vulnerability has been found in TOTOLINK LR350 up to 9.3.5u.6369 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /formLoginAuth.htm. The manipulation of the argument authCode with the input 1 leads to authorization bypass. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 9.3.5u.6698_B20230810 is able to address this issue. It is recommended to upgrade the affected component.	5.3	More Details
CVE-2024-37123	Missing Authorization vulnerability in VowelWeb Ibtana allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ibtana: from n/a through 1.2.3.3.	5.3	More Details
CVE-2024-47359	Missing Authorization vulnerability in Depicter Slider and Popup by Averta Depicter Slider allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Depicter Slider: from n/a through 3.2.2.	5.3	More Details
CVE-2024-51500	Meshtastic firmware is a device firmware for the Meshtastic project. The Meshtastic firmware does not check for packets claiming to be from the special broadcast address (0xFFFFFFFF) which could result in unexpected behavior and potential for DDoS attacks on the network. A malicious actor could craft a packet to be from that address which would result in an amplification of this one message into every node on the network sending multiple messages. Such an attack could result in degraded network performance for all users as the available bandwidth is consumed. This issue has been addressed in release version 2.5.6. All users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2024-37226	Missing Authorization vulnerability in Kanban for WordPress Kanban Boards for WordPress allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Kanban Boards for WordPress: from n/a through 2.5.21.	5.3	More Details
CVE-2024-37119	Missing Authorization vulnerability in Uncanny Owl Uncanny Automator Pro allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Uncanny Automator Pro: from n/a through 5.3.0.0.	5.3	More Details
CVE-2024-31973	Hitron CODA-4582 2AHKM-CODA4589 7.2.4.5.1b8 devices allow a remote attacker within Wi-Fi proximity to conduct stored XSS attacks via the 'Network Name (SSID)' input fields to the /index.html#wireless_basic page.	5.2	More Details
CVE-2024-51517	Vulnerability of improper memory access in the phone service module Impact: Successful exploitation of this vulnerability may affect availability.	5.1	More Details
CVE-2024-51527	Permission control vulnerability in the Gallery app Impact: Successful exploitation of this vulnerability may affect service confidentiality.	5.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45185	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 9110, W920, W930, Modem 5123, Modem 5300. There is an out-of-bounds write due to a heap overflow in the GPRS protocol.	5.1	More Details
CVE-2024-51519	Vulnerability of input parameters not being verified in the HDC module Impact: Successful exploitation of this vulnerability may affect availability.	5.0	More Details
CVE-2024-10749	A vulnerability, which was classified as critical, was found in ThinkAdmin up to 6.1.67. Affected is the function script of the file /app/admin/controller/api/Plugs.php. The manipulation of the argument uptoken leads to deserialization. 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. The vendor was contacted early about this disclosure but did not respond in any way.	5.0	More Details
CVE-2024-34882	Insufficiently protected credentials in SMTP server settings in 1C-Bitrix Bitrix24 23.300.100 allows remote administrators to send SMTP account passwords to an arbitrary server via HTTP POST request.	4.9	More Details
CVE-2024-34883	Insufficiently protected credentials in DAV server settings in 1C-Bitrix Bitrix24 23.300.100 allow remote administrators to read proxy-server accounts passwords via HTTP GET request.	4.9	More Details
CVE-2024-50335	SuiteCRM is an open-source, enterprise-ready Customer Relationship Management (CRM) software application. The "Publish Key" field in SuiteCRM's Edit Profile page is vulnerable to Reflected Cross-Site Scripting (XSS), allowing an attacker to inject malicious JavaScript code. This can be exploited to steal CSRF tokens and perform unauthorized actions, such as creating new administrative users without proper authentication. The vulnerability arises due to insufficient input validation and sanitization of the Publish Key field within the SuiteCRM application. When an attacker injects a malicious script, it gets executed within the context of an authenticated user's session. The injected script (o.js) then leverages the captured CSRF token to forge requests that create new administrative users, effectively compromising the integrity and security of the CRM instance. This issue has been addressed in versions 7.14.6 and 8.7.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.9	More Details
CVE-2023-5816	The Code Explorer plugin for WordPress is vulnerable to arbitrary external file reading in all versions up to, and including, 1.4.5. This is due to the fact that the plugin does not restrict accessing files to those outside of the WordPress instance, though the intention of the plugin is to only access WordPress related files. This makes it possible for authenticated attackers, with administrator-level access, to read files outside of the WordPress instance.	4.9	More Details
CVE-2024-34887	Insufficiently protected credentials in AD/LDAP server settings in 1C-Bitrix Bitrix24 23.300.100 allows remote administrators to send AD/LDAP administrators account passwords to an arbitrary server via HTTP POST request.	4.9	More Details
CVE-2024-51665	Server-Side Request Forgery (SSRF) vulnerability in Noor alam Magical Addons For Elementor allows Server Side Request Forgery.This issue affects Magical Addons For Elementor: from n/a through 1.2.1.	4.9	More Details
CVE-2024-10651	IDExpert from CHANGING Information Technology does not properly validate a specific parameter in the administrator interface, allowing remote attackers with administrator privileges to exploit this vulnerability to read arbitrary system files.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7877	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin WordPress plugin before 1.6.7.55 does not sanitise and escape some of its Notification settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2024-51432	Cross Site Scripting vulnerability in FiberHome HG6544C RP2743 allows an attacker to execute arbitrary code via the SSID field in the WIFI Clients List not being sanitized	4.8	More Details
CVE-2024-31975	EnGenius EWS356-Fit devices through 1.1.30 allow a remote attacker to conduct stored XSS attacks via the Wi-Fi SSID parameters. JavaScript embedded into a vulnerable field is executed when the user clicks the SSID field's corresponding EDIT button.	4.8	More Details
CVE-2024-7876	The Appointment Booking Calendar — Simply Schedule Appointments Booking Plugin WordPress plugin before 1.6.7.55 does not sanitise and escape some of its Appointment Type settings, which could allow high privilege users such as admin to perform Cross-Site Scripting attacks even when unfiltered_html is disallowed	4.8	More Details
CVE-2024-5578	The Table of Contents Plus WordPress plugin through 2408 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-2024-9883	The Pods WordPress plugin before 3.2.7.1 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-2024-30149	HCL AppScan Source <= 10.6.0 does not properly validate a TLS/SSL certificate for an executable.	4.8	More Details
CVE-2024-47255	In 2N Access Commander versions 3.1.1.2 and prior, a local attacker can escalate their privileges in the system which could allow for arbitrary code execution with root permissions.	4.7	More Details
CVE-2024-50135	In the Linux kernel, the following vulnerability has been resolved: nvme-pci: fix race condition between reset and nvme_dev_disable() nvme_dev_disable() modifies the dev->online_queues field, therefore nvme_pci_update_nr_queues() should avoid racing against it, otherwise we could end up passing invalid values to blk_mq_update_nr_hw_queues(). WARNING: CPU: 39 PID: 61303 at drivers/pci/msi/api.c:347 pci_irq_get_affinity+0x187/0x210 Workqueue: nvme-reset-wq nvme_reset_work [nvme] RIP: 0010:pci_irq_get_affinity+0x187/0x210 Call Trace: <TASK> ? blk_mq_pci_map_queues+0x87/0x3c0 ? pci_irq_get_affinity+0x187/0x210 blk_mq_pci_map_queues+0x87/0x3c0 nvme_pci_map_queues+0x189/0x460 [nvme] blk_mq_update_nr_hw_queues+0x2a/0x40 nvme_reset_work+0x1be/0x2a0 [nvme] Fix the bug by locking the shutdown_lock mutex before using dev->online_queues. Give up if nvme_dev_disable() is running or if it has been executed already.	4.7	More Details
CVE-2024-50344	I, Librarian is an open-source version of a PDF managing SaaS. Supplemental Files are allowed to be viewed in the browser, only if they have a white-listed MIME type. Unfortunately, this logic is broken, thus allowing unsafe files containing Javascript to be executed with the application context. An attacker can exploit this vulnerability by uploading a supplementary file that contains a malicious code or script. This code will then be executed when the file is loaded in the browser. The vulnerability was fixed in version 5.11.2.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27525	Cross Site Scripting vulnerability in Chamilo LMS v.1.11.26 allows a remote attacker to escalate privileges via a crafted script to the filename parameter of the home.php component.	4.6	More Details
CVE-2024-10523	This vulnerability exists in TP-Link IoT Smart Hub due to storage of Wi-Fi credentials in plain text within the device firmware. An attacker with physical access could exploit this by extracting the firmware and analyzing the binary data to obtain the Wi-Fi credentials stored on the vulnerable device.	4.6	More Details
CVE-2024-20112	In isp, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS09071481; Issue ID: MSV-1730.	4.4	More Details
CVE-2024-20124	In vdec, there is a possible out of bounds read due to improper structure design. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09008925; Issue ID: MSV-1568.	4.4	More Details
CVE-2024-20122	In vdec, there is a possible out of bounds read due to improper structure design. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09008925; Issue ID: MSV-1572.	4.4	More Details
CVE-2024-20117	In vdec, there is a possible out of bounds read due to improper structure design. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09008925; Issue ID: MSV-1681.	4.4	More Details
CVE-2024-20123	In vdec, there is a possible out of bounds read due to improper structure design. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09008925; Issue ID: MSV-1569.	4.4	More Details
CVE-2024-9878	The Photo Gallery by 10Web – Mobile-Friendly Image Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.8.30 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-37096	Missing Authorization vulnerability in Popup Box Team Popup allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Popup box: from n/a through 4.5.1.	4.3	More Details
CVE-2024-37440	Missing Authorization vulnerability in Andy Moyle Church Admin allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Church Admin: from n/a through 4.4.4.	4.3	More Details
CVE-2024-43297	Missing Authorization vulnerability in Migrate Clone allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Clone: from n/a through 2.4.5.	4.3	More Details
CVE-2024-43296	Missing Authorization vulnerability in bPlugins LLC Flash & HTML5 Video allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Flash & HTML5 Video: from n/a through 2.5.30.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43293	Missing Authorization vulnerability in WPZOOM Recipe Card Blocks for Gutenberg & Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Recipe Card Blocks for Gutenberg & Elementor: from n/a through 3.3.1.	4.3	More Details
CVE-2024-37204	Missing Authorization vulnerability in PropertyHive PropertyHive allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PropertyHive: from n/a through 2.0.9.	4.3	More Details
CVE-2024-9689	The Post From Frontend WordPress plugin through 1.0.0 does not have CSRF check when deleting posts, which could allow attackers to make logged in admin perform such action via a CSRF attack	4.3	More Details
CVE-2024-43254	Missing Authorization vulnerability in Zaytech Smart Online Order for Clover allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Smart Online Order for Clover: from n/a through 1.5.6.	4.3	More Details
CVE-2024-10329	The Ultimate Bootstrap Elements for Elementor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.6 via the 'ube_get_page_templates' function. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive data including the contents of templates that are private.	4.3	More Details
CVE-2024-43229	Missing Authorization vulnerability in Cornel Raiu WP Search Analytics allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Search Analytics: from n/a through 1.4.9.	4.3	More Details
CVE-2024-43302	Missing Authorization vulnerability in Fonts Plugin Fonts allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Fonts: from n/a through 3.7.7.	4.3	More Details
CVE-2024-43223	Missing Authorization vulnerability in EventPrime Events EventPrime allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects EventPrime: from n/a through 4.0.3.2.	4.3	More Details
CVE-2024-47362	Missing Authorization vulnerability in WPChill Strong Testimonials allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Strong Testimonials: from n/a through 3.1.16.	4.3	More Details
CVE-2024-43215	Missing Authorization vulnerability in creativemotion Social Slider Feed allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Social Slider Feed: from n/a through 2.2.2.	4.3	More Details
CVE-2024-38695	Missing Authorization vulnerability in Martin Gibson WP GoToWebinar allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP GoToWebinar: from n/a through 15.6.	4.3	More Details
CVE-2024-43162	Missing Authorization vulnerability in Easy Digital Downloads allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Easy Digital Downloads: from n/a through 3.2.12.	4.3	More Details
CVE-2024-48045	Missing Authorization vulnerability in Leevio Happy Addons for Elementor allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Happy Addons for Elementor: from n/a through 3.12.3.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44031	Missing Authorization vulnerability in BearDev JoomSport allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JoomSport: from n/a through 5.6.3.	4.3	More Details
CVE-2024-43298	Missing Authorization vulnerability in Migrate Clone allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Clone: from n/a through 2.4.5.	4.3	More Details
CVE-2024-43314	Missing Authorization vulnerability in Gabe Livan Asset CleanUp: Page Speed Booster allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Asset CleanUp: Page Speed Booster: from n/a through 1.3.9.3.	4.3	More Details
CVE-2024-43157	Missing Authorization vulnerability in nCrafts FormCraft allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects FormCraft: from n/a through 1.2.10.	4.3	More Details
CVE-2024-47318	Missing Authorization vulnerability in Magazine3 PWA for WP & AMP allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects PWA for WP & AMP: from n/a through 1.7.72.	4.3	More Details
CVE-2024-44006	Missing Authorization vulnerability in OnTheGoSystems WooCommerce Multilingual & Multicurrency multilingual allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WooCommerce Multilingual & Multicurrency: from n/a through 5.3.6.	4.3	More Details
CVE-2024-43981	Missing Authorization vulnerability in AyeCode – WP Business Directory Plugins GeoDirectory allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GeoDirectory: from n/a through 2.3.70.	4.3	More Details
CVE-2024-7429	The Zotpress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the Zotpress_process_accounts_AJAX function in all versions up to, and including, 7.3.12. This makes it possible for authenticated attackers, with Contributor-level access and above, to reset the plugin's settings.	4.3	More Details
CVE-2024-43973	Missing Authorization vulnerability in AyeCode Ltd GetPaid allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects GetPaid: from n/a through 2.8.11.	4.3	More Details
CVE-2024-43968	Broken Access Control vulnerability in Automattic Newspack allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Newspack: from n/a through 3.8.6.	4.3	More Details
CVE-2024-44020	Missing Authorization vulnerability in Prasad Kirpekar WP Free SSL – Free SSL Certificate for WordPress and force HTTPS allows . This issue affects WP Free SSL – Free SSL Certificate for WordPress and force HTTPS: from n/a through 1.2.6.	4.3	More Details
CVE-2024-43925	Missing Authorization vulnerability in Envira Gallery Team Envira Photo Gallery allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Envira Photo Gallery: from n/a through 1.8.14.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10319	The 140+ Widgets l Xpro Addons For Elementor – FREE plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.4.6 via the render function in widgets/content-toggle/layout/frontend.php. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft template data.	4.3	More Details
CVE-2024-51740	Combodo iTop is a simple, web based IT Service Management tool. This vulnerability can be used to create HTTP requests on behalf of the server, from a low privileged user. The user portal form manager has been fixed to only instantiate classes derived from it. This issue has been addressed in versions 2.7.11, 3.0.5, 3.1.2, and 3.2.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2024-37249	Missing Authorization vulnerability in WPEngine Inc. Advanced Custom Fields PRO allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Advanced Custom Fields PRO: from n/a through 6.3.1.	4.3	More Details
CVE-2024-31972	EnGenius ESR580 A8J-EMR5000 devices allow a remote attacker to conduct stored XSS attacks that could lead to arbitrary JavaScript code execution (under the context of the user's session) via the Wi-Fi SSID input fields. Web scripts embedded into the vulnerable fields this way are executed immediately when a user logs into the admin page. This affects /admin/wifi/wlan1 and /admin/wifi/wlan_guest.	4.3	More Details
CVE-2024-37254	Missing Authorization vulnerability in mndpsingh287 File Manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects File Manager: from n/a through 7.2.7.	4.3	More Details
CVE-2024-43355	Missing Authorization vulnerability in BearDev JoomSport allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects JoomSport: from n/a through 5.3.0.	4.3	More Details
CVE-2024-43343	Missing Authorization vulnerability in Etoile Web Design Order Tracking allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Order Tracking: from n/a through 3.3.12.	4.3	More Details
CVE-2024-37218	Missing Authorization vulnerability in WordPress Page Builder Sandwich Team Page Builder Sandwich – Front-End Page Builder allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Page Builder Sandwich – Front-End Page Builder: from n/a through 5.1.0.	4.3	More Details
CVE-2024-43332	Missing Authorization vulnerability in Jordy Meow Photo Engine allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Photo Engine: from n/a through 6.4.0.	4.3	More Details
CVE-2024-37443	Missing Authorization vulnerability in Automattic WP Job Manager - Resume Manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Job Manager - Resume Manager: from n/a through 2.1.0.	4.3	More Details
CVE-2024-43208	Missing Authorization vulnerability in Miller Media (Matt Miller) Send Emails with Mandrill allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Send Emails with Mandrill: from n/a through 1.4.1.	4.3	More Details
CVE-2024-43119	Missing Authorization vulnerability in Aruba.It Aruba HiSpeed Cache allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Aruba HiSpeed Cache: from n/a through 2.0.12.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37203	Missing Authorization vulnerability in Laybuy Laybuy Payment Extension for WooCommerce allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Laybuy Payment Extension for WooCommerce: from n/a through 5.3.9.	4.3	More Details
CVE-2024-37453	Missing Authorization vulnerability in ProfileGrid User Profiles ProfileGrid allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects ProfileGrid: from n/a through 5.8.7.	4.3	More Details
CVE-2024-37201	Missing Authorization vulnerability in javmah Woocommerce Customers Order History allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Woocommerce Customers Order History: from n/a through 5.2.2.	4.3	More Details
CVE-2024-10084	The Contact Form 7 – Dynamic Text Extension plugin for WordPress is vulnerable to Basic Information Disclosure in all versions up to, and including, 4.5 via the CF7_get_post_var shortcode. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract the titles and text contents of private and password-protected posts, they do not own.	4.3	More Details
CVE-2024-44052	Missing Authorization vulnerability in HelloAsso allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects HelloAsso: from n/a through 1.1.10.	4.3	More Details
CVE-2024-39639	Broken Access Control vulnerability in Nickolas Bossinas WordPress File Upload allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WordPress File Upload: from n/a through 4.24.7.	4.3	More Details
CVE-2024-48039	Missing Authorization vulnerability in CubeWP CubeWP – All-in-One Dynamic Content Framework allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects CubeWP – All-in-One Dynamic Content Framework: from n/a through 1.1.15.	4.3	More Details
CVE-2024-43930	Cross-Site Request Forgery (CSRF) vulnerability in eyecix JobSearch allows Cross Site Request Forgery.This issue affects JobSearch: from n/a through 2.5.3.	4.3	More Details
CVE-2024-43933	Cross-Site Request Forgery (CSRF) vulnerability in WPMobile.App allows Stored XSS.This issue affects WPMobile.App: from n/a through 11.48.	4.3	More Details
CVE-2024-37482	Missing Authorization vulnerability in Post Grid Team by RadiusTheme The Post Grid allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects The Post Grid: from n/a through 7.7.4.	4.3	More Details
CVE-2024-10605	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /file/request.php. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2024-37505	Missing Authorization vulnerability in Rara Themes Business One Page allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Business One Page: from n/a through 1.2.9.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51560	This vulnerability exists in the Wave 2.0 due to improper exception handling for invalid inputs at certain API endpoint. An authenticated remote attacker could exploit this vulnerability by providing invalid inputs for “userId” parameter in the API request leading to generation of error message containing sensitive information on the targeted system.	4.3	More Details
CVE-2024-37517	Missing Authorization vulnerability in Brainstorm Force Spectra allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Spectra: from n/a through 2.13.7.	4.3	More Details
CVE-2024-38727	Missing Authorization vulnerability in Seraphinite Solutions Seraphinite Post .DOCX Source allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Seraphinite Post .DOCX Source: from n/a through 2.16.9.	4.3	More Details
CVE-2024-38719	Missing Authorization vulnerability in Creative Motion Auto Featured Image (Auto Post Thumbnail) allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Auto Featured Image (Auto Post Thumbnail): from n/a through 4.1.2.	4.3	More Details
CVE-2024-38714	Missing Authorization vulnerability in Epsiloncool WP Fast Total Search allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects WP Fast Total Search: from n/a through 1.68.232.	4.3	More Details
CVE-2024-37095	Missing Authorization vulnerability in Envira Gallery Team Envira Photo Gallery allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Envira Photo Gallery: from n/a through 1.8.7.3.	4.3	More Details
CVE-2024-43154	Missing Authorization vulnerability in BracketSpace Advanced Cron Manager allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Advanced Cron Manager – debug & control: from n/a through 2.5.9.	4.3	More Details
CVE-2024-43118	Missing Authorization vulnerability in WPMU DEV Hummingbird allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Hummingbird: from n/a through 3.9.1.	4.3	More Details
CVE-2024-47317	Missing Authorization vulnerability in WP Quads Ads by WPQuads – Adsense Ads, Banner Ads, Popup Ads allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Ads by WPQuads – Adsense Ads, Banner Ads, Popup Ads: from n/a through 2.0.84.	4.3	More Details
CVE-2024-10399	The Download Monitor plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ajax_search_users function in all versions up to, and including, 5.0.13. This makes it possible for authenticated attackers, with Subscriber-level access and above, to obtain usernames and emails of site users.	4.3	More Details
CVE-2024-43142	Missing Authorization vulnerability in Themeum Tutor LMS allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Tutor LMS: from n/a through 2.7.3.	4.3	More Details
CVE-2024-10557	A vulnerability has been found in code-projects Blood Bank Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /file/updateprofile.php. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43136	Missing Authorization vulnerability in WP Sunshine Sunshine Photo Cart allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Sunshine Photo Cart: from n/a through 3.2.1.	4.3	More Details
CVE-2023-29116	Under certain conditions, through a request directed to the Waybox Enel X web management application, information like Waybox OS version or service configuration details could be obtained.	4.3	More Details
CVE-2024-43134	Missing Authorization vulnerability in xootix Waitlist Woocommerce (Back in stock notifier) allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Waitlist Woocommerce (Back in stock notifier): from n/a through 2.6.	4.3	More Details
CVE-2023-29126	The Waybox Enel X web management application contains a PHP-type juggling vulnerability that may allow a brute force process and under certain conditions bypass authentication.	4.2	More Details
CVE-2024-0134	NVIDIA Container Toolkit and NVIDIA GPU Operator for Linux contain a UNIX vulnerability where a specially crafted container image can lead to the creation of unauthorized files on the host. The name and location of the files cannot be controlled by an attacker. A successful exploit of this vulnerability might lead to data tampering.	4.1	More Details
CVE-2024-51528	Vulnerability of improper log printing in the Super Home Screen module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.0	More Details
CVE-2024-51524	Permission control vulnerability in the Wi-Fi module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	4.0	More Details
CVE-2024-7883	When using Arm Cortex-M Security Extensions (CMSE), Secure stack contents can be leaked to Non-secure state via floating-point registers when a Secure to Non-secure function call is made that returns a floating-point value and when this is the first use of floating-point since entering Secure state. This allows an attacker to read a limited quantity of Secure stack contents with an impact on confidentiality. This issue is specific to code generated using LLVM-based compilers.	3.7	More Details
CVE-2024-33623	A denial of service vulnerability exists in the Web Application functionality of LevelOne WBR-6012 R0.40e6. A specially crafted HTTP request can lead to a reboot. An attacker can send an HTTP request to trigger this vulnerability.	3.7	More Details
CVE-2024-10768	A vulnerability classified as problematic was found in PHPGurukul Online Shopping Portal 2.0. This vulnerability affects unknown code of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/two_tables.php. The manipulation of the argument scripts leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-10753	A vulnerability was found in PHPGurukul Online Shopping Portal 2.0. It has been declared as problematic. This vulnerability affects unknown code of the file admin/assets/plugins/DataTables/media/unit_testing/templates/dom_data_two_headers.php. The manipulation of the argument scripts leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10503	A vulnerability was found in Klokan MapTiler tileserver-gl 2.3.1 and classified as problematic. This issue affects some unknown processing of the component URL Handler. The manipulation of the argument key leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-10754	A vulnerability was found in PHPGurukul Online Shopping Portal 2.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/dymanic_table.php. The manipulation of the argument scripts leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-10746	A vulnerability classified as problematic has been found in PHPGurukul Online Shopping Portal 2.0. This affects an unknown part of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/dom_data.php. The manipulation of the argument scripts leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-10745	A vulnerability was found in PHPGurukul Online Shopping Portal 2.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/deferred_table.php. The manipulation of the argument scripts leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-10761	A vulnerability was found in Umbraco CMS 12.3.6. It has been classified as problematic. Affected is an unknown function of the file /Umbraco/preview/frame?id{} of the component Dashboard. The manipulation of the argument culture 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 real existence of this vulnerability is still doubted at the moment. The vendor is not able to reproduce the issue.	3.5	More Details
CVE-2024-10744	A vulnerability was found in PHPGurukul Online Shopping Portal 2.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/complex_header_2.php. The manipulation of the argument scripts 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-2024-10743	A vulnerability was found in PHPGurukul Online Shopping Portal 2.0. It has been classified as problematic. Affected is an unknown function of the file /shopping/admin/assets/plugins/DataTables/examples/examples_support/editable_ajax.php. The manipulation of the argument value 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.	3.5	More Details
CVE-2024-10701	A vulnerability was found in PHPGurukul Car Rental Portal 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /search.php. The manipulation of the argument searchdata leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-10757	A vulnerability, which was classified as problematic, has been found in PHPGurukul Online Shopping Portal 2.0. Affected by this issue is some unknown functionality of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/js_data.php. The manipulation of the argument scripts leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10756	A vulnerability classified as problematic was found in PHPGurukul Online Shopping Portal 2.0. Affected by this vulnerability is an unknown functionality of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/html_table.php. The manipulation of the argument scripts 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-2024-10755	A vulnerability classified as problematic has been found in PHPGurukul Online Shopping Portal 2.0. Affected is an unknown function of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/empty_table.php. The manipulation of the argument scripts 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.	3.5	More Details
CVE-2024-10747	A vulnerability classified as problematic was found in PHPGurukul Online Shopping Portal 2.0. This vulnerability affects unknown code of the file /admin/assets/plugins/DataTables/media/unit_testing/templates/dom_data_th.php. The manipulation of the argument scripts leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-50092	In the Linux kernel, the following vulnerability has been resolved: net: netconsole: fix wrong warning A warning is triggered when there is insufficient space in the buffer for userdata. However, this is not an issue since userdata will be sent in the next iteration. Current warning message: ------------[cut here]------------ WARNING: CPU: 13 PID: 3013042 at drivers/net/netconsole.c:1122 write_ext_msg+0x3b6/0x3d0 ? write_ext_msg+0x3b6/0x3d0 console_flush_all+0x1e9/0x330 The code incorrectly issues a warning when this_chunk is zero, which is a valid scenario. The warning should only be triggered when this_chunk is negative.	3.3	More Details
CVE-2024-47402	in OpenHarmony v4.0.0 and prior versions allow a local attacker cause DOS through out-of-bounds read.	3.3	More Details
CVE-2024-51744	golang-jwt is a Go implementation of JSON Web Tokens. Unclear documentation of the error behavior in `ParseWithClaims` can lead to situation where users are potentially not checking errors in the way they should be. Especially, if a token is both expired and invalid, the errors returned by `ParseWithClaims` return both error codes. If users only check for the `jwt.ErrTokenExpired ` using `error.Is`, they will ignore the embedded `jwt.ErrTokenSignatureInvalid` and thus potentially accept invalid tokens. A fix has been back-ported with the error handling logic from the `v5` branch to the `v4` branch. In this logic, the `ParseWithClaims` function will immediately return in "dangerous" situations (e.g., an invalid signature), limiting the combined errors only to situations where the signature is valid, but further validation failed (e.g., if the signature is valid, but is expired AND has the wrong audience). This fix is part of the 4.5.1 release. We are aware that this changes the behaviour of an established function and is not 100 % backwards compatible, so updating to 4.5.1 might break your code. In case you cannot update to 4.5.0, please make sure that you are properly checking for all errors ("dangerous" ones first), so that you are not running in the case detailed above.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-10748	A vulnerability, which was classified as problematic, has been found in Cosmote Greece What's Up App 4.47.3 on Android. This issue affects some unknown processing of the file gr/desquared/kmmsharedmodule/db/RealmDB.java of the component Realm Database Handler. The manipulation of the argument defaultRealmKey leads to use of default cryptographic key. Local access is required to approach this attack. The complexity of an attack is rather high. The exploitation is known to be difficult. The vendor was contacted early about this disclosure but did not respond in any way.	2.5	More Details
CVE-2024-10807	A vulnerability was found in PHPGurukul Hospital Management System 4.0. It has been rated as problematic. This issue affects some unknown processing of the file hms/doctor/search.php. The manipulation of the argument searchdata leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2024-10840	A vulnerability classified as problematic has been found in romadebrian WEB-Sekolah 1.0. Affected is an unknown function of the file /Admin/akun_edit.php of the component Backend. The manipulation of the argument kode leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2024-10806	A vulnerability was found in PHPGurukul Hospital Management System 4.0. It has been declared as problematic. This vulnerability affects unknown code of the file betweendates-detailsreports.php. The manipulation of the argument fromdate/todate leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2024-10842	A vulnerability, which was classified as problematic, has been found in romadebrian WEB-Sekolah 1.0. Affected by this issue is some unknown functionality of the file /Admin/Proses_Edit_Akun.php of the component Backend. The manipulation of the argument Username_Baru/Password leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2024-51734	Zope AccessControl provides a general security framework for use in Zope. In affected versions anonymous users can delete the user data maintained by an `AccessControl.userfolder.UserFolder` which may prevent any privileged access. This problem has been fixed in version 7.2. Users are advised to upgrade. Users unable to upgrade may address the issue by adding `data__roles__ = ()` to `AccessControl.userfolder.UserFolder`.	0.0	More Details
CVE-2024-50356	Press, a Frappe custom app that runs Frappe Cloud, manages infrastructure, subscription, marketplace, and software-as-a-service (SaaS). The password could be reset by anyone who have access to the mail inbox circumventing the 2FA. Even though they wouldn't be able to login by bypassing the 2FA. Only users who have enabled 2FA are affected. Commit ba0007c28ac814260f836849bc07d29beea7deb6 patches this bug.	0.0	More Details
CVE-2024-51752	The AuthKit library for Next.js provides convenient helpers for authentication and session management using WorkOS & AuthKit with Next.js. In affected versions refresh tokens are logged to the console when the disabled by default `debug` flag, is enabled. This issue has been patched in version 0.13.2 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51498	cobalt is a media downloader that doesn't piss you off. A malicious cobalt instance could serve links with the `javascript:` protocol, resulting in Cross-site Scripting (XSS) when the user tries to download an item from a picker. This issue has been present since commit `66bac03e`, was mitigated in commit `97977efa` (correctly configured web instances were no longer vulnerable) and fully fixed in commit `c4be1d3a` (included in release version 10.2.1). Users are advised to upgrade. Users unable to upgrade should enable a content-security-policy.	N/A	More Details
CVE-2024-47939	Stack-based buffer overflow vulnerability exists in multiple Ricoh laser printers and MFPs which implement Web Image Monitor. If this vulnerability is exploited, receiving a specially crafted request created and sent by an attacker may lead to arbitrary code execution and/or a denial-of-service (DoS) condition. As for the details of affected product names and versions, refer to the information provided by the vendor under [References].	N/A	More Details
CVE-2024-49501	Sysmac Studio provided by OMRON Corporation contains an incorrect authorization vulnerability. If this vulnerability is exploited, an attacker may access the program which is protected by Data Protection function.	N/A	More Details
CVE-2024-51756	The cap-std project is organized around the eponymous `cap-std` crate, and develops libraries to make it easy to write capability-based code. cap-std's filesystem sandbox implementation on Windows blocks access to special device filenames such as "COM1", "COM2", "LPT0", "LPT1", and so on, however it did not block access to the special device filenames which use superscript digits, such as "COM¹", "COM²", "LPT⁰", "LPT¹", and so on. Untrusted filesystem paths could bypass the sandbox and access devices through those special device filenames with superscript digits, and through them provide access peripheral devices connected to the computer, or network resources mapped to those devices. This can include modems, printers, network printers, and any other device connected to a serial or parallel port, including emulated USB serial ports. The bug is fixed in #371, which is published in cap-primitives 3.4.1, cap-std 3.4.1, and cap-async-std 3.4.1. There are no known workarounds for this issue. Affected Windows users are recommended to upgrade.	N/A	More Details
CVE-2024-51745	Wasmtime is a fast and secure runtime for WebAssembly. Wasmtime's filesystem sandbox implementation on Windows blocks access to special device filenames such as "COM1", "COM2", "LPT0", "LPT1", and so on, however it did not block access to the special device filenames which use superscript digits, such as "COM¹", "COM²", "LPT⁰", "LPT¹", and so on. Untrusted Wasm programs that are given access to any filesystem directory could bypass the sandbox and access devices through those special device filenames with superscript digits, and through them gain access peripheral devices connected to the computer, or network resources mapped to those devices. This can include modems, printers, network printers, and any other device connected to a serial or parallel port, including emulated USB serial ports. Patch releases for Wasmtime have been issued as 24.0.2, 25.0.3, and 26.0.1. Users of Wasmtime 23.0.x and prior are recommended to upgrade to one of these patched versions. There are no known workarounds for this issue. Affected Windows users are recommended to upgrade.	N/A	More Details
CVE-2024-51502	loona is an experimental, HTTP/1.1 and HTTP/2 implementation in Rust on top of io-uring. `loona-hpack` suffers from the same vulnerability as the original `hpack` as documented in issue #11. All users who try to decode untrusted input using the Decoder are vulnerable to this exploit. This issue has been addressed in release version 0.4.3. All users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51501	Refit is an automatic type-safe REST library for .NET Core, Xamarin and .NET The various header-related Refit attributes (Header, HeaderCollection and Authorize) are vulnerable to CRLF injection. The way HTTP headers are added to a request is via the `HttpHeaders.TryAddWithoutValidation` method. This method does not check for CRLF characters in the header value. This means that any headers added to a refit request are vulnerable to CRLF-injection. In general, CRLF-injection into a HTTP header (when using HTTP/1.1) means that one can inject additional HTTP headers or smuggle whole HTTP requests. If an application using the Refit library passes a user-controllable value through to a header, then that application becomes vulnerable to CRLF-injection. This is not necessarily a security issue for a command line application like the one above, but if such code were present in a web application then it becomes vulnerable to request splitting (as shown in the PoC) and thus Server Side Request Forgery. Strictly speaking this is a potential vulnerability in applications using Refit and not in Refit itself. This issue has been addressed in release versions 7.2.22 and 8.0.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2024-51753	The AuthKit library for Remix provides convenient helpers for authentication and session management using WorkOS & AuthKit with Remix. In affected versions refresh tokens are logged to the console when the disabled by default `debug` flag, is enabled. This issue has been patched in version 0.4.1. All users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2024-49770	`oak` is a middleware framework for Deno's native HTTP server, Deno Deploy, Node.js 16.5 and later, Cloudflare Workers and Bun. By default `oak` does not allow transferring of hidden files with `Context.send` API. However, prior to version 17.1.3, this can be bypassed by encoding `/` as its URL encoded form `%2F`. For an attacker this has potential to read sensitive user data or to gain access to server secrets. Version 17.1.3 fixes the issue.	N/A	More Details
CVE-2024-51746	Gitsign is a keyless Sigstore to signing tool for Git commits with your a GitHub / OIDC identity. gitsign may select the wrong Rekor entry to use during online verification when multiple entries are returned by the log. gitsign uses Rekor's search API to fetch entries that apply to a signature being verified. The parameters used for the search are the public key and the payload. The search API returns entries that match either condition rather than both. When gitsign's credential cache is used, there can be multiple entries that use the same ephemeral keypair / signing certificate. As gitsign assumes both conditions are matched by Rekor, there is no additional validation that the entry's hash matches the payload being verified, meaning that the wrong entry can be used to successfully pass verification. Impact is minimal as while gitsign does not match the payload against the entry, it does ensure that the certificate matches. This would need to be exploited during the certificate validity window (10 minutes) by the key holder.	N/A	More Details
CVE-2024-51483	changedetection.io is free, open source web page change detection software. Prior to version 0.47.5, when a WebDriver is used to fetch files, `source:file:///etc/passwd` can be used to retrieve local system files, where the more traditional `file:///etc/passwd` gets blocked. Version 0.47.5 fixes the issue.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-51735	Osmedeus is a Workflow Engine for Offensive Security. Cross-site Scripting (XSS) occurs on the Osmedues web server when viewing results from the workflow, allowing commands to be executed on the server. When using a workflow that contains the summary module, it generates reports in HTML and Markdown formats. The default report is based on the `general-template.md` template.The contents of the files are read and used to generate the report. However, the file contents are not properly filtered, leading to XSS. This may lead to commands executed on the host as well. This issue is not yet resolved. Users are advised to add their own filtering or to reach out to the developer to aid in developing a patch.	N/A	More Details
CVE-2024-50347	Laravel Reverb provides a real-time WebSocket communication backend for Laravel applications. Prior to 1.4.0, there is an issue where verification signatures for requests sent to Reverb's Pusher-compatible API were not being verified. This API is used in scenarios such as broadcasting a message from a backend service or for obtaining statistical information (such as number of connections) about a given channel. This issue only affects the Pusher-compatible API endpoints and not the WebSocket connections themselves. In order to exploit this vulnerability, the application ID which, should never be exposed, would need to be known by an attacker. This vulnerability is fixed in 1.4.0.	N/A	More Details
CVE-2024-51481	Nix is a package manager for Linux and other Unix systems. On macOS, built-in builders (such as `builtin:fetchurl`, exposed to users with `import <nix/fetchurl.nix>`) were not executed in the macOS sandbox. Thus, these builders (which are running under the `nixbld*` users) had read access to world-readable paths and write access to world-writable paths outside of the sandbox. This issue is fixed in 2.18.9, 2.19.7, 2.20.9, 2.21.5, 2.22.4, 2.23.4, and 2.24.10. Note that sandboxing is not enabled by default on macOS. The Nix sandbox is not primarily intended as a security mechanism, but as an aid to improve reproducibility and purity of Nix builds. However, sandboxing *can* mitigate the impact of other security issues by limiting what parts of the host system a build has access to.	N/A	More Details
CVE-2024-10389	There exists a Path Traversal vulnerability in Safearchive on Platforms with Case-Insensitive Filesystems (e.g., NTFS). This allows Attackers to Write Arbitrary Files via Archive Extraction containing symbolic links. We recommend upgrading past commit f7ce9d7b6f9c6ecd72d0b0f16216b046e55e44dc	N/A	More Details
CVE-2024-48342	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-2024-50089	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-20111	In ccu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS09065033; Issue ID: MSV-1754.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-50346	WebFeed is a lightweight web feed reader extension for Firefox/Chrome. Multiple HTML injection vulnerabilities in WebFeed can lead to CSRF and UI spoofing attacks. A remote attacker can provide malicious RSS feeds and attract the victim user to visit it using WebFeed. The attacker can then inject malicious HTML into the extension page and fool the victim into sending out HTTP requests to arbitrary sites with the victim's credentials. Users are vulnerable to CSRF attacks when visiting malicious RSS feeds via WebFeed. Unwanted actions could be executed on the user's behalf on arbitrary websites. This issue has been addressed in release version 0.9.2. All users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details