SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 20 March 2024

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-28354	There is a command injection vulnerability in the TRENDnet TEW-827DRU router with firmware version 2.10B01. An attacker can inject commands into the post request parameters usapps.@smb[%d].username in the apply.cgi interface, thereby gaining root shell privileges.	10.0	More Details
CVE-2024-24578	RaspberryMatic is an open-source operating system for HomeMatic internet-of-things devices. RaspberryMatic / OCCU prior to version 3.75.6.20240316 contains a unauthenticated remote code execution (RCE) vulnerability, caused by multiple issues within the Java based `HMIPServer.jar` component. RaspberryMatric includes a Java based `HMIPServer`, that can be accessed through URLs starting with `/pages/jpages`. The `FirmwareController` class does however not perform any session id checks, thus this feature can be accessed without a valid session. Due to this issue, attackers can gain remote code execution as root user, allowing a full system compromise. Version 3.75.6.20240316 contains a patch.	10.0	More Details
CVE-2024-27957	Unrestricted Upload of File with Dangerous Type vulnerability in Pie Register.This issue affects Pie Register: from n/a through 3.8.3.1.	10.0	More Details
CVE-2024-25139	In TP-Link Omada er605 1.0.1 through (v2.6) 2.2.3, a cloud-brd binary is susceptible to an integer overflow that leads to a heap-based buffer overflow. After heap shaping, an attacker can achieve code execution in the context of the cloud-brd binary that runs at the root level. This is fixed in ER605(UN)_v2_2.2.4 Build 020240119.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27767	CWE-287: Improper Authentication may allow Authentication Bypass	10.0	More Details
CVE-2024-27102	Wings is the server control plane for Pterodactyl Panel. This vulnerability impacts anyone running the affected versions of Wings. The vulnerability can potentially be used to access files and directories on the host system. The full scope of impact is exactly unknown, but reading files outside of a server's base directory (sandbox root) is possible. In order to use this exploit, an attacker must have an existing "server" allocated and controlled by Wings. Details on the exploitation of this vulnerability are embargoed until March 27th, 2024 at 18:00 UTC. In order to mitigate this vulnerability, a full rewrite of the entire server filesystem was necessary. Because of this, the size of the patch is massive, however effort was made to reduce the amount of breaking changes. Users are advised to update to version 1.11.9. There are no known workarounds for this vulnerability.	9.9	More Details
CVE-2024-2599	File upload restriction evasion vulnerability in AMSS++ version 4.31. This vulnerability could allow an authenticated user to potentially obtain RCE through webshell, compromising the entire infrastructure.	9.9	More Details
CVE-2024-29135	Unrestricted Upload of File with Dangerous Type vulnerability in Tourfic.This issue affects Tourfic: from n/a through 2.11.15.	9.9	More Details
CVE-2023-6825	The File Manager and File Manager Pro plugins for WordPress are vulnerable to Directory Traversal in versions up to, and including version 7.2.1 (free version) and 8.3.4 (Pro version) via the target parameter in the mk_file_folder_manager_action_callback_shortcode function. This makes it possible for attackers to read the contents of arbitrary files on the server, which can contain sensitive information and to upload files into directories other than the intended directory for file uploads. The free version requires Administrator access for this vulnerability to be exploitable. The Pro version allows a file manager to be embedded via a shortcode and also allows admins to grant file handling privileges to other user levels, which could lead to this vulnerability being exploited by lower-level users.	9.9	More Details
CVE-2024-2615	Memory safety bugs present in Firefox 123. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 124.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28255	OpenMetadata is a unified platform for discovery, observability, and governance powered by a central metadata repository, in-depth lineage, and seamless team collaboration. The `JwtFilter` handles the API authentication by requiring and verifying JWT tokens. When a new request comes in, the request's path is checked against this list. When the request's path contains any of the excluded endpoints the filter returns without validating the JWT. Unfortunately, an attacker may use Path Parameters to make any path contain any arbitrary strings. For example, a request to `GET /api/v1;v1%2fusers%2flogin/events/subscriptions/validation/condition/111` will match the excluded endpoint condition and therefore will be processed with no JWT validation allowing an attacker to bypass the authentication mechanism and reach any arbitrary endpoint, including the ones listed above that lead to arbitrary SpEL expression injection. This bypass will not work when the endpoint uses the `SecurityContext.getUserPrincipal()` since it will return `null` and will throw an NPE. This issue may lead to authentication bypass and has been addressed in version 1.2.4. Users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as `GHSL-2023-237`.	9.8	More Details
CVE-2024-28639	Buffer Overflow vulnerability in TOTOLink X5000R V9.1.0u.6118-B20201102 and A7000R V9.1.0u.6115-B20201022, allow remote attackers to execute arbitrary code and cause a denial of service (DoS) via the IP field.	9.8	More Details
CVE-2022-47036	Siklu TG Terragraph devices before approximately 2.1.1 have a hardcoded root password that has been revealed via a brute force attack on an MD5 hash. It can be used for "debug login" by an admin. NOTE: the vulnerability is not fixed by the 2.1.1 firmware; instead, it is fixed in newer hardware, which would typically be used with firmware 2.1.1 or later.	9.8	More Details
CVE-2018-25099	In the CryptX module before 0.062 for Perl, gcm_decrypt_verify() and chacha20poly1305_decrypt_verify() do not verify the tag.	9.8	More Details
CVE-2021-47157	The Kossy module before 0.60 for Perl allows JSON hijacking because of X-Requested-With mishandling.	9.8	More Details
CVE-2024-28125	FitNesse all releases allows a remote authenticated attacker to execute arbitrary OS commands. Note: A contributor of FitNesse has claimed that this is not a vulnerability but a product specification and this is currently under further investigation.	9.8	More Details
CVE-2024-28595	SQL Injection vulnerability in Employee Management System v1.0 allows attackers to run arbitrary SQL commands via the admin_id parameter in update-admin.php.	9.8	More Details
CVE-2024-28394	An issue in Advanced Plugins reportsstatistics v1.3.20 and before allows a remote attacker to execute arbitrary code via the Sales Reports, Statistics, Custom Fields & Export module.	9.8	More Details
CVE-2024-27768	Unitronics Unistream Unilogic – Versions prior to 1.35.227 - CWE-22: 'Path Traversal' may allow RCE	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28537	Tenda AC18 V15.03.05.05 has a stack overflow vulnerability in the page parameter of fromNatStaticSetting function.	9.8	More Details
CVE-2024-25153	A directory traversal within the ‘ftpservlet’ of the FileCatalyst Workflow Web Portal allows files to be uploaded outside of the intended ‘uploadtemp’ directory with a specially crafted POST request. In situations where a file is successfully uploaded to web portal’s DocumentRoot, specially crafted JSP files could be used to execute code, including web shells.	9.8	More Details
CVE-2024-2051	CWE-307: Improper Restriction of Excessive Authentication Attempts vulnerability exists that could cause account takeover and unauthorized access to the system when an attacker conducts brute-force attacks against the login form.	9.8	More Details
CVE-2024-21652	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Prior to versions 2.8.13, 2.9.9, and 2.10.4, an attacker can exploit a chain of vulnerabilities, including a Denial of Service (DoS) flaw and in-memory data storage weakness, to effectively bypass the application's brute force login protection. This is a critical security vulnerability that allows attackers to bypass the brute force login protection mechanism. Not only can they crash the service affecting all users, but they can also make unlimited login attempts, increasing the risk of account compromise. Versions 2.8.13, 2.9.9, and 2.10.4 contain a patch for this issue.	9.8	More Details
CVE-2024-28303	Open Source Medicine Ordering System v1.0 was discovered to contain a SQL injection vulnerability via the date parameter at /admin/reports/index.php.	9.8	More Details
CVE-2024-2413	Intumit SmartRobot uses a fixed encryption key for authentication. Remote attackers can use this key to encrypt a string composed of the user's name and timestamp to generate an authentication code. With this authentication code, they can obtain administrator privileges and subsequently execute arbitrary code on the remote server using built-in system functionality.	9.8	More Details
CVE-2023-7017	Sciener locks' firmware update mechanism do not authenticate or validate firmware updates if passed to the lock through the Bluetooth Low Energy service. A challenge request can be sent to the lock with a command to prepare for an update, rather than an unlock request, allowing an attacker to compromise the device.	9.8	More Details
CVE-2024-28390	An issue in Advanced Plugins ultimateimagetool module for PrestaShop before v.2.2.01, allows a remote attacker to escalate privileges and obtain sensitive information via Improper Access Control.	9.8	More Details
CVE-2024-28423	Airflow-Diagrams v2.1.0 was discovered to contain an arbitrary file upload vulnerability in the unsafe_load function at cli.py. This vulnerability allows attackers to execute arbitrary code via uploading a crafted YML file.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1071	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to SQL Injection via the 'sorting' parameter in versions 2.1.3 to 2.8.2 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-2024-2172	The Malware Scanner plugin and the Web Application Firewall plugin for WordPress (both by MiniOrange) are vulnerable to privilege escalation due to a missing capability check on the mo_wpns_init() function in all versions up to, and including, 4.7.2 (for Malware Scanner) and 2.1.1 (for Web Application Firewall). This makes it possible for unauthenticated attackers to escalate their privileges to that of an administrator.	9.8	More Details
CVE-2024-0799	An authentication bypass vulnerability exists in Arcserve Unified Data Protection 9.2 and 8.1 in the edge-app-base-webui.jar!com.ca.arcserve.edge.app.base.ui.server.EdgeLoginServiceImpl.doLogin() function within wizardLogin.	9.8	More Details
CVE-2023-41505	An arbitrary file upload vulnerability in the Add Student's Profile Picture function of Student Enrollment In PHP v1.0 allows attackers to execute arbitrary code via uploading a crafted PHP file.	9.8	More Details
CVE-2024-25250	SQL Injection vulnerability in code-projects Agro-School Management System 1.0 allows attackers to run arbitrary code via the Login page.	9.8	More Details
CVE-2024-25652	In Delinea PAM Secret Server 11.4, it is possible for a user (with access to the Report functionality) to gain unauthorized access to remote sessions created by legitimate users.	9.8	More Details
CVE-2024-28388	SQL injection vulnerability in SunnyToo stproductcomments module for PrestaShop v.1.0.5 and before, allows a remote attacker to escalate privileges and obtain sensitive information via the StProductCommentClass::getListcomments method.	9.8	More Details
CVE-2024-28391	SQL injection vulnerability in FME Modules quickproducttable module for PrestaShop v.1.2.1 and before, allows a remote attacker to escalate privileges and obtain information via the readCsv(), displayAjaxProductChangeAttr, displayAjaxProductAddToCart, getSearchProducts, and displayAjaxProductSku methods.	9.8	More Details
CVE-2024-28383	Tenda AX12 v1.0 v22.03.01.16 was discovered to contain a stack overflow via the ssid parameter in the sub_431CF0 function.	9.8	More Details
CVE-2024-28389	SQL injection vulnerability in KnowBand spinwheel v.3.0.3 and before allows a remote attacker to gain escalated privileges and obtain sensitive information via the SpinWheelFrameSpinWheelModuleFrontController::sendEmail() method.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1915	Incorrect Pointer Scaling vulnerability in Mitsubishi Electric Corporation MELSEC-Q Series and MELSEC-L Series CPU modules allows a remote unauthenticated attacker to execute malicious code on a target product by sending a specially crafted packet.	9.8	More Details
CVE-2024-0802	Incorrect Pointer Scaling vulnerability in Mitsubishi Electric Corporation MELSEC-Q Series and MELSEC-L Series CPU modules allows a remote unauthenticated attacker to read arbitrary information from a target product or execute malicious code on a target product by sending a specially crafted packet.	9.8	More Details
CVE-2024-1917	Integer Overflow or Wraparound vulnerability in Mitsubishi Electric Corporation MELSEC-Q Series and MELSEC-L Series CPU modules allows a remote unauthenticated attacker to execute malicious code on a target product by sending a specially crafted packet.	9.8	More Details
CVE-2024-0803	Integer Overflow or Wraparound vulnerability in Mitsubishi Electric Corporation MELSEC-Q Series and MELSEC-L Series CPU modules allows a remote unauthenticated attacker to execute malicious code on a target product by sending a specially crafted packet.	9.8	More Details
CVE-2024-1916	Integer Overflow or Wraparound vulnerability in Mitsubishi Electric Corporation MELSEC-Q Series and MELSEC-L Series CPU modules allows a remote unauthenticated attacker to execute malicious code on a target product by sending a specially crafted packet.	9.8	More Details
CVE-2024-28253	OpenMetadata is a unified platform for discovery, observability, and governance powered by a central metadata repository, in-depth lineage, and seamless team collaboration. `CompiledRule::validateExpression` is also called from `PolicyRepository.prepare`. `prepare()` is called from `EntityRepository.prepareInternal()` which, in turn, gets called from `EntityResource.createOrUpdate()`. Note that even though there is an authorization check (`authorizer.authorize()`), it gets called after `prepareInternal()` gets called and therefore after the SpEL expression has been evaluated. In order to reach this method, an attacker can send a PUT request to `/api/v1/policies` which gets handled by `PolicyResource.createOrUpdate()`. This vulnerability was discovered with the help of CodeQL's Expression language injection (Spring) query and is also tracked as `GHSL-2023-252`. This issue may lead to Remote Code Execution and has been addressed in version 1.3.1. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.4	More Details
CVE-2024-28752	A SSRF vulnerability using the Aegis DataBinding in versions of Apache CXF before 4.0.4, 3.6.3 and 3.5.8 allows an attacker to perform SSRF style attacks on webservices that take at least one parameter of any type. Users of other data bindings (including the default databinding) are not impacted.	9.3	More Details
CVE-2024-29151	Rocket.Chat.Audit through 5ad78e8 depends on filecachetools, which does not exist in PyPI.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28194	your_spotify is an open source, self hosted Spotify tracking dashboard. YourSpotify versions < 1.8.0 use a hardcoded JSON Web Token (JWT) secret to sign authentication tokens. Attackers can use this well-known value to forge valid authentication tokens for arbitrary users. This vulnerability allows attackers to bypass authentication and authenticate as arbitrary YourSpotify users, including admin users. This issue has been addressed in version 1.8.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.1	More Details
CVE-2023-40276	An issue was discovered in OpenClinic GA 5.247.01. An Unauthenticated File Download vulnerability has been discovered in pharmacy/exportFile.jsp.	9.1	More Details
CVE-2024-26503	Unrestricted File Upload vulnerability in Greek Universities Network Open eClass v.3.15 and earlier allows attackers to run arbitrary code via upload of crafted file to certbadge.php endpoint.	9.1	More Details
CVE-2023-40275	An issue was discovered in OpenClinic GA 5.247.01. It allows retrieval of patient lists via queries such as findFirstname= to _common/search/searchByAjax/patientslistShow.jsp.	9.1	More Details
CVE-2021-47155	The Net::IPV4Addr module 0.10 for Perl does not properly consider extraneous zero characters in an IP address string, which (in some situations) allows attackers to bypass access control that is based on IP addresses.	9.1	More Details
CVE-2023-7006	The unlockKey character in a lock using Sciener firmware can be brute forced through repeated challenge requests, compromising the locks integrity.	9.1	More Details
CVE-2024-2636	An Unrestricted Upload of File vulnerability has been found on Cegid Meta4 HR, that allows an attacker to upload malicios files to the server via '/config/espanol/update_password.jsp' file. Modifying the 'M4_NEW_PASSWORD' parameter, an attacker could store a malicious JSP file inside the file directory, to be executed the the file is loaded in the application.	9.0	More Details
CVE-2024-29027	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Prior to versions 6.5.5 and 7.0.0-alpha.29, calling an invalid Parse Server Cloud Function name or Cloud Job name crashes the server and may allow for code injection, internal store manipulation or remote code execution. The patch in versions 6.5.5 and 7.0.0-alpha.29 added string sanitation for Cloud Function name and Cloud Job name. As a workaround, sanitize the Cloud Function name and Cloud Job name before it reaches Parse Server.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28175	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Due to the improper URL protocols filtering of links specified in the `link.argocd.argoproj.io` annotations in the application summary component, an attacker can achieve cross-site scripting with elevated permissions. All unpatched versions of Argo CD starting with v1.0.0 are vulnerable to a cross-site scripting (XSS) bug allowing a malicious user to inject a javascript: link in the UI. When clicked by a victim user, the script will execute with the victim's permissions (up to and including admin). This vulnerability allows an attacker to perform arbitrary actions on behalf of the victim via the API, such as creating, modifying, and deleting Kubernetes resources. A patch for this vulnerability has been released in Argo CD versions v2.10.3 v2.9.8, and v2.8.12. There are no completely-safe workarounds besides upgrading. The safest alternative, if upgrading is not possible, would be to create a Kubernetes admission controller to reject any resources with an annotation starting with link.argocd.argoproj.io or reject the resource if the value use an improper URL protocol. This validation will need to be applied in all clusters managed by ArgoCD.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-28673	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /dede/mychannel_edit.php.	8.8	More Details
CVE-2024-28671	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /dede/stepselect_main.php.	8.8	More Details
CVE-2024-28675	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /dede/diy_edit.php	8.8	More Details
CVE-2024-28684	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via the component /dede/module_main.php	8.8	More Details
CVE-2024-2247	JFrog Artifactory versions below 7.77.7, 7.82.1, are vulnerable to DOM-based cross-site scripting due to improper handling of the import override mechanism.	8.8	More Details
CVE-2024-28353	There is a command injection vulnerability in the TRENDnet TEW-827DRU router with firmware version 2.10B01. An attacker can inject commands into the post request parameters usapps.config.smb_admin_name in the apply.cgi interface, thereby gaining root shell privileges.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2486	A vulnerability was found in Tenda AC18 15.03.05.05. It has been classified as critical. This affects the function formQuickIndex of the file /goform/QuickIndex. The manipulation of the argument PPPOEPassword leads to stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256893 was assigned to this vulnerability.	8.8	More Details
CVE-2024-2487	A vulnerability was found in Tenda AC18 15.03.05.05. It has been declared as critical. This vulnerability affects the function formSetDeviceName of the file /goform/SetOnlineDevName. The manipulation of the argument devName/mac leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-256894 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2023-5663	The News Announcement Scroll plugin for WordPress is vulnerable to SQL Injection via the plugin's shortcode in versions up to, and including, 9.0.0 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with contributor-level and above permissions to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2024-2488	A vulnerability was found in Tenda AC18 15.03.05.05. It has been rated as critical. This issue affects the function formSetPPTPServer of the file /goform/SetPptpServerCfg. The manipulation of the argument startIP leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256895. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-1685	The Social Media Share Buttons plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 2.1.0 via deserialization of untrusted input through the attachmentUrl parameter. This makes it possible for authenticated attackers, with subscriber-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details
CVE-2024-2489	A vulnerability classified as critical has been found in Tenda AC18 15.03.05.05. Affected is the function formSetQosBand of the file /goform/SetNetControlList. The manipulation of the argument list leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256896. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2450	Mattermost versions 8.1.x before 8.1.10, 9.2.x before 9.2.6, 9.3.x before 9.3.2, and 9.4.x before 9.4.3 fail to correctly verify account ownership when switching from email to SAML authentication, allowing an authenticated attacker to take over other user accounts via a crafted switch request under specific conditions.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2490	A vulnerability classified as critical was found in Tenda AC18 15.03.05.05. Affected by this vulnerability is the function setSchedWifi of the file /goform/openSchedWifi. The manipulation of the argument schedStartTime/schedEndTime leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256897 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-1772	The Play.ht – Make Your Blog Posts Accessible With Text to Speech Audio plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.6.4 via deserialization of untrusted input from the play_podcast_data post meta. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a PHP Object. No known POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details
CVE-2024-1751	The Tutor LMS – eLearning and online course solution plugin for WordPress is vulnerable to time-based SQL Injection via the question_id parameter in all versions up to, and including, 2.6.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with subscriber/student access or higher, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2024-1505	The Academy LMS – eLearning and online course solution for WordPress plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.9.19. This is due to plugin allowing arbitrary user meta updates through the saved_user_info() function. This makes it possible for authenticated attackers, with minimal permissions such as students, to elevate their user role to that of an administrator.	8.8	More Details
CVE-2024-25228	Vinchin Backup and Recovery 7.2 and Earlier is vulnerable to Authenticated Remote Code Execution (RCE) via the getVerifydiyResult function in ManoeuvreHandler.class.php.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28254	OpenMetadata is a unified platform for discovery, observability, and governance powered by a central metadata repository, in-depth lineage, and seamless team collaboration. The `AlertUtil::validateExpression` method evaluates an SpEL expression using `getValue` which by default uses the `StandardEvaluationContext`, allowing the expression to reach and interact with Java classes such as `java.lang.Runtime`, leading to Remote Code Execution. The `/api/v1/events/subscriptions/validation/condition/<expression>` endpoint passes user-controlled data `AlertUtil::validateExpession` allowing authenticated (non-admin) users to execute arbitrary system commands on the underlaying operating system. In addition, there is a missing authorization check since `Authorizer.authorize()` is never called in the affected path and, therefore, any authenticated non-admin user is able to trigger this endpoint and evaluate arbitrary SpEL expressions leading to arbitrary command execution. This vulnerability was discovered with the help of CodeQL's Expression language injection (Spring) query and is also tracked as `GHSL-2023-235`. This issue may lead to Remote Code Execution and has been addressed in version 1.2.4. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details
CVE-2024-28847	OpenMetadata is a unified platform for discovery, observability, and governance powered by a central metadata repository, in-depth lineage, and seamless team collaboration. Similarly to the GHSL-2023-250 issue, `AlertUtil::validateExpression` is also called from `EventSubscriptionRepository.prepare()`, which can lead to Remote Code Execution. `prepare()` is called from `EntityRepository.prepareInternal()` which, in turn, gets called from `EntityResource.createOrUpdate()`. Note that, even though there is an authorization check (`authorizer.authorize()`), it gets called after `prepareInternal()` gets called and, therefore, after the SpEL expression has been evaluated. In order to reach this method, an attacker can send a PUT request to `/api/v1/events/subscriptions` which gets handled by `EventSubscriptionResource.createOrUpdateEventSubscription()`. This vulnerability was discovered with the help of CodeQL's Expression language injection (Spring) query. This issue may lead to Remote Code Execution and has been addressed in version 1.2.4. Users are advised to upgrade. There are no known workarounds for this vulnerability. This issue is also tracked as `GHSL-2023-251`.	8.8	More Details
CVE-2024-28848	OpenMetadata is a unified platform for discovery, observability, and governance powered by a central metadata repository, in-depth lineage, and seamless team collaboration. The `CompiledRule::validateExpression` method evaluates an SpEL expression using an `StandardEvaluationContext`, allowing the expression to reach and interact with Java classes such as `java.lang.Runtime`, leading to Remote Code Execution. The `/api/v1/policies/validation/condition/<expression>` endpoint passes user-controlled data `CompiledRule::validateExpession` allowing authenticated (non-admin) users to execute arbitrary system commands on the underlaying operating system. In addition, there is a missing authorization check since `Authorizer.authorize()` is never called in the affected path and therefore any authenticated non-admin user is able to trigger this endpoint and evaluate arbitrary SpEL expressions leading to arbitrary command execution. This vulnerability was discovered with the help of CodeQL's Expression language injection (Spring) query and is also tracked as `GHSL-2023-236`. This issue may lead to Remote Code Execution and has been resolved in version 1.2.4. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28715	Cross Site Scripting vulnerability in DOraCMS v.2.18 and before allows a remote attacker to execute arbitrary code via the markdown0 function in the /app/public/apidoc/oas3/wrap-components/markdown.jsx endpoint.	8.8	More Details
CVE-2024-1358	The Elementor Addon Elements plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.12.12 via the render function. This makes it possible for authenticated attackers, with contributor access or higher, to include the contents of arbitrary PHP files on the server, which may expose sensitive information.	8.8	More Details
CVE-2024-1311	The Brizy – Page Builder plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the storeImages function in all versions up to, and including, 2.4.40. This makes it possible for authenticated attackers, with contributor access or above, to upload arbitrary files on the affected site's server which may make remote code execution possible.	8.8	More Details
CVE-2023-51474	Cross-Site Request Forgery (CSRF) vulnerability in Pixelemu TerraClassifieds.This issue affects TerraClassifieds: from n/a through 2.0.3.	8.8	More Details
CVE-2024-1203	The Conversios – Google Analytics 4 (GA4), Meta Pixel & more Via Google Tag Manager For WooCommerce plugin for WordPress is vulnerable to SQL Injection via the 'valueData' parameter in all versions up to, and including, 6.9.1 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with 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.	8.8	More Details
CVE-2024-2581	A vulnerability was found in Tenda AC10 16.03.10.13 and classified as critical. This issue affects the function fromSetRouteStatic of the file /goform/SetStaticRouteCfg. The manipulation of the argument list leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257081 was assigned to this vulnerability.	8.8	More Details
CVE-2024-2485	A vulnerability was found in Tenda AC18 15.03.05.05 and classified as critical. Affected by this issue is the function formSetSpeedWan of the file /goform/SetSpeedWan. The manipulation of the argument speed_dir leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256892. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-2614	Memory safety bugs present in Firefox 123, Firefox ESR 115.8, and Thunderbird 115.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 124, Firefox ESR < 115.9, and Thunderbird < 115.9.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2546	A vulnerability has been found in Tenda AC18 15.13.07.09 and classified as critical. Affected by this vulnerability is the function fromSetWirelessRepeat. The manipulation of the argument wpapsk_crypto5g leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256999. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-27771	Unitronics Unistream Unilogic – Versions prior to 1.35.227 - CWE-22: 'Path Traversal' may allow RCE	8.8	More Details
CVE-2024-0779	The Enjoy Social Feed plugin for WordPress website WordPress plugin through 6.2.2 does not have authorisation and CSRF in various function hooked to admin_init, allowing unauthenticated users to call them and unlink arbitrary users Instagram Account for example	8.8	More Details
CVE-2024-0858	The Innovs HR WordPress plugin through 1.0.3.4 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwanted actions via CSRF attacks such as adding them as employees.	8.8	More Details
CVE-2024-2558	A vulnerability was found in Tenda AC18 15.03.05.05. It has been rated as critical. This issue affects the function formexeCommand of the file /goform/execCommand. The manipulation of the argument cmdinput leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257057 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2015-10123	An unautheticated remote attacker could send specifically crafted packets to a affected device. If an authenticated user then views that data in a specific page of the web-based management a buffer overflow will be triggered to gain full access of the device.	8.8	More Details
CVE-2023-41504	SQL Injection vulnerability in Student Enrollment In PHP 1.0 allows attackers to run arbitrary code via the Student Search function.	8.8	More Details
CVE-2024-27769	Unitronics Unistream Unilogic – Versions prior to 1.35.227 - CWE-200: Exposure of Sensitive Information to an Unauthorized Actor may allow Taking Ownership Over Devices	8.8	More Details
CVE-2024-0800	A path traversal vulnerability exists in Arcserve Unified Data Protection 9.2 and 8.1 in edge-app-base-webui.jar!com.ca.arcserve.edge.app.base.ui.server.servlet.ImportNodeServlet.	8.8	More Details
CVE-2024-27770	Unitronics Unistream Unilogic – Versions prior to 1.35.227 - CWE-23: Relative Path Traversal	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2547	A vulnerability was found in Tenda AC18 15.03.05.05 and classified as critical. Affected by this issue is the function R7WebsSecurityHandler. The manipulation of the argument password leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257000. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	8.8	More Details
CVE-2024-27756	GLPI through 10.0.12 allows CSV injection by an attacker who is able to create an asset with a crafted title.	8.8	More Details
CVE-2024-2414	The primary channel is unprotected on Movistar 4G router affecting E version S_WLD71-T1_v2.0.201820. This device has the 'adb' service open on port 5555 and provides access to a shell with root privileges.	8.8	More Details
CVE-2024-27772	Unitronics Unistream Unilogic – Versions prior to 1.35.227 - CWE-78: 'OS Command Injection' may allow RCE	8.8	More Details
CVE-2024-24042	Directory Traversal vulnerability in Devan-Kerman ARRP v.0.8.1 and before allows a remote attacker to execute arbitrary code via the dumpDirect in RuntimeResourcePackImpl component.	8.8	More Details
CVE-2024-27773	Unitronics Unistream Unilogic – Versions prior to 1.35.227 - CWE-348: Use of Less Trusted Source may allow RCE	8.8	More Details
CVE-2024-28424	zenml v0.55.4 was discovered to contain an arbitrary file upload vulnerability in the load function at /materializers/cloudpickle_materializer.py. This vulnerability allows attackers to execute arbitrary code via uploading a crafted file.	8.8	More Details
CVE-2024-28431	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via the component /dede/catalog_del.php.	8.8	More Details
CVE-2024-28432	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via the component /dede/article_edit.php.	8.8	More Details
CVE-2024-28665	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via the component /dede/article_add.php	8.8	More Details
CVE-2024-2006	The Post Grid, Slider & Carousel Ultimate – with Shortcode, Gutenberg Block & Elementor Widget plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.6.7 via deserialization of untrusted input in the outpost_shortcode_metabox_markup function. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a PHP Object. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-50677	An issue in NETGEAR-DGND4000 v.1.1.00.15_1.00.15 allows a remote attacker to escalate privileges via the next_file parameter to the /setup.cgi component.	8.8	More Details
CVE-2024-1795	The HUSKY – Products Filter for WooCommerce Professional plugin for WordPress is vulnerable to SQL Injection via the 'name' parameter in the woof shortcode in all versions up to, and including, 1.3.5.2 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	8.8	More Details
CVE-2024-2400	Use after free in Performance Manager in Google Chrome prior to 122.0.6261.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-38534	Improper authentication vulnerability in OpenText™ Exceed Turbo X affecting versions 12.5.0 and 12.5.1. The vulnerability could allow disclosure of restricted information in unauthenticated RPC.	8.6	More Details
CVE-2024-1753	A flaw was found in Buildah (and subsequently Podman Build) which allows containers to mount arbitrary locations on the host filesystem into build containers. A malicious Containerfile can use a dummy image with a symbolic link to the root filesystem as a mount source and cause the mount operation to mount the host root filesystem inside the RUN step. The commands inside the RUN step will then have read-write access to the host filesystem, allowing for full container escape at build time.	8.6	More Details
CVE-2020-11862	Allocation of Resources Without Limits or Throttling vulnerability in OpenText NetIQ Privileged Account Manager on Linux, Windows, 64 bit allows Flooding.This issue affects NetIQ Privileged Account Manager: before 3.7.0.2.	8.6	More Details
CVE-2023-7060	Zephyr OS IP packet handling does not properly drop IP packets arriving on an external interface with a source address equal to 127.0.01 or the destination address.	8.6	More Details
CVE-2024-1222	This allows attackers to use a maliciously formed API request to gain access to an API authorization level with elevated privileges. This applies to a small subset of PaperCut NG/MF API calls.	8.6	More Details
CVE-2024-0368	The Hustle – Email Marketing, Lead Generation, Optins, Popups plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 7.8.3 via hardcoded API Keys. This makes it possible for unauthenticated attackers to extract sensitive data including PII.	8.6	More Details
CVE-2024-29136	Deserialization of Untrusted Data vulnerability in Themefic Tourfic.This issue affects Tourfic: from n/a through 2.11.17.	8.5	More Details
CVE-2024-22346	Db2 for IBM i 7.2, 7.3, 7.4, and 7.5 infrastructure could allow a local user to gain elevated privileges due to an unqualified library call. A malicious actor could cause user-controlled code to run with administrator privilege. IBM X-Force ID: 280203.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41334	Astropy is a project for astronomy in Python that fosters interoperability between Python astronomy packages. Version 5.3.2 of the Astropy core package is vulnerable to remote code execution due to improper input validation in the `TranformGraph().to_dot_graph` function. A malicious user can provide a command or a script file as a value to the `savelayout` argument, which will be placed as the first value in a list of arguments passed to `subprocess.Popen`. Although an error will be raised, the command or script will be executed successfully. Version 5.3.3 fixes this issue.	8.4	More Details
CVE-2024-2588	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/admin/index.php, in the 'id' parameter. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	8.2	More Details
CVE-2024-2586	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/index.php, in the 'username' parameter. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	8.2	More Details
CVE-2024-2587	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/book/main/bookdetail_khet_person.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	8.2	More Details
CVE-2024-22257	In Spring Security, versions 5.7.x prior to 5.7.12, 5.8.x prior to 5.8.11, versions 6.0.x prior to 6.0.9, versions 6.1.x prior to 6.1.8, versions 6.2.x prior to 6.2.3, an application is possible vulnerable to broken access control when it directly uses the AuthenticatedVoter#vote passing a null Authentication parameter.	8.2	More Details
CVE-2024-2050	CWE-79: Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’) vulnerability exists when an attacker injects then executes arbitrary malicious JavaScript code within the context of the product.	8.2	More Details
CVE-2024-2585	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/book/main/select_send_2.php, in the 'sd_index' parameter. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	8.2	More Details
CVE-2024-27266	IBM Maximo Application Suite 7.6.1.3 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 284566.	8.2	More Details
CVE-2024-2584	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/book/main/select_send.php, in the 'sd_index' parameter. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2589	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/book/main/bookdetail_school_person.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	8.2	More Details
CVE-2023-7009	Some Sciener-based locks support plaintext message processing over Bluetooth Low Energy, allowing unencrypted malicious commands to be passed to the lock. These malicious commands, less then 16 bytes in length, will be processed by the lock as if they were encrypted communications. This can be further exploited by an attacker to compromise the lock's integrity.	8.2	More Details
CVE-2024-2591	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/book/main/bookdetail_group.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	8.2	More Details
CVE-2024-2592	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/person/pic_show.php, in the 'person_id' parameter. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	8.2	More Details
CVE-2024-2590	Vulnerability in AMSS++ version 4.31 that allows SQL injection through /amssplus/modules/mail/main/select_send.php, in the 'sd_index' parameter. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the server and retrieve all the information stored in the DB.	8.2	More Details
CVE-2024-2607	Return registers were overwritten which could have allowed an attacker to execute arbitrary code. *Note:* This issue only affected Armv7-A systems. Other operating systems are unaffected. This vulnerability affects Firefox < 124, Firefox ESR < 115.9, and Thunderbird < 115.9.	8.1	More Details
CVE-2024-1862	The WooCommerce Add to Cart Custom Redirect plugin for WordPress is vulnerable to unauthorized modification of data and loss of data due to a missing capability check on the 'wcr_dismiss_admin_notice' function in all versions up to, and including, 1.2.13. This makes it possible for authenticated attackers, with contributor access and above, to update the values of arbitrary site options to 'dismissed'.	8.1	More Details
CVE-2024-28195	your_spotify is an open source, self hosted Spotify tracking dashboard. YourSpotify versions < 1.9.0 do not protect the API and login flow against Cross-Site Request Forgery (CSRF). Attackers can use this to execute CSRF attacks on victims, allowing them to retrieve, modify or delete data on the affected YourSpotify instance. Using repeated CSRF attacks, it is also possible to create a new user on the victim instance and promote the new user to instance administrator if a legitimate administrator visits a website prepared by an attacker. Note: Real-world exploitability of this vulnerability depends on the browser version and browser settings in use by the victim. This issue has been addressed in version 1.9.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28746	Apache Airflow, versions 2.8.0 through 2.8.2, has a vulnerability that allows an authenticated user with limited permissions to access resources such as variables, connections, etc from the UI which they do not have permission to access. Users of Apache Airflow are recommended to upgrade to version 2.8.3 or newer to mitigate the risk associated with this vulnerability	8.1	More Details
CVE-2024-28855	ZITADEL, open source authentication management software, uses Go templates to render the login UI. Due to a improper use of the `text/template` instead of the `html/template` package, the Login UI did not sanitize input parameters prior to versions 2.47.3, 2.46.1, 2.45.1, 2.44.3, 2.43.9, 2.42.15, and 2.41.15. An attacker could create a malicious link, where he injected code which would be rendered as part of the login screen. While it was possible to inject HTML including JavaScript, the execution of such scripts would be prevented by the Content Security Policy. Versions 2.47.3, 2.46.1, 2.45.1, 2.44.3, 2.43.9, 2.42.15, and 2.41.15 contain a patch for this issue. No known workarounds are available.	8.1	More Details
CVE-2024-22259	Applications that use UriComponentsBuilder in Spring Framework to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the parsed URL may be vulnerable to a open redirect https://cwe.mitre.org/data/definitions/601.html attack or to a SSRF attack if the URL is used after passing validation checks. This is the same as CVE-2024-22243 https://spring.io/security/cve-2024-22243 , but with different input.	8.1	More Details
CVE-2024-2612	If an attacker could find a way to trigger a particular code path in `SafeRefPtr`, it could have triggered a crash or potentially be leveraged to achieve code execution. This vulnerability affects Firefox < 124, Firefox ESR < 115.9, and Thunderbird < 115.9.	8.1	More Details
CVE-2024-24336	A multiple Cross-site scripting (XSS) vulnerability in the '/members/moremember.pl', and '/members/members-home.pl' endpoints within Koha Library Management System version 23.05.05 and earlier allows malicious staff users to carry out CSRF attacks, including unauthorized changes to usernames and passwords of users visiting the affected page, via the 'Circulation note' and 'Patrons Restriction' components.	8.1	More Details
CVE-2024-28181	turbo_boost-commands is a set of commands to help you build robust reactive applications with Rails & Hotwire. TurboBoost Commands has existing protections in place to guarantee that only public methods on Command classes can be invoked; however, the existing checks aren't as robust as they should be. It's possible for a sophisticated attacker to invoke more methods than should be permitted depending on the the strictness of authorization checks that individual applications enforce. Being able to call some of these methods can have security implications. Commands verify that the class must be a `Command` and that the method requested is defined as a public method; however, this isn't robust enough to guard against all unwanted code execution. The library should more strictly enforce which methods are considered safe before allowing them to be executed. This issue has been addressed in versions 0.1.3, and 0.2.2. Users are advised to upgrade. Users unable to upgrade should see the repository GHSA for workaround advice.	8.1	More Details
CVE-2024-28404	TOTOLINK X2000R before V1.0.0-B20231213.1013 contains a Stored Cross-site scripting (XSS) vulnerability in MAC Filtering under the Firewall Page.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0860	The affected product is vulnerable to a cleartext transmission of sensitive information vulnerability, which may allow an attacker to capture packets to craft their own requests.	8.0	More Details
CVE-2024-22167	A potential DLL hijacking vulnerability in the SanDisk PrivateAccess application for Windows that could lead to arbitrary code execution in the context of the system user. This vulnerability is only exploitable locally if an attacker has access to a copy of the user's vault or has already gained access into a user's system. This attack is limited to the system in context and cannot be propagated.	7.9	More Details
CVE-2024-23333	LDAP Account Manager (LAM) is a webfrontend for managing entries stored in an LDAP directory. LAM's log configuration allows to specify arbitrary paths for log files. Prior to version 8.7, an attacker could exploit this by creating a PHP file and cause LAM to log some PHP code to this file. When the file is then accessed via web the code would be executed. The issue is mitigated by the following: An attacker needs to know LAM's master configuration password to be able to change the main settings; and the webserver needs write access to a directory that is accessible via web. LAM itself does not provide any such directories. The issue has been fixed in 8.7. As a workaround, limit access to LAM configuration pages to authorized users.	7.9	More Details
CVE-2023-42920	Claris International has fixed a dylib hijacking vulnerability in the FileMaker Pro.app and Claris Pro.app versions on macOS.	7.8	More Details
CVE-2023-52614	In the Linux kernel, the following vulnerability has been resolved: PM / devfreq: Fix buffer overflow in trans_stat_show Fix buffer overflow in trans_stat_show(). Convert simple snprintf to the more secure scnprintf with size of PAGE_SIZE. Add condition checking if we are exceeding PAGE_SIZE and exit early from loop. Also add at the end a warning that we exceeded PAGE_SIZE and that stats is disabled. Return -EFBIG in the case where we don't have enough space to write the full transition table. Also document in the ABI that this function can return -EFBIG error.	7.8	More Details
CVE-2024-20745	Premiere Pro versions 24.1, 23.6.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-23139	An Out-Of-Bounds Write Vulnerability in Autodesk FBX Review version 1.5.3.0 and prior may lead to code execution or information disclosure through maliciously crafted ActionScript Byte Code “ABC” files. ABC files are created by the Flash compiler and contain executable code. This vulnerability in conjunction with other vulnerabilities could lead to code execution in the context of the current process.	7.8	More Details
CVE-2023-42938	A logic issue was addressed with improved checks. This issue is fixed in iTunes 12.13.1 for Windows. A local attacker may be able to elevate their privileges.	7.8	More Details
CVE-2024-20746	Premiere Pro versions 24.1, 23.6.2 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 Number	Description	Base Score	Reference
CVE-2024-20320	A vulnerability in the SSH client feature of Cisco IOS XR Software for Cisco 8000 Series Routers and Cisco Network Convergence System (NCS) 540 Series and 5700 Series Routers could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient validation of arguments that are included with the SSH client CLI command. An attacker with low-privileged access to an affected device could exploit this vulnerability by issuing a crafted SSH client command to the CLI. A successful exploit could allow the attacker to elevate privileges to root on the affected device.	7.8	More Details
CVE-2024-2390	As a part of Tenable's vulnerability disclosure program, a vulnerability in a Nessus plugin was identified and reported. This vulnerability could allow a malicious actor with sufficient permissions on a scan target to place a binary in a specific filesystem location, and abuse the impacted plugin in order to escalate privileges.	7.8	More Details
CVE-2024-20754	Lightroom Desktop versions 7.1.2 and earlier are affected by an Untrusted Search Path vulnerability that could result in arbitrary code execution in the context of the current user. If the application uses a search path to locate critical resources such as programs, then an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-2415	Command injection vulnerability in Movistar 4G router affecting version ES_WLD71-T1_v2.0.201820. This vulnerability allows an authenticated user to execute commands inside the router by making a POST request to the URL '/cgi-bin/gui.cgi'.	7.8	More Details
CVE-2024-20755	Bridge versions 13.0.5, 14.0.1 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-26540	A heap-based buffer overflow in CImg before 3.3.3 can occur via a crafted file to cimg_library::CImg<unsigned char>::_load_analyze.	7.8	More Details
CVE-2024-2229	CWE-502: Deserialization of Untrusted Data vulnerability exists that could cause remote code execution when a malicious project file is loaded into the application by a valid user.	7.8	More Details
CVE-2024-20756	Bridge versions 13.0.5, 14.0.1 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-2024-20752	Bridge versions 13.0.5, 14.0.1 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6597	An issue was found in the CPython `tempfile.TemporaryDirectory` class affecting versions 3.12.1, 3.11.7, 3.10.13, 3.9.18, and 3.8.18 and prior. The tempfile.TemporaryDirectory class would dereference symlinks during cleanup of permissions-related errors. This means users which can run privileged programs are potentially able to modify permissions of files referenced by symlinks in some circumstances.	7.8	More Details
CVE-2024-20761	Animate versions 24.0, 23.0.3 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-2023-50168	Pega Platform from 6.x to 8.8.4 is affected by an XXE issue with PDF Generation.	7.7	More Details
CVE-2024-1623	Insufficient session timeout vulnerability in the FAST3686 V2 Vodafone router from Sagemcom. This vulnerability could allow a local attacker to access the administration panel without requiring login credentials. This vulnerability is possible because the 'Login.asp and logout.asp' files do not handle session details correctly.	7.7	More Details
CVE-2024-27096	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. An authenticated user can exploit a SQL injection vulnerability in the search engine to extract data from the database. This issue has been patched in version 10.0.13.	7.7	More Details
CVE-2023-44092	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Pandora FMS on all allows OS Command Injection. This vulnerability allowed to create a reverse shell and execute commands in the OS. This issue affects Pandora FMS: from 700 through <776.	7.6	More Details
CVE-2024-28425	greykite v1.0.0 was discovered to contain an arbitrary file upload vulnerability in the load_obj function at /templates/pickle_utils.py. This vulnerability allows attackers to execute arbitrary code via uploading a crafted file.	7.5	More Details
CVE-2024-28640	Buffer Overflow vulnerability in TOTOLink X5000R V9.1.0u.6118-B20201102 and A7000R V9.1.0u.6115-B20201022 allows a remote attacker to cause a denial of service (D0S) via the command field.	7.5	More Details
CVE-2024-2442	Franklin Fueling System EVO 550 and EVO 5000 are vulnerable to a Path Traversal vulnerability that could allow an attacker to access sensitive files on the system.	7.5	More Details
CVE-2024-23138	A maliciously crafted DWG file when parsed through Autodesk DWG TrueView can be used to cause a Stack-based Overflow. A malicious actor can leverage this vulnerability to cause a crash, read sensitive data, or execute arbitrary code in the context of the current process.	7.5	More Details
CVE-2024-2169	Implementations of UDP application protocol are vulnerable to network loops. An unauthenticated attacker can use maliciously-crafted packets against a vulnerable implementation that can lead to Denial of Service (DOS) and/or abuse of resources.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40747	Directory traversal vulnerability exists in A.K.I Software's PMailServer/PMailServer2 products' CGIs included in Internal Simple Webserver. If this vulnerability is exploited, a remote attacker may access arbitrary files outside DocumentRoot.	7.5	More Details
CVE-2024-24549	Denial of Service due to improper input validation vulnerability for HTTP/2 requests in Apache Tomcat. When processing an HTTP/2 request, if the request exceeded any of the configured limits for headers, the associated HTTP/2 stream was not reset until after all of the headers had been processed.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M16, from 10.1.0-M1 through 10.1.18, from 9.0.0-M1 through 9.0.85, from 8.5.0 through 8.5.98. Users are recommended to upgrade to version 11.0.0-M17, 10.1.19, 9.0.86 or 8.5.99 which fix the issue.	7.5	More Details
CVE-2024-1950	The Product Carousel Slider & Grid Ultimate for WooCommerce plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.9.7 via deserialization of untrusted input via shortcode. This makes it possible for authenticated attackers, with contributor access and above, to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	7.5	More Details
CVE-2024-1951	The Logo Showcase Ultimate – Logo Carousel, Logo Slider & Logo Grid plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.3.8 via deserialization via shortcode of untrusted input. This makes it possible for authenticated attackers, with contributor access and above, to inject a PHP Object. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary files, retrieve sensitive data, or execute code.	7.5	More Details
CVE-2024-2052	CWE-552: Files or Directories Accessible to External Parties vulnerability exists that could allow unauthenticated files and logs exfiltration and download of files when an attacker modifies the URL to download to a different location.	7.5	More Details
CVE-2024-2002	A double-free vulnerability was found in libdwarf. In a multiply-corrupted DWARF object, libdwarf may try to dealloc(free) an allocation twice, potentially causing unpredictable and various results.	7.5	More Details
CVE-2023-6960	TTLock App virtual keys and settings are only deleted client side, and if preserved, can access the lock after intended deletion.	7.5	More Details
CVE-2024-24230	Komm.One CMS 10.4.2.14 has a Server-Side Template Injection (SSTI) vulnerability via the Velocity template engine. It allows remote attackers to execute arbitrary code via a URL that specifies java.lang.Runtime in conjunction with getRuntime().exec followed by an OS command.	7.5	More Details
CVE-2022-47037	Siklu TG Terragraph devices before 2.1.1 allow attackers to discover valid, randomly generated credentials via GetCredentials.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26529	An issue in mz-automation libiec61850 v.1.5.3 and before, allows a remote attacker to cause a denial of service (DoS) via the mmsServer_handleDeleteNamedVariableListRequest function of src/mms/iso_mms/server/mms_named_variable_list_service.c.	7.5	More Details
CVE-2023-40279	An issue was discovered in OpenClinic GA 5.247.01. An attacker can perform a directory path traversal via the Page parameter in a GET request to main.do.	7.5	More Details
CVE-2024-21661	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Prior to versions 2.8.13, 2.9.9, and 2.10.4, an attacker can exploit a critical flaw in the application to initiate a Denial of Service (DoS) attack, rendering the application inoperable and affecting all users. The issue arises from unsafe manipulation of an array in a multi-threaded environment. The vulnerability is rooted in the application's code, where an array is being modified while it is being iterated over. This is a classic programming error but becomes critically unsafe when executed in a multi-threaded environment. When two threads interact with the same array simultaneously, the application crashes. This is a Denial of Service (DoS) vulnerability. Any attacker can crash the application continuously, making it impossible for legitimate users to access the service. The issue is exacerbated because it does not require authentication, widening the pool of potential attackers. Versions 2.8.13, 2.9.9, and 2.10.4 contain a patch for this issue.	7.5	More Details
CVE-2024-21662	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. Prior to versions 2.8.13, 2.9.9, and 2.10.4, an attacker can effectively bypass the rate limit and brute force protections by exploiting the application's weak cache-based mechanism. This loophole in security can be combined with other vulnerabilities to attack the default admin account. This flaw undermines a patch for CVE-2020-8827 intended to protect against brute-force attacks. The application's brute force protection relies on a cache mechanism that tracks login attempts for each user. This cache is limited to a `defaultMaxCacheSize` of 1000 entries. An attacker can overflow this cache by bombarding it with login attempts for different users, thereby pushing out the admin account's failed attempts and effectively resetting the rate limit for that account. This is a severe vulnerability that enables attackers to perform brute force attacks at an accelerated rate, especially targeting the default admin account. Users should upgrade to version 2.8.13, 2.9.9, or 2.10.4 to receive a patch.	7.5	More Details
CVE-2024-0801	A denial of service vulnerability exists in Arcserve Unified Data Protection 9.2 and 8.1 in ASNative.dll.	7.5	More Details
CVE-2024-2613	Data was not properly sanitized when decoding a QUIC ACK frame; this could have led to unrestricted memory consumption and a crash. This vulnerability affects Firefox < 124.	7.5	More Details
CVE-2023-40280	An issue was discovered in OpenClinic GA 5.247.01. An attacker can perform a directory path traversal via the Page parameter in a GET request to popup.jsp.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44091	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pandora FMS on all allows SQL Injection. This ulnerability allowed SQL injections to be made even if authentication failed.This issue affects Pandora FMS: from 700 through <776.	7.5	More Details
CVE-2024-28854	tls-listener is a rust lang wrapper around a connection listener to support TLS. With the default configuration of tls-listener, a malicious user can open 6.4 `TcpStream`s a second, sending 0 bytes, and can trigger a DoS. The default configuration options make any public service using `TlsListener::new()` vulnerable to a slow-loris DoS attack. This impacts any publicly accessible service using the default configuration of tls-listener in versions prior to 0.10.0. Users are advised to upgrade. Users unable to upgrade may mitigate this by passing a large value, such as `usize::MAX` as the parameter to `Builder::max_handshakes`.	7.5	More Details
CVE-2024-28865	django-wiki is a wiki system for Django. Installations of django-wiki prior to version 0.10.1 are vulnerable to maliciously crafted article content that can cause severe use of server CPU through a regular expression loop. Version 0.10.1 fixes this issue. As a workaround, close off access to create and edit articles by anonymous users.	7.5	More Details
CVE-2024-28252	CoreWCF is a port of the service side of Windows Communication Foundation (WCF) to .NET Core. If you have a NetFraming based CoreWCF service, extra system resources could be consumed by connections being left established instead of closing or aborting them. There are two scenarios when this can happen. When a client established a connection to the service and sends no data, the service will wait indefinitely for the client to initiate the NetFraming session handshake. Additionally, once a client has established a session, if the client doesn't send any requests for the period of time configured in the binding ReceiveTimeout, the connection is not properly closed as part of the session being aborted. The bindings affected by this behavior are NetTcpBinding, NetNamedPipeBinding, and UnixDomainSocketBinding. Only NetTcpBinding has the ability to accept non local connections. The currently supported versions of CoreWCF are v1.4.x and v1.5.x. The fix can be found in v1.4.2 and v1.5.2 of the CoreWCF packages. Users are advised to upgrade. There are no workarounds for this issue.	7.5	More Details
CVE-2024-26369	An issue in the HistoryQosPolicy component of FastDDS v2.12.x, v2.11.x, v2.10.x, and v2.6.x leads to a SIGABRT (signal abort) upon receiving DataWriter's data.	7.5	More Details
CVE-2024-2632	A Information Exposure Vulnerability has been found on Meta4 HR. This vulnerability allows an attacker to obtain a lot of information about the application such as the variables set in the process, the Tomcat versions, library versions and underlying operation system via HTTP GET '/sitetest/english/dumpenv.jsp'.	7.5	More Details
CVE-2024-27774	Unitronics Unistream Unilogic – Versions prior to 1.35.227 - CWE-259: Use of Hard-coded Password may allow disclosing Sensitive Information Embedded inside Device's Firmware	7.5	More Details
CVE-2023-40278	An issue was discovered in OpenClinic GA 5.247.01. An Information Disclosure vulnerability has been identified in the printAppointmentPdf.jsp component of OpenClinic GA. By changing the AppointmentUid parameter, an attacker can determine whether a specific appointment exists based on the error message.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20327	A vulnerability in the PPP over Ethernet (PPPoE) termination feature of Cisco IOS XR Software for Cisco ASR 9000 Series Aggregation Services Routers could allow an unauthenticated, adjacent attacker to crash the ppp_ma process, resulting in a denial of service (DoS) condition. This vulnerability is due to the improper handling of malformed PPPoE packets that are received on a router that is running Broadband Network Gateway (BNG) functionality with PPPoE termination on a Lightspeed-based or Lightspeed-Plus-based line card. An attacker could exploit this vulnerability by sending a crafted PPPoE packet to an affected line card interface that does not terminate PPPoE. A successful exploit could allow the attacker to crash the ppp_ma process, resulting in a DoS condition for PPPoE traffic across the router.	7.4	More Details
CVE-2024-29154	danielmiessler fabric through 1.3.0 allows installer/client/gui/static/js/index.js XSS because of innerHTML mishandling, such as in htmlToPlainText.	7.4	More Details
CVE-2024-27920	projectdiscovery/nuclei is a fast and customisable vulnerability scanner based on simple YAML based DSL. A significant security oversight was identified in Nuclei v3, involving the execution of unsigned code templates through workflows. This vulnerability specifically affects users utilizing custom workflows, potentially allowing the execution of malicious code on the user's system. This advisory outlines the impacted users, provides details on the security patch, and suggests mitigation strategies. The vulnerability is addressed in Nuclei v3.2.0. Users are strongly recommended to update to this version to mitigate the security risk. Users should refrain from using custom workflows if unable to upgrade immediately. Only trusted, verified workflows should be executed.	7.4	More Details
CVE-2024-1536	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's event calendar widget in all versions up to, and including, 5.9.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.4	More Details
CVE-2024-20318	A vulnerability in the Layer 2 Ethernet services of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause the line card network processor to reset, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of specific Ethernet frames that are received on line cards that have the Layer 2 services feature enabled. An attacker could exploit this vulnerability by sending specific Ethernet frames through an affected device. A successful exploit could allow the attacker to cause the ingress interface network processor to reset, resulting in a loss of traffic over the interfaces that are supported by the network processor. Multiple resets of the network processor would cause the line card to reset, resulting in a DoS condition.	7.4	More Details
CVE-2024-20767	ColdFusion versions 2023.6, 2021.12 and earlier are affected by an Improper Access Control vulnerability that could result in arbitrary file system read. An attacker could leverage this vulnerability to access or modify restricted files. Exploitation of this issue does not require user interaction. Exploitation of this issue requires the admin panel be exposed to the internet.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2647	A vulnerability, which was classified as critical, has been found in Netentsec NS-ASG Application Security Gateway 6.3. This issue affects some unknown processing of the file /admin/singlelogin.php. The manipulation of the argument loginId leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257285 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details
CVE-2024-27301	Support App is an opensource application specialized in managing Apple devices. It's possible to abuse a vulnerability inside the postinstall installer script to make the installer execute arbitrary code as root. The cause of the vulnerability is the fact that the shebang `#!/bin/zsh` is being used. When the installer is executed it asks for the users password to be executed as root. However, it'll still be using the $HOME of the user and therefore loading the file `$HOME/.zshenv` when the `postinstall` script is executed. An attacker could add malicious code to `$HOME/.zshenv` and it will be executed when the app is installed. An attacker may leverage this vulnerability to escalate privilege on the system. This issue has been addressed in version 2.5.1 Rev 2. All users are advised to upgrade. There are no known workarounds for this vulnerability.	7.3	More Details
CVE-2024-2566	A vulnerability was found in Fujian Kelixin Communication Command and Dispatch Platform up to 20240313. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file api/client/get_extension_yl.php. The manipulation of the argument imei leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257065 was assigned to this vulnerability.	7.3	More Details
CVE-2024-0683	The Bulgarisation for WooCommerce plugin for WordPress is vulnerable to unauthorized access due to missing capability checks on several functions in all versions up to, and including, 3.0.14. This makes it possible for unauthenticated and authenticated attackers, with subscriber-level access and above, to generate and delete labels.	7.3	More Details
CVE-2024-2570	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been classified as critical. This affects an unknown part of the file /edit-task.php. The manipulation leads to execution after redirect. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257073 was assigned to this vulnerability.	7.3	More Details
CVE-2024-2514	A vulnerability classified as critical was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected by this vulnerability is an unknown functionality of the file /login.php. The manipulation of the argument email leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256951. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2571	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /manage-admin.php. The manipulation leads to execution after redirect. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257074 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-2577	A vulnerability has been found in SourceCodester Employee Task Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /update-employee.php. The manipulation of the argument admin_id leads to authorization bypass. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257080.	7.3	More Details
CVE-2024-2635	The configuration pages available are not intended to be placed on an Internet facing web server, as they expose file paths to the client, who can be an attacker. Instead of rewriting these pages to avoid this vulnerability, they will be dismissed from future releases of Cegid Meta4 HR, as they do not offer product functionality	7.3	More Details
CVE-2024-2575	A vulnerability, which was classified as critical, has been found in SourceCodester Employee Task Management System 1.0. Affected by this issue is some unknown functionality of the file /task-details.php. The manipulation of the argument task_id leads to authorization bypass. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257078 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2024-2576	A vulnerability, which was classified as critical, was found in SourceCodester Employee Task Management System 1.0. This affects an unknown part of the file /update-admin.php. The manipulation of the argument admin_id leads to authorization bypass. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257079.	7.3	More Details
CVE-2024-2574	A vulnerability classified as critical was found in SourceCodester Employee Task Management System 1.0. Affected by this vulnerability is an unknown functionality of the file /edit-task.php. The manipulation of the argument task_id leads to authorization bypass. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257077 was assigned to this vulnerability.	7.3	More Details
CVE-2024-2569	A vulnerability was found in SourceCodester Employee Task Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin-manage-user.php. The manipulation leads to execution after redirect. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257072.	7.3	More Details
CVE-2024-2642	A vulnerability was found in Ruijie RG-NBS2009G-P up to 20240305. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /EXCU_SHELL. The manipulation of the argument Command1 leads to command injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257281 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2573	A vulnerability classified as critical has been found in SourceCodester Employee Task Management System 1.0. Affected is an unknown function of the file /task-info.php. The manipulation leads to execution after redirect. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257076.	7.3	More Details
CVE-2024-2572	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /task-details.php. The manipulation leads to execution after redirect. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257075.	7.3	More Details
CVE-2024-24693	Improper access control in the installer for Zoom Rooms Client for Windows before version 5.17.5 may allow an authenticated user to conduct a denial of service via local access.	7.2	More Details
CVE-2023-32282	Race condition in BIOS firmware for some Intel(R) Processors may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	More Details
CVE-2023-32666	On-chip debug and test interface with improper access control in some 4th Generation Intel(R) Xeon(R) Processors when using Intel(R) SGX or Intel(R) TDX may allow a privileged user to potentially enable escalation of privilege via local access.	7.2	More Details
CVE-2024-28092	UBEE DDW365 XCNDDW365 8.14.3105 software on hardware 3.13.1 allows a remote attacker within Wi-Fi proximity to conduct stored XSS attacks via RgFirewallEL.asp, RgDdns.asp, RgTime.asp, RgDiagnostics.asp, or RgParentalBasic.asp. The affected fields are SMTP Server Name, SMTP Username, Host Name, Time Server 1, Time Server 2, Time Server 3, Target, Add Keyword, Add Domain, and Add Allowed Domain.	7.2	More Details
CVE-2024-0161	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain an Improper SMM communication buffer verification vulnerability. A local low privileged attacker could potentially exploit this vulnerability leading to arbitrary writes to SMRAM.	7.2	More Details
CVE-2024-1882	This vulnerability allows an already authenticated admin user to create a malicious payload that could be leveraged for remote code execution on the server hosting the PaperCut NG/MF application server.	7.2	More Details
CVE-2024-2123	The Ultimate Member – User Profile, Registration, Login, Member Directory, Content Restriction & Membership Plugin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the several parameters in all versions up to, and including, 2.8.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	7.2	More Details
CVE-2024-1654	This vulnerability potentially allows unauthorized write operations which may lead to remote code execution. An attacker must already have authenticated admin access and knowledge of both an internal system identifier and details of another valid user to exploit this.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2194	The WP Statistics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the URL search parameter in all versions up to, and including, 14.5 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-2024-22453	Dell PowerEdge Server BIOS contains a heap-based buffer overflow vulnerability. A local high privileged attacker could potentially exploit this vulnerability to write to otherwise unauthorized memory.	7.2	More Details
CVE-2024-1793	The AWeber – Free Sign Up Form and Landing Page Builder Plugin for Lead Generation and Email Newsletter Growth plugin for WordPress is vulnerable to SQL Injection via the 'post_id' parameter in all versions up to, and including, 7.3.14 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.2	More Details
CVE-2024-28248	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Starting in version 1.13.9 and prior to versions 1.13.13, 1.14.8, and 1.15.2, Cilium's HTTP policies are not consistently applied to all traffic in the scope of the policies, leading to HTTP traffic being incorrectly and intermittently forwarded when it should be dropped. This issue has been patched in Cilium 1.15.2, 1.14.8, and 1.13.13. There are no known workarounds for this issue.	7.2	More Details
CVE-2024-1935	The Giveaways and Contests by RafflePress – Get More Website Traffic, Email Subscribers, and Social Followers plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘parent_url’ parameter in all versions up to, and including, 1.12.5 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-2024-2020	The Calculated Fields Form plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form page href parameter in all versions up to, and including, 5.1.56 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. Exploitation requires the professional version or higher.	7.2	More Details
CVE-2024-1713	A user who can create objects in a database with plv8 3.2.1 installed is able to cause deferred triggers to execute as the Superuser during autovacuum.	7.2	More Details
CVE-2024-25155	In FileCatalyst Direct 3.8.8 and earlier through 3.8.6, the web server does not properly sanitize illegal characters in a URL which is then displayed on a subsequent error page. A malicious actor could craft a URL which would then execute arbitrary code within an HTML script tag.	7.2	More Details
CVE-2024-27961	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Codekraft AntiSpam for Contact Form 7 allows Reflected XSS.This issue affects AntiSpam for Contact Form 7: from n/a through 0.6.0.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27958	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themeisle Visualizer allows Reflected XSS.This issue affects Visualizer: from n/a through 3.10.5.	7.1	More Details
CVE-2024-29137	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themefic Tourfic allows Reflected XSS.This issue affects Tourfic: from n/a through 2.11.7.	7.1	More Details
CVE-2024-27960	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in I Thirteen Web Solution Email Subscription Popup allows Stored XSS.This issue affects Email Subscription Popup: from n/a through 1.2.20.	7.1	More Details
CVE-2024-29130	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Scott Paterson Contact Form 7 – PayPal & Stripe Add-on allows Reflected XSS.This issue affects Contact Form 7 – PayPal & Stripe Add-on: from n/a through 2.0.	7.1	More Details
CVE-2024-29138	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in DEV Institute Restrict User Access – Membership Plugin with Force allows Reflected XSS.This issue affects Restrict User Access – Membership Plugin with Force: from n/a through 2.5.	7.1	More Details
CVE-2024-29128	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Post SMTP POST SMTP allows Reflected XSS.This issue affects POST SMTP: from n/a through 2.8.6.	7.1	More Details
CVE-2024-29127	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AAM Advanced Access Manager allows Reflected XSS.This issue affects Advanced Access Manager: from n/a through 6.9.20.	7.1	More Details
CVE-2024-29103	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in NinjaTeam Database for Contact Form 7 allows Stored XSS.This issue affects Database for Contact Form 7: from n/a through 3.0.6.	7.1	More Details
CVE-2024-29129	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPLIT Pty Ltd OxyExtras allows Reflected XSS.This issue affects OxyExtras: from n/a through 1.4.4.	7.1	More Details
CVE-2024-29126	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jose Mortellaro Specific Content For Mobile – Customize the mobile version without redirections allows Reflected XSS.This issue affects Specific Content For Mobile – Customize the mobile version without redirections: from n/a through 0.1.9.5.	7.1	More Details
CVE-2024-29102	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasThemes Extensions For CF7 allows Stored XSS.This issue affects Extensions For CF7: from n/a through 3.0.6.	7.1	More Details
CVE-2024-29139	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Mark Tilly MyCurator Content Curation allows Reflected XSS.This issue affects MyCurator Content Curation: from n/a through 3.76.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29125	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Elliot Sowersby, RelyWP Coupon Affiliates allows Reflected XSS.This issue affects Coupon Affiliates: from n/a through 5.12.7.	7.1	More Details
CVE-2024-29123	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Yannick Lefebvre Link Library allows Reflected XSS.This issue affects Link Library: from n/a through 7.6.	7.1	More Details
CVE-2024-27987	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GiveWP Give allows Reflected XSS.This issue affects Give: from n/a through 3.3.1.	7.1	More Details
CVE-2024-25921	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Concerted Action Action Network allows Reflected XSS.This issue affects Action Network: from n/a through 1.4.2.	7.1	More Details
CVE-2024-27197	Cross-Site Request Forgery (CSRF) vulnerability in Bee BeePress allows Stored XSS.This issue affects BeePress: from n/a through 6.9.8.	7.1	More Details
CVE-2024-27193	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PayU PayU India allows Reflected XSS.This issue affects PayU India: from n/a through 3.8.2.	7.1	More Details
CVE-2024-27196	Cross Site Scripting (XSS) vulnerability in Joel Starnes postMash – custom post order allows Reflected XSS.This issue affects postMash – custom post order: from n/a through 1.2.0.	7.1	More Details
CVE-2024-29121	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Firassaidi WooCommerce License Manager allows Reflected XSS.This issue affects WooCommerce License Manager: from n/a through 5.3.1.	7.1	More Details
CVE-2024-25597	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Etoile Web Design Ultimate Reviews allows Stored XSS.This issue affects Ultimate Reviews: from n/a through 3.2.8.	7.1	More Details
CVE-2024-29117	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cimatti Consulting Contact Forms by Cimatti allows Stored XSS.This issue affects Contact Forms by Cimatti: from n/a through 1.7.0.	7.1	More Details
CVE-2024-29116	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in IconicWP WooThumbs for WooCommerce by Iconic allows Reflected XSS.This issue affects WooThumbs for WooCommerce by Iconic: from n/a through 5.5.3.	7.1	More Details
CVE-2024-1013	An out-of-bounds stack write flaw was found in unixODBC on 64-bit architectures where the caller has 4 bytes and callee writes 8 bytes. This issue may go unnoticed on little-endian architectures, while big-endian architectures can be broken.	7.1	More Details
CVE-2024-28318	gpac 2.3-DEV-rev921-g422b78ecf-master was discovered to contain a out of boundary write vulnerability via swf_get_string at scene_manager/swf_parse.c:325	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29113	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Metagauss RegistrationMagic allows Reflected XSS.This issue affects RegistrationMagic: from n/a through 5.2.5.9.	7.1	More Details
CVE-2024-29110	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pauple Table & Contact Form 7 Database – Tablesome allows Reflected XSS.This issue affects Table & Contact Form 7 Database – Tablesome: from n/a through 1.0.27.	7.1	More Details
CVE-2024-29099	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Evergreen Content Poster allows Reflected XSS.This issue affects Evergreen Content Poster: from n/a through 1.4.1.	7.1	More Details
CVE-2024-27195	Cross-Site Request Forgery (CSRF) vulnerability in Sandi Verdev Watermark RELOADED allows Stored XSS.This issue affects Watermark RELOADED: from n/a through 1.3.5.	7.1	More Details
CVE-2024-29142	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WebberZone Better Search – Relevant search results for WordPress allows Stored XSS.This issue affects Better Search – Relevant search results for WordPress: from n/a through 3.3.0.	7.1	More Details
CVE-2024-27194	Cross-Site Request Forgery (CSRF) vulnerability in Andrei Ivasiuc Fontific I Google Fonts allows Stored XSS.This issue affects Fontific I Google Fonts: from n/a through 0.1.6.	7.1	More Details
CVE-2024-27192	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Scott Reilly Configure SMTP allows Reflected XSS.This issue affects Configure SMTP: from n/a through 3.1.	7.1	More Details
CVE-2024-27959	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Wpexpertsio WC Shop Sync – Integrate Square and WooCommerce for Seamless Shop Management allows Reflected XSS.This issue affects WC Shop Sync – Integrate Square and WooCommerce for Seamless Shop Management: from n/a through 4.2.9.	7.1	More Details
CVE-2024-2598	Vulnerability in AMSS++ version 4.31, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /amssplus/modules/book/main/select_send_2.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	7.1	More Details
CVE-2024-27952	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Codeus Advanced Sermons allows Reflected XSS.This issue affects Advanced Sermons: from n/a through 3.2.	7.1	More Details
CVE-2024-29091	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Dnesscarkey WP Armour – Honeypot Anti Spam allows Reflected XSS.This issue affects WP Armour – Honeypot Anti Spam: from n/a through 2.1.13.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2593	Vulnerability in AMSS++ version 4.31, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /amssplus/modules/book/main/bookdetail_group.php, in the 'b_id' parameter. This vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	7.1	More Details
CVE-2024-2594	Vulnerability in AMSS++ version 4.31, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /amssplus/admin/index.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	7.1	More Details
CVE-2024-2595	Vulnerability in AMSS++ version 4.31, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /amssplus/modules/book/main/bookdetail_khet_person.php, in the 'b_id' parameter. This vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	7.1	More Details
CVE-2024-29092	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Maciej Bis Permalink Manager Lite allows Reflected XSS.This issue affects Permalink Manager Lite: from n/a through 2.4.3.	7.1	More Details
CVE-2024-29094	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in HasThemes HT Easy GA4 (Google Analytics 4) allows Stored XSS.This issue affects HT Easy GA4 (Google Analytics 4): from n/a through 1.1.7.	7.1	More Details
CVE-2024-2596	Vulnerability in AMSS++ version 4.31, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /amssplus/modules/mail/main/select_send.php, in multiple parameters. This vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	7.1	More Details
CVE-2024-2597	Vulnerability in AMSS++ version 4.31, which does not sufficiently encode user-controlled input, resulting in a Cross-Site Scripting (XSS) vulnerability through /amssplus/modules/book/main/bookdetail_school_person.php, in the 'b_id' parameter. This vulnerability could allow a remote attacker to send a specially crafted URL to an authenticated user and steal their session cookie credentials.	7.1	More Details
CVE-2024-27998	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in UkrSolution Barcode Scanner with Inventory & Order Manager allows Reflected XSS.This issue affects Barcode Scanner with Inventory & Order Manager: from n/a through 1.5.3.	7.1	More Details
CVE-2023-44090	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Pandora FMS on all allows CVE-2008-5817. This vulnerability allowed SQL changes to be made to several files in the Grafana module. This issue affects Pandora FMS: from 700 through <776.	6.8	More Details
CVE-2023-7003	The AES key utilized in the pairing process between a lock using Sciener firmware and a wireless keypad is not unique, and can be reused to compromise other locks using the Sciener firmware.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35191	Uncontrolled resource consumption for some Intel(R) SPS firmware versions may allow a privileged user to potentially enable denial of service via network access.	6.8	More Details
CVE-2023-41793	: Path Traversal vulnerability in Pandora FMS on all allows Path Traversal. This vulnerability allowed changing directories and creating files and downloading them outside the allowed directories. This issue affects Pandora FMS: from 700 through <776.	6.7	More Details
CVE-2023-32633	Improper input validation in the Intel(R) CSME installer software before version 2328.5.5.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2023-28389	Incorrect default permissions in some Intel(R) CSME installer software before version 2328.5.5.0 may allow an authenticated user to potentially enable escalation of privilege via local access.	6.7	More Details
CVE-2024-25649	In Delinea PAM Secret Server 11.4, it is possible for an attacker (with Administrator access to the Secret Server machine) to read the following data from a memory dump: the decrypted master key, database credentials (when SQL Server Authentication is enabled), the encryption key of RabbitMQ queue messages, and session cookies.	6.7	More Details
CVE-2024-28283	There is stack-based buffer overflow vulnerability in pc_change_act function in Linksys E1000 router firmware version v.2.1.03 and before, leading to remote code execution.	6.7	More Details
CVE-2024-1605	BMC Control-M branches 9.0.20 and 9.0.21 upon user login load all Dynamic Link Libraries (DLL) from a directory that grants Write and Read permissions to all users. Leveraging it leads to loading of a potentially malicious libraries, which will execute with the application's privileges. Fix for 9.0.20 branch was released in version 9.0.20.238. Fix for 9.0.21 branch was released in version 9.0.21.201.	6.6	More Details
CVE-2023-6725	An access-control flaw was found in the OpenStack Designate component where private configuration information including access keys to BIND were improperly made world readable. A malicious attacker with access to any container could exploit this flaw to access sensitive information.	6.6	More Details
CVE-2024-0054	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX APIs local_list.cgi, create_overlay.cgi and irissetup.cgi was vulnerable for file globbing which could lead to a resource exhaustion attack. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	6.5	More Details
CVE-2024-29122	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Foliovision: Making the web work for you FV Flowplayer Video Player allows Stored XSS.This issue affects FV Flowplayer Video Player: from n/a through 7.5.41.7212.	6.5	More Details
CVE-2024-29104	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zimma Ltd. Ticket Tailor allows Stored XSS.This issue affects Ticket Tailor: from n/a through 1.10.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29141	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PDF Embedder allows Stored XSS.This issue affects PDF Embedder: from n/a through 4.6.4.	6.5	More Details
CVE-2024-28447	Shenzhen Libituo Technology Co., Ltd LBT-T300-mini1 v1.2.9 was discovered to contain a buffer overflow via lan_ipaddr parameters at /apply.cgi.	6.5	More Details
CVE-2024-25097	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ThemeNcode LLC TNC PDF viewer allows Stored XSS.This issue affects TNC PDF viewer: from n/a through 2.8.0.	6.5	More Details
CVE-2024-0365	The Fancy Product Designer WordPress plugin before 6.1.5 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by adminstrators.	6.5	More Details
CVE-2024-29134	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Themefic Tourfic allows Stored XSS.This issue affects Tourfic: from n/a through 2.11.8.	6.5	More Details
CVE-2024-2481	A vulnerability, which was classified as critical, was found in Surya2Developer Hostel Management System 1.0. Affected is an unknown function of the file /admin/manage-students.php. The manipulation of the argument del leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-256890 is the identifier assigned to this vulnerability.	6.5	More Details
CVE-2024-29143	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Cozmoslabs, sareiodata Passwordless Login passwordless-login allows Stored XSS.This issue affects Passwordless Login: from n/a through 1.1.2.	6.5	More Details
CVE-2024-0055	Sandro Poppi, member of the AXIS OS Bug Bounty Program, has found that the VAPIX APIs mediaclip.cgi and playclip.cgi was vulnerable for file globbing which could lead to a resource exhaustion attack. Axis has released patched AXIS OS versions for the highlighted flaw. Please refer to the Axis security advisory for more information and solution.	6.5	More Details
CVE-2023-32259	Insufficient Granularity of Access Control vulnerability in OpenText™ Service Management Automation X (SMAX), OpenText™ Asset Management X (AMX) allows Exploiting Incorrectly Configured Access Control Security Levels.This issue affects Service Management Automation X (SMAX) versions 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11; and Asset Management X (AMX) versions 2021.08, 2021.11, 2022.05, 2022.11.	6.5	More Details
CVE-2024-1884	This is a Server-Side Request Forgery (SSRF) vulnerability in the PaperCut NG/MF server-side module that allows an attacker to induce the server-side application to make HTTP requests to an arbitrary domain of the attacker's choosing.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32260	Misinterpretation of Input vulnerability in OpenText™ Service Management Automation X (SMAX), OpenText™ Asset Management X (AMX), and OpenText™ Hybrid Cloud Management X (HCMX) products. The vulnerability could allow Input data manipulation.This issue affects Service Management Automation X (SMAX) versions: 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11, 2023.05; Asset Management X (AMX) versions: 2021.08, 2021.11, 2022.05, 2022.11, 2023.05; and Hybrid Cloud Management X (HCMX) versions: 2020.05, 2020.08, 2020.11, 2021.02, 2021.05, 2021.08, 2021.11, 2022.05, 2022.11, 2023.05.	6.5	More Details
CVE-2024-25099	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in David de Boer Paytium: Mollie payment forms & donations allows Stored XSS.This issue affects Paytium: Mollie payment forms & donations: from n/a through 4.4.2.	6.5	More Details
CVE-2024-27085	Discourse is an open source platform for community discussion. In affected versions users that are allowed to invite others can inject arbitrarily large data in parameters used in the invite route. The problem has been patched in the latest version of Discourse. Users are advised to upgrade. Users unable to upgrade should disable invites or restrict access to them using the `invite allowed groups` site setting.	6.5	More Details
CVE-2024-27100	Discourse is an open source platform for community discussion. In affected versions the endpoints for suspending users, silencing users and exporting CSV files weren't enforcing limits on the sizes of the parameters that they accept. This could lead to excessive resource consumption which could render an instance inoperable. A site could be disrupted by either a malicious moderator on the same site or a malicious staff member on another site in the same multisite cluster. This issue is patched in the latest stable, beta and tests-passed versions of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2024-29096	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Matt Manning MJM Clinic.This issue affects MJM Clinic: from n/a through 1.1.22.	6.5	More Details
CVE-2024-29115	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Zaytech Smart Online Order for Clover allows Stored XSS.This issue affects Smart Online Order for Clover: from n/a through 1.5.5.	6.5	More Details
CVE-2024-1668	The Avada	Website Builder For WordPress & WooCommerce theme for WordPress is vulnerable to Sensitive Information Exposure in versions up to and including 7.11.5 via the form entries page. This makes it possible for authenticated attackers, with contributor access and above, to view the contents of all form submissions, including fields that are obfuscated (such as the contact form's "password" field).	6.5	More Details
CVE-2023-7004	The TTLock App does not employ proper verification procedures to ensure that it is communicating with the expected device, allowing for connection to a device that spoofs the MAC address of a lock, which compromises the legitimate locks integrity.	6.5	More Details
CVE-2024-29111	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Webvitaly Sitekit allows Stored XSS.This issue affects Sitekit: from n/a through 1.6.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29118	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Scrollsequence allows Stored XSS.This issue affects Scrollsequence: from n/a through 1.5.4.	6.5	More Details
CVE-2024-25593	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Basix NEX-Forms – Ultimate Form Builder allows Stored XSS.This issue affects NEX-Forms – Ultimate Form Builder: from n/a through 8.5.5.	6.5	More Details
CVE-2024-29109	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jan-Peter Lambeck & 3UU Shariff Wrapper allows Stored XSS.This issue affects Shariff Wrapper: from n/a through 4.6.10.	6.5	More Details
CVE-2024-29089	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Five Star Plugins Five Star Restaurant Menu allows Stored XSS.This issue affects Five Star Restaurant Menu: from n/a through 2.4.14.	6.5	More Details
CVE-2024-27189	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in catchsquare WP Social Widget allows Stored XSS.This issue affects WP Social Widget: from n/a through 2.2.5.	6.5	More Details
CVE-2024-25936	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SoundCloud Inc., Lawrie Malen SoundCloud Shortcode allows Stored XSS.This issue affects SoundCloud Shortcode: from n/a through 4.0.1.	6.5	More Details
CVE-2024-25934	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FormFacade allows Stored XSS.This issue affects FormFacade: from n/a through 1.0.0.	6.5	More Details
CVE-2024-1763	The Wp Social Login and Register Social Counter plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the /wp_social/v1/ REST API endpoint in all versions up to, and including, 3.0.0. This makes it possible for unauthenticated attackers to enable and disable certain providers for the social share and login features.	6.5	More Details
CVE-2024-25919	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Hiroaki Miyashita Custom Field Template allows Stored XSS.This issue affects Custom Field Template: from n/a through 2.6.	6.5	More Details
CVE-2024-25916	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Joseph C Dolson My Calendar allows Stored XSS.This issue affects My Calendar: from n/a through 3.4.23.	6.5	More Details
CVE-2024-25598	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Livemesh Livemesh Addons for Elementor allows Stored XSS.This issue affects Livemesh Addons for Elementor: from n/a through 8.3.	6.5	More Details
CVE-2024-29114	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in W3 Eden, Inc. Download Manager allows Stored XSS.This issue affects Download Manager: from n/a through 3.2.84.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2416	Cross-Site Request Forgery vulnerability in Movistar's 4G router affecting version ES_WLD71-T1_v2.0.201820. This vulnerability allows an attacker to force an end user to execute unwanted actions in a web application in which they are currently authenticated.	6.5	More Details
CVE-2023-39368	Protection mechanism failure of bus lock regulator for some Intel(R) Processors may allow an unauthenticated user to potentially enable denial of service via network access.	6.5	More Details
CVE-2024-28547	Tenda AC18 V15.03.05.05 has a stack overflow vulnerability in the firewallEn parameter of formSetFirewallCfg function.	6.5	More Details
CVE-2024-28849	follow-redirects is an open source, drop-in replacement for Node's `http` and `https` modules that automatically follows redirects. In affected versions follow-redirects only clears authorization header during cross-domain redirect, but keep the proxy-authentication header which contains credentials too. This vulnerability may lead to credentials leak, but has been addressed in version 1.15.6. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2024-25655	Insecure storage of LDAP passwords in the authentication functionality of AVSystem Unified Management Platform (UMP) 23.07.0.16567~LTS allows members (with read access to the application database) to decrypt the LDAP passwords of users who successfully authenticate to web management via LDAP.	6.5	More Details
CVE-2024-20262	A vulnerability in the Secure Copy Protocol (SCP) and SFTP feature of Cisco IOS XR Software could allow an authenticated, local attacker to create or overwrite files in a system directory, which could lead to a denial of service (DoS) condition. The attacker would require valid user credentials to perform this attack. This vulnerability is due to a lack of proper validation of SCP and SFTP CLI input parameters. An attacker could exploit this vulnerability by authenticating to the device and issuing SCP or SFTP CLI commands with specific parameters. A successful exploit could allow the attacker to impact the functionality of the device, which could lead to a DoS condition. The device may need to be manually rebooted to recover. Note: This vulnerability is exploitable only when a local user invokes SCP or SFTP commands at the Cisco IOS XR CLI. A local user with administrative privileges could exploit this vulnerability remotely.	6.5	More Details
CVE-2023-28746	Information exposure through microarchitectural state after transient execution from some register files for some Intel(R) Atom(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.	6.5	More Details
CVE-2023-50811	An issue discovered in SELESTA Visual Access Manager 4.38.6 allows attackers to modify the “computer” POST parameter related to the ID of a specific reception by POST HTTP request interception. Iterating that parameter, it has been possible to access to the application and take control of many other receptions in addition the assigned one.	6.5	More Details
CVE-2024-1144	Improper access control vulnerability in Devklan's Alma Blog that affects versions 2.1.10 and earlier. This vulnerability could allow an unauthenticated user to access the application's functionalities without the need for credentials.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28193	your_spotify is an open source, self hosted Spotify tracking dashboard. YourSpotify version <1.8.0 allows users to create a public token in the settings, which can be used to provide guest-level access to the information of that specific user in YourSpotify. The /me API endpoint discloses Spotify API access and refresh tokens to guest users. Attackers with access to a public token for guest access to YourSpotify can therefore obtain access to Spotify API tokens of YourSpotify users. As a consequence, attackers may extract profile information, information about listening habits, playlists and other information from the corresponding Spotify profile. In addition, the attacker can pause and resume playback in the Spotify app at will. This issue has been resolved in version 1.8.0. Users are advised to upgrade. There are no known workarounds for this issue.	6.5	More Details
CVE-2024-28323	The bwdates-report-result.php file in Phpgurukul User Registration & Login and User Management System 3.1 contains a potential security vulnerability related to user input validation. The script retrieves user-provided date inputs without proper validation, making it susceptible to SQL injection attacks.	6.5	More Details
CVE-2024-25156	A path traversal vulnerability exists in GoAnywhere MFT prior to 7.4.2 which allows attackers to circumvent endpoint-specific permission checks in the GoAnywhere Admin and Web Clients.	6.5	More Details
CVE-2024-28418	Webedition CMS 9.2.2.0 has a File upload vulnerability via /webEdition/we_cmd.php	6.5	More Details
CVE-2024-28196	your_spotify is an open source, self hosted Spotify tracking dashboard. YourSpotify version < 1.9.0 does not prevent other pages from displaying it in an iframe and is thus vulnerable to clickjacking. Clickjacking can be used to trick an existing user of YourSpotify to trigger actions, such as allowing signup of other users or deleting the current user account. Clickjacking works by opening the target application in an invisible iframe on an attacker-controlled site and luring a victim to visit the attacker page and interacting with it. By positioning elements over the invisible iframe, a victim can be tricked into triggering malicious or destructive actions in the invisible iframe, while they think they interact with a totally different site altogether. When a victim visits an attacker-controlled site while they are logged into YourSpotify, they can be tricked into performing actions on their YourSpotify instance without their knowledge. These actions include allowing signup of other users or deleting the current user account, resulting in a high impact to the integrity of YourSpotify. This issue has been addressed in version 1.9.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2024-29101	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Jegtheme Jeg Elementor Kit allows Stored XSS.This issue affects Jeg Elementor Kit: from n/a through 2.6.2.	6.5	More Details
CVE-2024-29108	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Leevio Happy Addons for Elementor allows Stored XSS.This issue affects Happy Addons for Elementor: from n/a through 3.10.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36238	Insecure Direct Object Reference (IDOR) in Bagisto v.1.5.1 allows an attacker to obtain sensitive information via the invoice ID parameter.	6.5	More Details
CVE-2023-5388	NSS was susceptible to a timing side-channel attack when performing RSA decryption. This attack could potentially allow an attacker to recover the private data. This vulnerability affects Firefox < 124, Firefox ESR < 115.9, and Thunderbird < 115.9.	6.5	More Details
CVE-2024-27439	An error in the evaluation of the fetch metadata headers could allow a bypass of the CSRF protection in Apache Wicket. This issue affects Apache Wicket: from 9.1.0 through 9.16.0, and the milestone releases for the 10.0 series. Apache Wicket 8.x does not support CSRF protection via the fetch metadata headers and as such is not affected. Users are recommended to upgrade to version 9.17.0 or 10.0.0, which fixes the issue.	6.5	More Details
CVE-2024-24683	Improper Input Validation vulnerability in Apache Hop Engine.This issue affects Apache Hop Engine: before 2.8.0. Users are recommended to upgrade to version 2.8.0, which fixes the issue. When Hop Server writes links to the PrepareExecutionPipelineServlet page one of the parameters provided to the user was not properly escaped. The variable not properly escaped is the "id", which is not directly accessible by users creating pipelines making the risk of exploiting this low. This issue only affects users using the Hop Server component and does not directly affect the client.	6.5	More Details
CVE-2024-29107	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPVibes Elementor Addon Elements allows Stored XSS.This issue affects Elementor Addon Elements: from n/a through 1.12.10.	6.5	More Details
CVE-2024-29106	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Leap13 Premium Addons for Elementor allows Stored XSS.This issue affects Premium Addons for Elementor: from n/a through 4.10.16.	6.5	More Details
CVE-2024-29098	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Calameo WP Calameo allows Stored XSS.This issue affects WP Calameo: from n/a through 2.1.7.	6.5	More Details
CVE-2024-27986	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Livemesh Elementor Addons by Livemesh allows Stored XSS.This issue affects Elementor Addons by Livemesh: from n/a through 8.3.5.	6.5	More Details
CVE-2024-23523	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Elementor Pro.This issue affects Elementor Pro: from n/a through 3.19.2.	6.5	More Details
CVE-2023-36483	Authorization bypass can be achieved by session ID prediction in MASmobile Classic Android version 1.16.18 and earlier and MASmobile Classic iOS version 1.7.24 and earlier which allows remote attackers to retrieve sensitive data including customer data, security system status, and event history.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27930	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. An authenticated user can access sensitive fields data from items on which he has read access. This issue has been patched in version 10.0.13.	6.5	More Details
CVE-2024-27937	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. An authenticated user can obtain the email address of all GLPI users. This issue has been patched in version 10.0.13.	6.5	More Details
CVE-2024-1363	The Easy Accordion – Best Accordion FAQ Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'accordion_content_source' attribute in all versions up to, and including, 2.3.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1535	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 4.15.2 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-38723	IBM Maximo Application Suite 7.6.1.3 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 262192.	6.4	More Details
CVE-2024-2308	The ElementInvader Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the button link in the EliSlider in all versions up to, and including, 1.2.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1507	The Prime Slider – Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'title_tags' attribute of the Rubix widget in all versions up to, and including, 3.13.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1497	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form widget addr2_width attribute in all versions up to, and including, 2.10.30 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, 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-2024-1499	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Pricing Table widget in the $settings['title_tags'] parameter in all versions up to, and including, 2.10.30 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1537	The Essential Addons for Elementor – Best Elementor Templates, Widgets, Kits & WooCommerce Builders plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Data Table widget in all versions up to, and including, 5.9.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-6954	The Download Manager Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 3.2.85 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-2024-0326	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Link Wrapper functionality in all versions up to, and including, 4.10.17 due to insufficient input sanitization and output escaping on user supplied links. 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-2024-1080	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the via the heading tag in all versions up to, and including, 2.7.4.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor 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-2024-1074	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the audio widget 'link_url' parameter in all versions up to, and including, 2.7.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor 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-2024-1585	The Metform Elementor Contact Form Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 3.8.3 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 Number	Description	Base Score	Reference
CVE-2024-0700	The Simple Tweet plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Tweet this text value in all versions up to, and including, 1.4.0.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1582	The WP Go Maps (formerly WP Google Maps) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'wpgmza' shortcode in all versions up to, and including, 9.0.32 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-2024-1422	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the modal popup widget's effect setting in all versions up to, and including, 1.12.12 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1239	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the blog post read more button 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 contributor 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-2024-1508	The Prime Slider – Addons For Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'settings['title_tags']' attribute of the Mercury widget in all versions up to, and including, 3.13.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-27098	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. An authenticated user can execute a SSRF based attack using Arbitrary Object Instantiation. This issue has been patched in version 10.0.13.	6.4	More Details
CVE-2024-1296	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's block upload in all versions up to, and including, 2.4.40 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1391	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘eae_custom_overlay_switcher’ attribute of the Thumbnail Slider widget in all versions up to, and including, 1.12.12 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-2024-1392	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'button1_icon' attribute of the Dual Button widget in all versions up to, and including, 1.12.12 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-2024-1393	The Elementor Addon Elements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'icon_align' attribute of the Content Switcher widget in all versions up to, and including, 1.12.12 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-2024-1409	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's [reg-select-role] shortcode in all versions up to, and including, 4.15.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-0897	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the image URL parameter in all versions up to, and including, 2.7.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1293	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the embedded media custom block in all versions up to, and including, 2.4.40 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-6809	The Custom fields shortcode plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's cf shortcode in all versions up to, and including, 0.1 due to insufficient input sanitization and output escaping on user supplied custom post meta values. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1413	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Countdown Timer widget in all versions up to, and including, 2.6.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1414	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Call To Action widget in all versions up to, and including, 2.6.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1291	The Brizy – Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Countdown URL parameter in all versions up to, and including, 2.4.40 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1237	The Elementor Header & Footer Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the flyout_layout attribute in all versions up to, and including, 1.6.24 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor 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-2023-6880	The Visual Composer Website Builder, Landing Page Builder, Custom Theme Builder, Maintenance Mode & Coming Soon Pages plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's custom fields in all versions up to, and including, 45.6.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2042	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Image Accordion widget in all versions up to, and including, 3.0.5 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1234	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via data attribute in all versions up to, and including, 2.6.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, 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-2024-0896	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the button link parameter in all versions up to, and including, 2.7.4.2 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers with contributor access or higher to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1541	The Gutenberg Blocks by Kadence Blocks – Page Builder Features plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the htmlTag attribute in all versions up to, and including, 3.2.23 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor 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-2024-2030	The Database for Contact Form 7, WPforms, Elementor forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 1.3.3 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-2024-2286	The Sky Addons for Elementor (Free Templates Library, Live Copy, Animations, Post Grid, Post Carousel, Particles, Sliders, Chart) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the wrapper link URL value in all versions up to, and including, 2.4.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2126	The Orbit Fox by ThemeIsle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Registration Form widget in all versions up to, and including, 2.10.32 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-2023-50726	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. "Local sync" is an Argo CD feature that allows developers to temporarily override an Application's manifests with locally-defined manifests. Use of the feature should generally be limited to highly-trusted users, since it allows the user to bypass any merge protections in git. An improper validation bug allows users who have `create` privileges but not `override` privileges to sync local manifests on app creation. All other restrictions, including AppProject restrictions are still enforced. The only restriction which is not enforced is that the manifests come from some approved git/Helm/OCI source. The bug was introduced in 1.2.0-rc1 when the local manifest sync feature was added. The bug has been patched in Argo CD versions 2.10.3, 2.9.8, and 2.8.12. Users are advised to upgrade. Users unable to upgrade may mitigate the risk of branch protection bypass by removing `applications, create` RBAC access. The only way to eliminate the issue without removing RBAC access is to upgrade to a patched version.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1997	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'premium_fbchat_app_id' parameter of the Messenger Chat Widget in all versions up to, and including, 2.9.12 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-2024-1996	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's IHover widget link in all versions up to, and including, 2.9.12 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1894	The Burst Statistics – Privacy-Friendly Analytics for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'burst_total_pageviews_count' custom meta field in all versions up to, and including, 1.5.6.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Note that this exploit only functions if the victim has the 'Show Toolbar when viewing site' option enabled in their profile.	6.4	More Details
CVE-2024-1854	The Essential Blocks – Page Builder Gutenberg Blocks, Patterns & Templates plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the blockId parameter in all versions up to, and including, 4.5.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or higher, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2249	The LA-Studio Element Kit for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the LinkWrapper attribute found in several widgets in all versions up to, and including, 1.3.7.4 due to insufficient input sanitization and output escaping the user supplied attribute. 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-2024-1796	The HUSKY – Products Filter for WooCommerce Professional plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'woof' shortcode in all versions up to, and including, 1.3.5.1 due to insufficient input sanitization and output escaping on user supplied attributes such as 'swoof_slug'. 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-2024-1723	The SiteOrigin Widgets Bundle plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several parameters in all versions up to, and including, 1.58.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor access or above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Affected parameters include: $instance['fonts']['title_options']['tag'], $headline_tag, $sub_headline_tag, $feature['icon'].	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38536	HTML injection in OpenText™ Exceed Turbo X affecting version 12.5.1. The vulnerability could result in Cross site scripting.	6.4	More Details
CVE-2024-1604	Improper authorization in the report management and creation module of BMC Control-M branches 9.0.20 and 9.0.21 allows logged-in users to read and make unauthorized changes to any reports available within the application, even without proper permissions. The attacker must know the unique identifier of the report they want to manipulate. Fix for 9.0.20 branch was released in version 9.0.20.238. Fix for 9.0.21 branch was released in version 9.0.21.201.	6.4	More Details
CVE-2024-2293	The Site Reviews plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the user display name in all versions up to, and including, 6.11.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with subscriber 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-2024-1806	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcode(s) in all versions up to, and including, 4.15.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1680	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Image Settings URL of the Banner, Team Members, and Image Scroll widgets in all versions up to, and including, 4.10.21 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-2024-2239	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Premium Magic Scroll module in all versions up to, and including, 2.9.12 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-2024-2028	The Exclusive Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Covid-19 Stats Widget in all versions up to, and including, 2.6.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2237	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Global Badge module in all versions up to, and including, 2.9.12 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-2024-2238	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Custom Mouse Cursor module in all versions up to, and including, 2.9.12 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-2024-2079	The WPBakery Page Builder Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'per_line_mobile' shortcode in all versions up to, and including, 3.8.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-2399	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 4.10.23 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-2024-2256	The oik plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's shortcodes such as bw_contact_button and bw_button shortcodes in all versions up to, and including, 4.10.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-1684	The Otter Blocks – Gutenberg Blocks, Page Builder for Gutenberg Editor & FSE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the contact form file field CSS metabox in all versions up to, and including, 2.6.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor 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-2024-2000	The Premium Addons PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'navigation_dots' parameter of the Multi Scroll Widget in all versions up to, and including, 2.9.12 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-2024-27974	Cross-site request forgery vulnerability in FUJIFILM printers which implement CentreWare Internet Services or Internet Services allows a remote unauthenticated attacker to alter user information. In the case the user is an administrator, the settings such as the administrator's ID, password, etc. may be altered. As for the details of affected product names, model numbers, and versions, refer to the information provided by the vendor listed under [References].	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2621	A vulnerability was found in Fujian Kelixin Communication Command and Dispatch Platform up to 20240318 and classified as critical. Affected by this issue is some unknown functionality of the file api/client/user/pwd_update.php. The manipulation of the argument uuid leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257198 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-28678	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via the component /dede/article_description_main.php	6.3	More Details
CVE-2024-2517	A vulnerability has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as critical. This vulnerability affects unknown code of the file book_history.php. The manipulation of the argument del_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-256954 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2480	A vulnerability classified as critical was found in MHA Sistemas arMHAzena 9.6.0.0. This vulnerability affects unknown code of the component Executa Page. The manipulation of the argument Companhia/Planta/Agente de/Agente até leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256888. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2478	A vulnerability was found in BradWenqiang HR 2.0. It has been rated as critical. Affected by this issue is the function selectAll of the file /bishe/register of the component Background Management. The manipulation of the argument userName leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-256886 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2516	A vulnerability, which was classified as critical, was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. This affects an unknown part of the file home.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 identifier VDB-256953 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2604	A vulnerability was found in SourceCodester File Manager App 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /endpoint/update-file.php. The manipulation of the argument file leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257182 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2024-28682	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /dede/sys_cache_up.php.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2644	A vulnerability was found in Netentsec NS-ASG Application Security Gateway 6.3. It has been rated as critical. Affected by this issue is some unknown functionality of the file /protocol/firewall/addfirewall.php. The manipulation of the argument FireWallTableArray leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257282 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2620	A vulnerability has been found in Fujian Kelixin Communication Command and Dispatch Platform up to 20240318 and classified as critical. Affected by this vulnerability is an unknown functionality of the file api/client/down_file.php. The manipulation of the argument uuid leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257197 was assigned to this vulnerability.	6.3	More Details
CVE-2024-2418	A vulnerability was found in SourceCodester Best POS Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /view_order.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256705 was assigned to this vulnerability.	6.3	More Details
CVE-2024-28417	Webedition CMS 9.2.2.0 has a Stored XSS vulnerability via /webEdition/we_cmd.php.	6.3	More Details
CVE-2024-2622	A vulnerability was found in Fujian Kelixin Communication Command and Dispatch Platform up to 20240318. It has been classified as critical. This affects an unknown part of the file /api/client/editemedia.php. The manipulation of the argument number/enterprise_uuid 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 associated identifier of this vulnerability is VDB-257199.	6.3	More Details
CVE-2024-29097	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PickPlugins User profile allows Stored XSS.This issue affects User profile: from n/a through 2.0.20.	6.3	More Details
CVE-2024-2522	A vulnerability classified as critical has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. This affects an unknown part of the file /admin/booktime.php. The manipulation of the argument room_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 associated identifier of this vulnerability is VDB-256959. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2555	A vulnerability was found in SourceCodester Employee Task Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file update-admin.php. The manipulation of the argument admin_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-257054 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47154	The Net::CIDR::Lite module before 0.22 for Perl does not properly consider extraneous zero characters at the beginning of an IP address string, which (in some situations) allows attackers to bypass access control that is based on IP addresses.	6.3	More Details
CVE-2024-2532	A vulnerability classified as critical was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected by this vulnerability is an unknown functionality of the file /admin/update-users.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256969 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2531	A vulnerability classified as critical has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected is an unknown function of the file /admin/update-rooms.php. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256968. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2520	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /admin/bookdate.php. The manipulation of the argument room_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256957 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-1883	This is a reflected cross site scripting vulnerability in the PaperCut NG/MF application server. An attacker can exploit this weakness by crafting a malicious URL that contains a script. When an unsuspecting user clicks on this malicious link, it could potentially lead to limited loss of confidentiality, integrity or availability.	6.3	More Details
CVE-2024-2561	A vulnerability, which was classified as critical, has been found in 74CMS 3.28.0. Affected by this issue is the function sendCompanyLogo of the file /controller/company/Index.php#sendCompanyLogo of the component Company Logo Handler. The manipulation of the argument imgBase64 leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257060.	6.3	More Details
CVE-2024-2529	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/rooms.php. The manipulation leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-256966 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2556	A vulnerability was found in SourceCodester Employee Task Management System 1.0. It has been classified as critical. This affects an unknown part of the file attendance-info.php. The manipulation of the argument user_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 associated identifier of this vulnerability is VDB-257055.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2528	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/update-rooms.php. The manipulation of the argument room_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 identifier VDB-256965 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2646	A vulnerability classified as critical was found in Netentsec NS-ASG Application Security Gateway 6.3. This vulnerability affects unknown code of the file /vpnweb/index.php?para=index. The manipulation of the argument check_VirtualSiteId leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257284. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-2527	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/rooms.php. The manipulation of the argument room_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256964. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-23672	Denial of Service via incomplete cleanup vulnerability in Apache Tomcat. It was possible for WebSocket clients to keep WebSocket connections open leading to increased resource consumption.This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.0-M16, from 10.1.0-M1 through 10.1.18, from 9.0.0-M1 through 9.0.85, from 8.5.0 through 8.5.98. Users are recommended to upgrade to version 11.0.0-M17, 10.1.19, 9.0.86 or 8.5.99 which fix the issue.	6.3	More Details
CVE-2024-2562	A vulnerability, which was classified as critical, was found in PandaXGO PandaX up to 20240310. This affects the function InsertRole of the file /apps/system/services/role_menu.go. The manipulation of the argument roleKey leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257061 was assigned to this vulnerability.	6.3	More Details
CVE-2024-2564	A vulnerability was found in PandaXGO PandaX up to 20240310 and classified as critical. This issue affects the function ExportUser of the file /apps/system/api/user.go. The manipulation of the argument filename leads to path traversal: '../filedir'. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257063.	6.3	More Details
CVE-2024-2524	A vulnerability, which was classified as critical, has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. This issue affects some unknown processing of the file /admin/receipt.php. The manipulation of the argument room_id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256961 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2565	A vulnerability was found in PandaXGO PandaX up to 20240310. It has been classified as critical. Affected is an unknown function of the file /apps/system/router/upload.go of the component File Extension Handler. The manipulation of the argument file leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257064.	6.3	More Details
CVE-2024-2554	A vulnerability has been found in SourceCodester Employee Task Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file update-employee.php. The manipulation of the argument admin_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257053 was assigned to this vulnerability.	6.3	More Details
CVE-2024-2534	A vulnerability, which was classified as critical, was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. This affects an unknown part of the file /admin/users.php. The manipulation of the argument user_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 associated identifier of this vulnerability is VDB-256971. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2021-38938	IBM Host Access Transformation Services (HATS) 9.6 through 9.6.1.4 and 9.7 through 9.7.0.3 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 210989.	6.2	More Details
CVE-2024-0450	An issue was found in the CPython `zipfile` module affecting versions 3.12.1, 3.11.7, 3.10.13, 3.9.18, and 3.8.18 and prior. The zipfile module is vulnerable to “quoted-overlap” zip-bombs which exploit the zip format to create a zip-bomb with a high compression ratio. The fixed versions of CPython makes the zipfile module reject zip archives which overlap entries in the archive.	6.2	More Details
CVE-2024-28623	RiteCMS v3.0.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component main_menu/edit_section.	6.1	More Details
CVE-2023-7015	The File Manager Pro plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tb' parameter in all versions up to, and including, 8.3.4 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-28668	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via the component /dede/mychannel_add.php	6.1	More Details
CVE-2024-0711	The Buttons Shortcode and Widget WordPress plugin through 1.16 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22655	Protection mechanism failure in some 3rd and 4th Generation Intel(R) Xeon(R) Processors when using Intel(R) SGX or Intel(R) TDX may allow a privileged user to potentially enable escalation of privilege via local access.	6.1	More Details
CVE-2024-21504	Versions of the package livewire/livewire from 3.3.5 and before 3.4.9 are vulnerable to Cross-site Scripting (XSS) when a page uses [Url] for a property. An attacker can inject HTML code in the context of the user's browser session by crafting a malicious link and convincing the user to click on it.	6.1	More Details
CVE-2024-28430	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via the component /dede/catalog_edit.php.	6.1	More Details
CVE-2024-28667	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via the component /dede/templets_one_edit.php	6.1	More Details
CVE-2024-0973	The Widget for Social Page Feeds WordPress plugin before 6.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	6.1	More Details
CVE-2024-24156	Cross Site Scripting (XSS) vulnerability in Gnuboard g6 before Github commit 58c737a263ac0c523592fd87ff71b9e3c07d7cf5, allows remote attackers execute arbitrary code via the wr_content parameter.	6.1	More Details
CVE-2024-1331	The Team Members WordPress plugin before 5.3.2 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the author role and above to perform Stored Cross-Site Scripting attacks.	6.1	More Details
CVE-2024-28670	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /dede/freelist_main.php.	6.1	More Details
CVE-2024-2633	A Cross-Site Scripting Vulnerability has been found on Meta4 HR affecting version 819.001.022 and earlier. The endpoint '/sitetest/english/dumpenv.jsp' is vulnerable to XSS attack by 'lang' query, i.e. '/sitetest/english/dumpenv.jsp?snoop=yes&lang=%27%3Cimg%20src/onerror=alert(1)%3E&params'.	6.1	More Details
CVE-2024-2445	Mattermost Jira plugin versions shipped with Mattermost versions 8.1.x before 8.1.10, 9.2.x before 9.2.6, 9.3.x before 9.3.2, and 9.4.x before 9.4.3 fail to escape user-controlled outputs when generating HTML pages, which allows an attacker to perform reflected cross-site scripting attacks against the users of the Mattermost server.	6.1	More Details
CVE-2024-1383	The WPvivid Backup for MainWP plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 0.9.32 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1691	The Otter Blocks – Gutenberg Blocks, Page Builder for Gutenberg Editor & FSE PRO plugin for WordPress is vulnerable to Stored Cross-Site Scripting via file upload form, which allows SVG uploads, in all versions up to, and including, 2.6.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. Note that the patch in 2.6.4 allows SVG uploads but the uploaded SVG files are sanitized.	6.1	More Details
CVE-2024-0591	The wpDataTables – WordPress Data Table, Dynamic Tables & Table Charts Plugin plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'A' parameter in all versions up to, and including, 3.4.2.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-1365	The YML for Yandex Market plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the feed_id parameter in all versions up to, and including, 4.2.3 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-1484	The Booking for Appointments and Events Calendar – Amelia plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the date parameters in all versions up to, and including, 1.0.98 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-27757	flusity CMS through 2.45 allows tools/addons_model.php Gallery Name XSS. The reporter indicates that this product "ceased its development as of February 2024."	6.1	More Details
CVE-2024-2242	The Contact Form 7 plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘active-tab’ parameter in all versions up to, and including, 5.9 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-28676	DedeCMS v5.7 was discovered to contain a cross-site scripting (XSS) vulnerability via /dede/article_edit.php.	6.1	More Details
CVE-2024-22475	Cross-site request forgery vulnerability in multiple printers and scanners which implement Web Based Management provided by BROTHER INDUSTRIES, LTD. allows a remote unauthenticated attacker to perform unintended operations on the affected product. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28677	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /dede/article_keywords_main.php.	6.1	More Details
CVE-2024-28734	Cross Site Scripting vulnerability in Unit4 Financials by Coda prior to 2023Q4 allows a remote attacker to run arbitrary code via a crafted GET request using the cols parameter.	6.1	More Details
CVE-2024-28679	DedeCMS v5.7 was discovered to contain a cross-site scripting (XSS) vulnerability via Photo Collection.	6.1	More Details
CVE-2024-2634	A Cross-Site Scripting Vulnerability has been found on Meta4 HR affecting version 819.001.022 and earlier. The endpoint '/sse_generico/generico_login.jsp' is vulnerable to XSS attack via 'lang' query, i.e. '/sse_generico/generico_login.jsp?lang=%27%3balert(%27BLEUSS%27)%2f%2f&params='.	6.1	More Details
CVE-2024-28680	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /dede/diy_add.php.	6.1	More Details
CVE-2023-40277	An issue was discovered in OpenClinic GA 5.247.01. A Reflected Cross-Site Scripting (XSS) vulnerability has been discovered in the login.jsp message parameter.	6.1	More Details
CVE-2024-28681	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /dede/plus_edit.php.	6.1	More Details
CVE-2023-47699	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 270974.	6.1	More Details
CVE-2024-2610	Using a markup injection an attacker could have stolen nonce values. This could have been used to bypass strict content security policies. This vulnerability affects Firefox < 124, Firefox ESR < 115.9, and Thunderbird < 115.9.	6.1	More Details
CVE-2024-2609	The permission prompt input delay could expire while the window is not in focus. This makes it vulnerable to clickjacking by malicious websites. This vulnerability affects Firefox < 124, Firefox ESR < 115.10, and Thunderbird < 115.10.	6.1	More Details
CVE-2024-0976	The WP Event Manager – Events Calendar, Registrations, Sell Tickets with WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the plugin parameter in all versions up to, and including, 3.1.41 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-2307	A flaw was found in osbuild-composer. A condition can be triggered that disables GPG verification for package repositories, which can expose the build phase to a Man-in-the-Middle attack, allowing untrusted code to be installed into an image being built.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28683	DedeCMS v5.7 was discovered to contain a cross-site scripting (XSS) vulnerability via create file.	6.1	More Details
CVE-2024-28250	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Starting in version 1.14.0 and prior to versions 1.14.8 and 1.15.2, In Cilium clusters with WireGuard enabled and traffic matching Layer 7 policies Wireguard-eligible traffic that is sent between a node's Envoy proxy and pods on other nodes is sent unencrypted and Wireguard-eligible traffic that is sent between a node's DNS proxy and pods on other nodes is sent unencrypted. This issue has been resolved in Cilium 1.14.8 and 1.15.2 in in native routing mode (`routingMode=native`) and in Cilium 1.14.4 in tunneling mode (`routingMode=tunnel`). Not that in tunneling mode, `encryption.wireguard.encapsulate` must be set to `true`. There is no known workaround for this issue.	6.1	More Details
CVE-2023-47162	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 270973.	6.1	More Details
CVE-2024-28249	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.13.13, 1.14.8, and 1.15.2, in Cilium clusters with IPsec enabled and traffic matching Layer 7 policies, IPsec-eligible traffic between a node's Envoy proxy and pods on other nodes is sent unencrypted and IPsec-eligible traffic between a node's DNS proxy and pods on other nodes is sent unencrypted. This issue has been resolved in Cilium 1.15.2, 1.14.8, and 1.13.13. There is no known workaround for this issue.	6.1	More Details
CVE-2024-27997	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Visualcomposer Visual Composer Website Builder allows Stored XSS.This issue affects Visual Composer Website Builder: from n/a through 45.6.0.	5.9	More Details
CVE-2024-29105	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Timersys WP Popups allows Stored XSS.This issue affects WP Popups: from n/a through 2.1.5.5.	5.9	More Details
CVE-2024-25592	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPMU DEV Broken Link Checker allows Stored XSS.This issue affects Broken Link Checker: from n/a through 2.2.3.	5.9	More Details
CVE-2024-25596	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Doofinder Doofinder for WooCommerce allows Stored XSS.This issue affects Doofinder for WooCommerce: from n/a through 2.1.8.	5.9	More Details
CVE-2024-25650	Insecure key exchange between Delinea PAM Secret Server 11.4 and the Distributed Engine 8.4.3 allows a PAM administrator to obtain the Symmetric Key (used to encrypt RabbitMQ messages) via crafted payloads to the /pre-authenticate, /authenticate, and /execute-and-respond REST API endpoints. This makes it possible for a PAM administrator to impersonate the Engine and exfiltrate sensitive information from the messages published in the RabbitMQ exchanges, without being audited in the application.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29124	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in AAM Advanced Access Manager allows Stored XSS.This issue affects Advanced Access Manager: from n/a through 6.9.20.	5.9	More Details
CVE-2024-27996	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Survey Maker team Survey Maker allows Stored XSS.This issue affects Survey Maker: from n/a through 4.0.5.	5.9	More Details
CVE-2024-29140	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Matt Manning MJM Clinic allows Stored XSS.This issue affects MJM Clinic: from n/a through 1.1.22.	5.9	More Details
CVE-2024-25101	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in yonifre Maspik – Spam Blacklist allows Stored XSS.This issue affects Maspik – Spam Blacklist: from n/a through 0.10.6.	5.9	More Details
CVE-2024-29112	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Marketing Robot WooCommerce Google Feed Manager allows Stored XSS.This issue affects WooCommerce Google Feed Manager: from n/a through 2.2.0.	5.9	More Details
CVE-2024-29095	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Paul Ryley Site Reviews allows Stored XSS.This issue affects Site Reviews: from n/a through 6.11.6.	5.9	More Details
CVE-2024-25656	Improper input validation in AVSystem Unified Management Platform (UMP) 23.07.0.16567~LTS can result in unauthenticated CPE (Customer Premises Equipment) devices storing arbitrarily large amounts of data during registration. This can potentially lead to DDoS attacks on the application database and, ultimately, affect the entire product.	5.9	More Details
CVE-2023-47147	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 could allow an attacker to overwrite a log message under specific conditions. IBM X-Force ID: 270598.	5.9	More Details
CVE-2024-2605	An attacker could have leveraged the Windows Error Reporter to run arbitrary code on the system escaping the sandbox. *Note:* This issue only affected Windows operating systems. Other operating systems are unaffected. This vulnerability affects Firefox < 124, Firefox ESR < 115.9, and Thunderbird < 115.9.	5.9	More Details
CVE-2024-20322	A vulnerability in the access control list (ACL) processing on Pseudowire interfaces in the ingress direction of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to improper assignment of lookup keys to internal interface contexts. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to access resources behind the affected device that were supposed to be protected by a configured ACL.	5.8	More Details
CVE-2024-28039	Improper restriction of XML external entity references vulnerability exists in FitNesse all releases, which allows a remote unauthenticated attacker to obtain sensitive information, alter data, or cause a denial-of-service (DoS) condition.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20315	A vulnerability in the access control list (ACL) processing on MPLS interfaces in the ingress direction of Cisco IOS XR Software could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to improper assignment of lookup keys to internal interface contexts. An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to access resources behind the affected device that were supposed to be protected by a configured ACL.	5.8	More Details
CVE-2024-1146	Cross-Site Scripting vulnerability in Devklan's Alma Blog that affects versions 2.1.10 and earlier. This vulnerability could allow an attacker to store a malicious JavaScript payload within the application by adding the payload to 'Community Description' or 'Community Rules'.	5.8	More Details
CVE-2024-2193	A Speculative Race Condition (SRC) vulnerability that impacts modern CPU architectures supporting speculative execution (related to Spectre V1) has been disclosed. An unauthenticated attacker can exploit this vulnerability to disclose arbitrary data from the CPU using race conditions to access the speculative executable code paths.	5.7	More Details
CVE-2024-28446	Shenzhen Libituo Technology Co., Ltd LBT-T300-mini1 v1.2.9 was discovered to contain a buffer overflow via lan_netmask parameter at /apply.cgi.	5.7	More Details
CVE-2024-28251	Querybook is a Big Data Querying UI, combining collocated table metadata and a simple notebook interface. Querybook's datadocs functionality works by using a Websocket Server. The client talks to this WSS whenever updating/deleting/reading any cells as well as for watching the live status of query executions. Currently the CORS setting allows all origins, which could result in cross-site websocket hijacking and allow attackers to read/edit/remove datadocs of the user. This issue has been addressed in version 3.32.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.6	More Details
CVE-2024-20762	Animate versions 24.0, 23.0.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
	In the Linux kernel, the following vulnerability has been resolved: ip6_tunnel: fix NEXTHDR_FRAGMENT handling in ip6_tnl_parse_tlv_enc_lim() syzbot pointed out [1] that NEXTHDR_FRAGMENT handling is broken. Reading frag_off can only be done if we pulled enough bytes to skb->head. Currently we might access garbage. [1] BUG: KMSAN: uninit-value in ip6_tnl_parse_tlv_enc_lim+0x94f/0xbb0 ip6_tnl_parse_tlv_enc_lim+0x94f/0xbb0 ipxip6_tnl_xmit net/ipv6/ip6_tunnel.c:1326 [inline] ip6_tnl_start_xmit+0xab2/0x1a70 net/ipv6/ip6_tunnel.c:1432 __netdev_start_xmit include/linux/netdevice.h:4940 [inline] netdev_start_xmit include/linux/netdevice.h:4954 [inline] xmit_one net/core/dev.c:3548 [inline] dev_hard_start_xmit+0x247/0xa10 net/core/dev.c:3564 __dev_queue_xmit+0x33b8/0x5130 net/core/dev.c:4349 dev_queue_xmit include/linux/netdevice.h:3134 [inline] neigh_connected_output+0x569/0x660 net/core/neighbour.c:1592 neigh_output include/net/neighbour.h:542 [inline] ip6_finish_output2+0x23a9/0x2b30 net/ipv6/ip6_output.c:137		

CVE Number	Description	Base Score	Reference
	ip6_finish_output+0x855/0x12b0 net/ipv6/ip6_output.c:222 NF_HOOK_COND include/linux/netfilter.h:303 [inline] ip6_output+0x323/0x610 net/ipv6/ip6_output.c:243 dst_output include/net/dst.h:451 [inline] ip6_local_out+0xe9/0x140		
CVE-2024-26633	net/ipv6/output_core.c:155 ip6_send_skb net/ipv6/ip6_output.c:1952 [inline] ip6_push_pending_frames+0x1f9/0x560 net/ipv6/ip6_output.c:1972 rawv6_push_pending_frames+0xbe8/0xdf0 net/ipv6/raw.c:582 rawv6_sendmsg+0x2b66/0x2e70 net/ipv6/raw.c:920 inet_sendmsg+0x105/0x190 net/ipv4/af_inet.c:847 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg net/socket.c:745 [inline] ____sys_sendmsg+0x9c2/0xd60 net/socket.c:2584 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2638 __sys_sendmsg net/socket.c:2667 [inline] __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] __x64_sys_sendmsg+0x307/0x490 net/socket.c:2674 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0x44/0x110 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Uninit was created at: slab_post_alloc_hook+0x129/0xa70 mm/slab.h:768 slab_alloc_node mm/slub.c:3478 [inline] __kmem_cache_alloc_node+0x5c9/0x970 mm/slub.c:3517 __do_kmalloc_node mm/slab_common.c:1006 [inline] __kmalloc_node_track_caller+0x118/0x3c0 mm/slab_common.c:1027 kmalloc_reserve+0x249/0x4a0 net/core/skbuff.c:582 pskb_expand_head+0x226/0x1a00 net/core/skbuff.c:2098 __pskb_pull_tail+0x13b/0x2310 net/core/skbuff.c:2655 pskb_may_pull_reason include/linux/skbuff.h:2673 [inline] pskb_may_pull include/linux/skbuff.h:2681 [inline] ip6_tnl_parse_tlv_enc_lim+0x901/0xbb0 net/ipv6/ip6_tunnel.c:408 ipxip6_tnl_xmit net/ipv6/ip6_tunnel.c:1326 [inline] ip6_tnl_start_xmit+0xab2/0x1a70 net/ipv6/ip6_tunnel.c:1432 __netdev_start_xmit include/linux/netdevice.h:4940 [inline] netdev_start_xmit include/linux/netdevice.h:4954 [inline] xmit_one net/core/dev.c:3548 [inline] dev_hard_start_xmit+0x247/0xa10 net/core/dev.c:3564 __dev_queue_xmit+0x33b8/0x5130 net/core/dev.c:4349 dev_queue_xmit include/linux/netdevice.h:3134 [inline] neigh_connected_output+0x569/0x660 net/core/neighbour.c:1592 neigh_output include/net/neighbour.h:542 [inline] ip6_finish_output2+0x23a9/0x2b30 net/ipv6/ip6_output.c:137 ip6_finish_output+0x855/0x12b0 net/ipv6/ip6_output.c:222 NF_HOOK_COND include/linux/netfilter.h:303 [inline] ip6_output+0x323/0x610 net/ipv6/ip6_output.c:243 dst_output include/net/dst.h:451 [inline] ip6_local_out+0xe9/0x140 net/ipv6/output_core.c:155 ip6_send_skb net/ipv6/ip6_output.c:1952 [inline] ip6_push_pending_frames+0x1f9/0x560 net/ipv6/ip6_output.c:1972 rawv6_push_pending_frames+0xbe8/0xdf0 net/ipv6/raw.c:582 rawv6_sendmsg+0x2b66/0x2e70 net/ipv6/raw.c:920 inet_sendmsg+0x105/0x190 net/ipv4/af_inet.c:847 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg net/socket.c:745 [inline] ____sys_sendmsg+0x9c2/0xd60 net/socket.c:2584 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2638 __sys_sendmsg net/socket.c:2667 [inline] __do_sys_sendms ---truncated---	5.5	More Details
CVE-2024-20763	Animate versions 24.0, 23.0.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
	In the Linux kernel, the following vulnerability has been resolved: drivers/thermal/loongson2_thermal: Fix incorrect PTR_ERR() judgment PTR_ERR() returns -ENODEV when thermal-zones are undefined, and we need -ENODEV as the right value for comparison. Otherwise, tz->type is NULL when thermal-zones is undefined, resulting in the following error: [12.290030] CPU 1 Unable to handle kernel paging request at virtual address ffffffffffffffff1, era == 900000000355f410, ra ==		

CVE Number	Description	Base Score	Reference
CVE-2023-52613	90000000031579b8 [12.302877] Oops[#1]: [12.305190] CPU: 1 PID: 181 Comm: systemd-udevd Not tainted 6.6.0-rc7+ #5 [12.312304] pc 900000000355f410 ra 90000000031579b8 tp 90000001069e8000 sp 90000001069eba10 [12.320739] a0 0000000000000000 a1 ffffffffffffffe1 a2 0000000000000014 a3 0000000000000001 [12.329173] a4 90000001069eb990 a5 0000000000000001 a6 0000000000001001 a7 900000010003431c [12.337606] t0 ffffffffffffffe1 t1 54567fd5da9b4fd4 t2 900000010614ec40 t3 00000000000dc901 [12.346041] t4 0000000000000000 t5 0000000000000004 t6 900000010614ee20 t7 900000000d00b790 [12.354472] t8 00000000000dc901 u0 54567fd5da9b4fd4 s9 900000000402ae10 s0 900000010614ec40 [12.362916] s1 90000000039fced0 s2 fffffffffffffed0 s3 fffffffffffffed4 s4 9000000003acc000 [12.362931] s5 0000000000000004 s6 fffffffffffff000 s7 0000000000000490 s8 90000001028b2ec8 [12.362938] ra: 90000000031579b8 thermal_add_hwmon_sysfs+0x258/0x300 [12.386411] ERA: 900000000355f410 strscpy+0xf0/0x160 [12.391626] CRMD: 000000b0 (PLV0 -IE -DA +PG DACF=CC DACM=CC -WE) [12.397898] PRMD: 00000004 (PPLV0 +PIE -PWE) [12.403678] EUEN: 00000000 (-FPE -SXE -ASXE -BTE) [12.409859] ECFG: 00071c1c (LIE=2-4,10-12 VS=7) [12.415882] ESTAT: 00010000 [PIL] (IS= ECode=1 EsubCode=0) [12.415907] BADV: ffffffffffffffe1 [12.415911] PRID: 0014a000 (Loongson-64bit, Loongson-2K1000) [12.415917] Modules linked in: loongson2_thermal(+) vfat fat uio_pdrv_genirq uio fuse zram zsmalloc [12.415950] Process systemd-udevd (pid: 181, threadinfo=00000000358b9718, task=00000000ace72fe3) [12.415961] Stack : 0000000000000dc0 54567fd5da9b4fd4 900000000402ae10 9000000002df9358 [12.415982] fffffffffffffed 0000000000000004 9000000107a10aa8 90000001002a3410 [12.415999] fffffffffffffed fffffffffffffed 9000000107a11268 9000000003157ab0 [12.416016] 9000000107a10aa8 ffffff80020fc0c8 90000001002a3410 fffffffffffffed [12.416032] 0000000000000024 ffffff80020cc1e8 900000000402b2a0 9000000003acc000 [12.416048] 90000001002a3410 0000000000000000 ffffff80020f4030 90000001002a3410 [12.416065] 0000000000000000 9000000002df6808 90000001002a3410 0000000000000000 [12.416081] ffffff80020f4030 0000000000000000 90000001002a3410 9000000002df2ba8 [12.416097] 00000000000000b4 90000001002a34f4 90000001002a3410 0000000000000002 [12.416114] ffffff80020f4030 fffffffffffffff0 90000001002a3410 9000000002df2f30 [12.416131] ... [12.416138] Call Trace: [12.416142] [<900000000355f410>] strscpy+0xf0/0x160 [12.416167] [<90000000031579b8>] thermal_add_hwmon_sysfs+0x258/0x300 [12.416183] [<9000000003157ab0>] devm_thermal_add_hwmon_sysfs+0x50/0xe0 [12.416200] [<ffffff80020cc1e8>] loongson2_thermal_probe+0x128/0x200 [loongson2_thermal] [12.416232] [<9000000002df6808>] platform_probe+0x68/0x140 [12.416249] [<9000000002df2ba8>] really_probe+0xc8/0x3c0 [12.416269] [<9000000002df2f30>] __driver_probe_device+0x90/0x180 [12.416286] [<9000000002df3058>] driver_probe_device+0x38/0x160 [12.416302] [<9000000002df33a8>] __driver_attach+0xa8/0x200 [12.416314] [<9000000002deffec>] bus_for_each_dev+0x8c/0x120 [12.416330] [<9000000002df198c>] bus_add_driver+0x10c/0x2a0 [12.416346] [<9000000002df46b4>] driver_register+0x74/0x160 [12.416358] [<90000000022201a4>] do_one_initcall+0x84/0x220 [12.416372] [<90000000022f3ab8>] do_init_module+0x58/0x2c0 [---truncated---	5.5	More Details
CVE-2023-52615	In the Linux kernel, the following vulnerability has been resolved: hwrng: core - Fix page fault dead lock on mmap-ed hwrng There is a dead-lock in the hwrng device read path. This triggers when the user reads from /dev/hwrng into memory also mmap-ed from /dev/hwrng. The resulting page fault triggers a recursive read which then dead-locks. Fix this by using a stack buffer when calling copy_to_user.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-20764	Animate versions 24.0, 23.0.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-20757	Bridge versions 13.0.5, 14.0.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2024-23298	A logic issue was addressed with improved state management.	5.5	More Details
CVE-2024-1853	Zemana AntiLogger v2.74.204.664 is vulnerable to an Arbitrary Process Termination vulnerability by triggering the 0x80002048 IOCTL code of the zam64.sys and zamguard64.sys drivers.	5.5	More Details
CVE-2024-28429	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via the component /dede/archives_do.php	5.5	More Details
CVE-2023-38575	Non-transparent sharing of return predictor targets between contexts in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.	5.5	More Details
CVE-2024-0313	A malicious insider exploiting this vulnerability can circumvent existing security controls put in place by the organization. On the contrary, if the victim is legitimately using the temporary bypass to reach out to the Internet for retrieving application and system updates, a remote device could target it and undo the bypass, thereby denying the victim access to the update service, causing it to fail.	5.5	More Details
CVE-2024-0312	A malicious insider can uninstall Skyhigh Client Proxy without a valid uninstall password.	5.5	More Details
CVE-2024-0311	A malicious insider can bypass the existing policy of Skyhigh Client Proxy without a valid release code.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47114	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix data corruption by fallocate When fallocate punches holes out of inode size, if original isize is in the middle of last cluster, then the part from isize to the end of the cluster will be zeroed with buffer write, at that time isize is not yet updated to match the new size, if writeback is kicked in, it will invoke ocfs2_writepage()->block_write_full_page() where the pages out of inode size will be dropped. That will cause file corruption. Fix this by zero out eof blocks when extending the inode size. Running the following command with qemu-image 4.2.1 can get a corrupted coverted image file easily. qemu-img convert -p -t none -T none -f qcow2 $qcow_image \ -O qcow2 -o compat=1.1 $qcow_image.conv The usage of fallocate in qemu is like this, it first punches holes out of inode size, then extend the inode size. fallocate(11, FALLOC_FL_KEEP_SIZEIFALLOC_FL_PUNCH_HOLE, 2276196352, 65536) = 0 fallocate(11, 0, 2276196352, 65536) = 0 v1: https://www.spinics.net/lists/linux-fsdevel/msg193999.html v2: https://lore.kernel.org/linux-fsdevel/20210525093034.GB4112@quack2.suse.cz/T/	5.5	More Details
CVE-2021-47126	In the Linux kernel, the following vulnerability has been resolved: ipv6: Fix KASAN: slab-out-of-bounds Read in fib6_nh_flush_exceptions Reported by syzbot: HEAD commit: 90c911ad Merge tag 'fixes' of git://git.kernel.org/pub/scm.. git tree: git://git.kernel.org/pub/scm/linux/kernel/git/torvalds/linux.git master dashboard link: https://syzkaller.appspot.com/bug?extid=123aa35098fd3c000eb7 compiler: Debian clang version 11.0.1-2 == BUG: KASAN: slab-out-of-bounds in fib6_nh_get_excptn_bucket net/ipv6/route.c:1604 [inline] BUG: KASAN: slab-out-of-bounds in fib6_nh_flush_exceptions+0xbd/0x360 net/ipv6/route.c:1732 Read of size 8 at addr ffff8880145c78f8 by task syz-executor.4/17760 CPU: 0 PID: 17760 Comm: syz-executor.4 Not tainted 5.12.0-rc8-syzkaller #0 Call Trace: <IRQ> __dump_stack lib/dump_stack.c:79 [inline] dump_stack+0x202/0x31e lib/dump_stack.c:120 print_address_description+0x5f/0x3b0 mm/kasan/report.c:232 __kasan_report mm/kasan/report.c:399 [inline] kasan_report+0x15c/0x200 mm/kasan/report.c:416 fib6_nh_get_excptn_bucket net/ipv6/route.c:1604 [inline] fib6_nh_flush_exceptions+0xbd/0x360 net/ipv6/route.c:1732 fib6_nh_release+0x9a/0x430 net/ipv6/route.c:3536 fib6_info_destroy_rcu+0xcb/0x1c0 net/ipv6/ip6_fib.c:174 rcu_do_batch kernel/rcu/tree.c:2559 [inline] rcu_core+0x8f6/0x1450 kernel/rcu/tree.c:2794 __do_softirq+0x372/0x7a6 kernel/softirq.c:345 invoke_softirq kernel/softirq.c:221 [inline] __irq_exit_rcu+0x22c/0x260 kernel/softirq.c:422 irq_exit_rcu+0x5/0x20 kernel/softirq.c:434 sysvec_apic_timer_interrupt+0x91/0xb0 arch/x86/kernel/apic/apic.c:1100 </IRQ> asm_sysvec_apic_timer_interrupt+0x12/0x20 arch/x86/include/asm/idtentry.h:632 RIP: 0010:lock_acquire+0x1f6/0x720 kernel/locking/lockdep.c:5515 Code: f6 84 24 a1 00 00 00 02 0f 85 8d 02 00 00 f7 c3 00 02 00 00 49 bd 00 00 00 00 00 fc ff df 74 01 fb 48 c7 44 24 40 0e 36 e0 45 <4b> c7 44 3d 00 00 00 00 00 4b c7 44 3d 09 00 00 00 00 43 c7 44 3d RSP: 0018:ffffc90009e06560 EFLAGS: 00000206 RAX: 1ffff920013c0cc0 RBX: 0000000000000246 RCX: dfffffc0000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffc90009e066e0 R08: dfffffc0000000000 R09: fffffbfff1f992b1 R10: fffffbfff1f992b1 R11: 0000000000000000 R12: 0000000000000000 R13: dfffffc0000000000 R14: 0000000000000000 R15: 1ffff920013c0cb4 rcu_lock_acquire+0x2a/0x30 include/linux/rcupdate.h:267 rcu_read_lock include/linux/rcupdate.h:656 [inline] ext4_get_group_info+0xea/0x340	5.5	More Details

CVE Number	Description	Base Score	Reference
	fs/ext4/ext4.h:3231 ext4_mb_prefetch+0x123/0x5d0 fs/ext4/mballoc.c:2212 ext4_mb_regular_allocator+0x8a5/0x2f80 fs/ext4/mballoc.c:2379 ext4_mb_new_blocks+0xc6e/0x24f0 fs/ext4/mballoc.c:4982 ext4_ext_map_blocks+0x2be3/0x7210 fs/ext4/extents.c:4238 ext4_map_blocks+0xab3/0x1cb0 fs/ext4/inode.c:638 ext4_getblk+0x187/0x6c0 fs/ext4/inode.c:848 ext4_bread+0x2a/0x1c0 fs/ext4/inode.c:900 ext4_append+0x1a4/0x360 fs/ext4/namei.c:67 ext4_init_new_dir+0x337/0xa10 fs/ext4/namei.c:2768 ext4_mkdir+0x4b8/0xc00 fs/ext4/namei.c:2814 vfs_mkdir+0x45b/0x640 fs/namei.c:3819 ovl_do_mkdir fs/overlayfs/overlayfs.h:161 [inline] ovl_mkdir_real+0x53/0x1a0 fs/overlayfs/dir.c:146 ovl_create_real+0x280/0x490 fs/overlayfs/dir.c:193 ovl_workdir_create+0x425/0x600 fs/overlayfs/super.c:788 ovl_make_workdir+0xed/0x1140 fs/overlayfs/super.c:1355 ovl_get_workdir fs/overlayfs/super.c:1492 [inline] ovl_fill_super+0x39ee/0x5370 fs/overlayfs/super.c:2035 mount_nodev+0x52/0xe0 fs/super.c:1413 legacy_get_tree+0xea/0x180 fs/fs_context.c:592 vfs_get_tree+0x86/0x270 fs/super.c:1497 do_new_mount fs/namespace.c:2903 [inline] path_mount+0x196f/0x2be0 fs/namespace.c:3233 do_mount fs/namespace.c:3246 [inline] __do_sys_mount fs/namespace.c:3454 [inline] __se_sys_mount+0x2f9/0x3b0 fs/namespace.c:3431 do_syscall_64+0x2d/0x70 arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x4665f9 Code: ff ff c3 66 2e 0f 1f 84 ---truncated---		
CVE-2024-2611	A missing delay on when pointer lock was used could have allowed a malicious page to trick a user into granting permissions. This vulnerability affects Firefox < 124, Firefox ESR < 115.9, and Thunderbird < 115.9.	5.5	More Details
CVE-2024-2204	Zemana AntiLogger v2.74.204.664 is vulnerable to a Denial of Service (DoS) vulnerability by triggering the 0x80002004 and 0x80002010 IOCTL codes of the zam64.sys and zamguard64.sys drivers.	5.5	More Details
CVE-2023-6525	The ElementsKit Elementor addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the progress bar element attributes in all versions up to, and including, 3.0.3 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with editor-level access, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This primarily affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2024-2431	An issue in the Palo Alto Networks GlobalProtect app enables a non-privileged user to disable the GlobalProtect app in configurations that allow a user to disable GlobalProtect with a passcode.	5.5	More Details
CVE-2024-2180	Zemana AntiLogger v2.74.204.664 is vulnerable to a Memory Information Leak vulnerability by triggering the 0x80002020 IOCTL code of the zam64.sys and zamguard64.sys drivers	5.5	More Details
CVE-2024-24043	Directory Traversal vulnerability in Speedy11CZ MCRPX v.1.4.0 and before allows a local attacker to execute arbitrary code via a crafted file.	5.5	More Details
CVE-2024-22513	djangorestframework-simplejwt version 5.3.1 and before is vulnerable to information disclosure. A user can access web application resources even after their account has been disabled due to missing user validation checks via the for_user method.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28666	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via the component /dede/media_add.php	5.5	More Details
CVE-2024-26032	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable web pages. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable script. This could result in arbitrary code execution in the context of the victim's browser. Exploitation of this issue requires user interaction.	5.4	More Details
CVE-2024-26041	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26040	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26038	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-25657	An open redirect in the Login/Logout functionality of web management in AVSystem Unified Management Platform (UMP) 23.07.0.16567~LTS could allow attackers to redirect authenticated users to malicious websites.	5.4	More Details
CVE-2024-24562	vantage6-UI is the official user interface for the vantage6 server. In affected versions a number of security headers are not set. This issue has been addressed in commit `68dfa6614` which is expected to be included in future releases. Users are advised to upgrade when a new release is made. While an upgrade path is not available users may modify the docker image build to insert the headers into nginx.	5.4	More Details
CVE-2024-26035	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26034	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1038	The Beaver Builder – WordPress Page Builder plugin for WordPress is vulnerable to DOM-Based Reflected Cross-Site Scripting via a 'playground.wordpress.net' parameter in all versions up to, and including, 2.7.4.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	5.4	More Details
CVE-2024-0828	The Play.ht – Make Your Blog Posts Accessible With Text to Speech Audio plugin for WordPress is vulnerable to unauthorized access of functionality due to a missing capability check on several functions in all versions up to, and including, 3.6.4. This makes it possible for authenticated attackers, with subscriber access or higher, to delete, retrieve, or modify post metadata, retrieve posts contents of protected posts, modify conversion data and delete article audio.	5.4	More Details
CVE-2024-1333	The Responsive Pricing Table WordPress plugin before 5.1.11 does not validate and escape some of its Pricing Table options before outputting them back in a page/post where the related shortcode is embed, which could allow users with the author role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details
CVE-2024-26125	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26033	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26124	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26031	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-0592	The Related Posts for WordPress plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 2.2.1. This is due to missing or incorrect nonce validation on the handle_create_link() function. This makes it possible for unauthenticated attackers to add related posts to other posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This ultimately makes it possible for attackers to view draft and password protected posts.	5.4	More Details
CVE-2024-0719	The Tabs Shortcode and Widget WordPress plugin through 1.17 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26030	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-28669	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /dede/freelist_edit.php.	5.4	More Details
CVE-2024-27703	Cross Site Scripting vulnerability in Leantime 3.0.6 allows a remote attacker to execute arbitrary code via the to-do title parameter.	5.4	More Details
CVE-2024-2252	The Droit Elementor Addons – Widgets, Blocks, Templates Library For Elementor Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's widgets in all versions up to, and including, 3.1.5 due to insufficient input sanitization and output escaping on user supplied attributes such as URL. 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.	5.4	More Details
CVE-2023-7085	The Scalable Vector Graphics (SVG) WordPress plugin through 3.4 does not sanitize uploaded SVG files, which could allow users with a role as low as Author to upload a malicious SVG containing XSS payloads.	5.4	More Details
CVE-2024-20768	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-28662	A Cross Site Scripting vulnerability exists in Piwigo before 14.3.0 script because of missing sanitization in create_tag in admin/include/functions.php.	5.4	More Details
CVE-2018-25090	An unauthenticated remote attacker can use an XSS attack due to improper neutralization of input during web page generation. User interaction is required. This leads to a limited impact of confidentiality and integrity but no impact of availability.	5.4	More Details
CVE-2024-20760	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-28517	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 250421.	5.4	More Details
CVE-2024-26028	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28672	DedeCMS v5.7 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /dede/media_edit.php.	5.4	More Details
CVE-2024-26042	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable web pages. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable script. This could result in arbitrary code execution in the context of the victim's browser.	5.4	More Details
CVE-2024-26101	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2023-51521	Cross-Site Request Forgery (CSRF) vulnerability in ExpressTech Quiz And Survey Master.This issue affects Quiz And Survey Master: from n/a through 8.1.18.	5.4	More Details
CVE-2024-26043	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-51486	Cross-Site Request Forgery (CSRF) vulnerability in RedNao WooCommerce PDF Invoice Builder.This issue affects WooCommerce PDF Invoice Builder: from n/a through 1.2.101.	5.4	More Details
CVE-2023-51487	Cross-Site Request Forgery (CSRF) vulnerability in ARI Soft ARI Stream Quiz.This issue affects ARI Stream Quiz: from n/a through 1.2.32.	5.4	More Details
CVE-2024-26080	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable web pages. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable script.	5.4	More Details
CVE-2024-26094	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26096	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26102	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51489	Cross-Site Request Forgery (CSRF) vulnerability in Automattic, Inc. Crowdsignal Dashboard – Polls, Surveys & more.This issue affects Crowdsignal Dashboard – Polls, Surveys & more: from n/a through 3.0.11.	5.4	More Details
CVE-2024-26103	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-26104	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-26105	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-26106	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-2563	A vulnerability has been found in PandaXGO PandaX up to 20240310 and classified as critical. This vulnerability affects the function DeleteImage of the file /apps/system/router/upload.go. The manipulation of the argument fileName with the input ../../../../../../../../../tmp/1.txt leads to path traversal: '../filedir'. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-257062 is the identifier assigned to this vulnerability.	5.4	More Details
CVE-2024-26107	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2024-26118	Adobe Experience Manager versions 6.5.19 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2023-51491	Cross-Site Request Forgery (CSRF) vulnerability in Averta Depicter Slider.This issue affects Depicter Slider: from n/a through 2.0.6.	5.4	More Details
CVE-2024-0871	The Beaver Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the Icon Widget 'fl_builder_data[node_preview][link]' and 'fl_builder_data[settings][link_target]' parameters in all versions up to, and including, 2.7.4.2 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 Number	Description	Base Score	Reference
CVE-2024-26073	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2023-50898	Missing Authorization vulnerability in sirv.Com Sirv.This issue affects Sirv: from n/a through 7.1.2.	5.4	More Details
CVE-2024-26045	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26067	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26065	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26064	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into a webpage. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable script. This could result in arbitrary code execution in the context of the victim's browser. Exploitation of this issue requires user interaction.	5.4	More Details
CVE-2024-26120	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26062	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26061	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26059	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-46182	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 269692.	5.4	More Details
CVE-2024-26056	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26052	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26051	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26069	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	5.4	More Details
CVE-2024-26044	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into a webpage. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable script. This could result in arbitrary code execution in the context of the victim's browser.	5.4	More Details
CVE-2024-0687	The Restrict User Access – Ultimate Membership & Content Protection plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 2.5 via API. This makes it possible for unauthenticated attackers to obtain the contents of posts and pages via API.	5.3	More Details
CVE-2024-0681	The Page Restriction WordPress (WP) – Protect WP Pages/Post plugin for WordPress is vulnerable to information disclosure in all versions up to, and including, 1.3.4. This is due to the plugin not properly restricting access to pages via the REST API when a page has been made private. This makes it possible for unauthenticated attackers to view protected pages. The vendor has decided that they will not implement REST API protection on posts and pages and the restrictions will only apply to the front-end of the site. The vendors solution was to add notices throughout the dashboard and recommends installing the WordPress REST API Authentication plugin for REST API coverage.	5.3	More Details
CVE-2024-0839	The FeedWordPress plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2022.0222 due to missing validation on the user controlled 'guid' key. This makes it possible for unauthenticated attackers to view draft posts that may contain sensitive information.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0631	The Duitku Payment Gateway plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the check_duitku_response function in all versions up to, and including, 2.11.4. This makes it possible for unauthenticated attackers to change the payment status of orders to failed.	5.3	More Details
CVE-2024-25154	Improper URL validation leads to path traversal in FileCatalyst Direct 3.8.8 and earlier allowing an encoded payload to cause the web server to return files located outside of the web root which may lead to data leakage.	5.3	More Details
CVE-2024-0377	The LifterLMS – WordPress LMS Plugin for eLearning plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'process_review' function in all versions up to, and including, 7.5.1. This makes it possible for unauthenticated attackers to publish an unrestricted number of reviews on the site.	5.3	More Details
CVE-2024-2641	A vulnerability was found in Ruijie RG-NBS2009G-P up to 20240305. It has been classified as critical. Affected is an unknown function of the file /system/passwdManage.htm of the component Password Handler. The manipulation leads to improper authorization. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257280. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2023-6969	The User Shortcodes Plus plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 2.0.2 via the user_meta shortcode due to missing validation on a user controlled key. This makes it possible for authenticated attackers, with contributor-level access and above, to retrieve potentially sensitive user meta.	5.3	More Details
CVE-2023-6785	The Download Manager plugin for WordPress is vulnerable to unauthorized file download of files added via the plugin in all versions up to, and including, 3.2.84. This makes it possible for unauthenticated attackers to download files added with the plugin (even when privately published).	5.3	More Details
CVE-2024-27914	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. An unauthenticated user can provide a malicious link to a GLPI administrator in order to exploit a reflected XSS vulnerability. The XSS will only trigger if the administrator navigates through the debug bar. This issue has been patched in version 10.0.13.	5.3	More Details
CVE-2024-26063	Adobe Experience Manager versions 6.5.19 and earlier are affected by an Information Exposure vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to gain unauthorized access to sensitive information, potentially bypassing security measures. Exploitation of this issue does not require user interaction.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-10130	The Team Circle Image Slider With Lightbox plugin for WordPress is vulnerable to Cross-Site Request Forgery in version 1.0. This is due to missing or incorrect nonce validation on the circle_thumbnail_slider_with_lightbox_image_management_func() function. This makes it possible for unauthenticated attackers to edit image data which can be used to inject malicious JavaScript, along with deleting images, and uploading malicious files via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	5.3	More Details
CVE-2024-2412	The disabling function of the user registration page for Heimavista Rpage and Epage is not properly implemented, allowing remote attackers to complete user registration on sites where user registration is supposed to be disabled.	5.3	More Details
CVE-2024-25591	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Benjamin Rojas WP Editor.This issue affects WP Editor: from n/a through 1.2.7.	5.3	More Details
CVE-2024-1083	The Simple Restrict plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.2.6 via the REST API. This makes it possible for authenticated attackers to bypass the plugin's restrictions to extract post titles and content	5.3	More Details
CVE-2024-27351	In Django 3.2 before 3.2.25, 4.2 before 4.2.11, and 5.0 before 5.0.3, the django.utils.text.Truncator.words() method (with html=True) and the truncatewords_html template filter are subject to a potential regular expression denial-of-service attack via a crafted string. NOTE: this issue exists because of an incomplete fix for CVE-2019-14232 and CVE-2023-43665.	5.3	More Details
CVE-2024-22396	An Integer-based buffer overflow vulnerability in the SonicOS via IPSec allows a remote attacker in specific conditions to cause Denial of Service (DoS) and potentially execute arbitrary code by sending a specially crafted IKEv2 payload.	5.3	More Details
CVE-2023-43490	Incorrect calculation in microcode keying mechanism for some Intel(R) Xeon(R) D Processors with Intel(R) SGX may allow a privileged user to potentially enable information disclosure via local access.	5.3	More Details
CVE-2024-1126	The EventPrime – Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the get_attendees_email_by_event_id() function in all versions up to, and including, 3.4.1. This makes it possible for authenticated attackers, with subscriber-level access and above, to to retrieve the attendees list for any event.	5.3	More Details
CVE-2024-24770	vantage6 is an open source framework built to enable, manage and deploy privacy enhancing technologies like Federated Learning and Multi-Party Computation. Much like GHSA-45gq-q4xh-cp53, it is possible to find which usernames exist in vantage6 by calling the API routes `/recover/lost` and `/2fa/lost`. These routes send emails to users if they have lost their password or MFA token. This issue has been addressed in commit `aecfd6d0e` and is expected to ship in subsequent releases. Users are advised to upgrade as soon as a new release is available. There are no known workarounds for this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-23944	Information disclosure in persistent watchers handling in Apache ZooKeeper due to missing ACL check. It allows an attacker to monitor child znodes by attaching a persistent watcher (addWatch command) to a parent which the attacker has already access to. ZooKeeper server doesn't do ACL check when the persistent watcher is triggered and as a consequence, the full path of znodes that a watch event gets triggered upon is exposed to the owner of the watcher. It's important to note that only the path is exposed by this vulnerability, not the data of znode, but since znode path can contain sensitive information like user name or login ID, this issue is potentially critical. Users are recommended to upgrade to version 3.9.2, 3.8.4 which fixes the issue.	5.3	More Details
CVE-2023-51525	Cross-Site Request Forgery (CSRF) vulnerability in Veribo, Roland Murg WP Simple Booking Calendar.This issue affects WP Simple Booking Calendar: from n/a through 2.0.8.4.	5.3	More Details
CVE-2023-50966	erlang-jose (aka JOSE for Erlang and Elixir) through 1.11.6 allow attackers to cause a denial of service (CPU consumption) via a large p2c (aka PBES2 Count) value in a JOSE header.	5.3	More Details
CVE-2024-21824	Improper authentication vulnerability in exists in multiple printers and scanners which implement Web Based Management provided by BROTHER INDUSTRIES, LTD. If this vulnerability is exploited, a network-adjacent user who can access the product may impersonate an administrative user. As for the details of affected product names, model numbers, and versions, refer to the information provided by the respective vendors listed under [References].	5.3	More Details
CVE-2024-24748	Discourse is an open source platform for community discussion. In affected versions an attacker can learn that a secret subcategory exists under a public category which has no public subcategories. The issue is patched in the latest stable, beta and tests-passed version of Discourse. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2024-24827	Discourse is an open source platform for community discussion. Without a rate limit on the POST /uploads endpoint, it makes it easier for an attacker to carry out a DoS attack on the server since creating an upload can be a resource intensive process. Do note that the impact varies from site to site as various site settings like `max_image_size_kb`, `max_attachment_size_kb` and `max_image_megapixels` will determine the amount of resources used when creating an upload. The issue is patched in the latest stable, beta and tests-passed version of Discourse. Users are advised to upgrade. Users unable to upgrade should reduce `max_image_size_kb`, `max_attachment_size_kb` and `max_image_megapixels` as smaller uploads require less resources to process. Alternatively, `client_max_body_size` can be reduced in Nginx to prevent large uploads from reaching the server.	5.3	More Details
CVE-2024-28242	Discourse is an open source platform for community discussion. In affected versions an attacker can learn that secret categories exist when they have backgrounds set. The issue is patched in the latest stable, beta and tests-passed version of Discourse. Users are advised to upgrade. Users unable to upgrade should temporarily remove category backgrounds.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7250	A flaw was found in iperf, a utility for testing network performance using TCP, UDP, and SCTP. A malicious or malfunctioning client can send less than the expected amount of data to the iperf server, which can cause the server to hang indefinitely waiting for the remainder or until the connection gets closed. This will prevent other connections to the server, leading to a denial of service.	5.3	More Details
CVE-2024-24539	FusionPBX before 5.2.0 does not validate a session.	5.3	More Details
CVE-2024-28862	The Ruby One Time Password library (ROTP) is an open source library for generating and validating one time passwords. Affected versions had overly permissive default permissions. Users should patch to version 6.3.0. Users unable to patch may correct file permissions after installation.	5.3	More Details
CVE-2024-24845	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Sewpafly Post Thumbnail Editor.This issue affects Post Thumbnail Editor: from n/a through 2.4.8.	5.3	More Details
CVE-2024-1733	The Word Replacer Pro plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the word_replacer_ultra() function in all versions up to, and including, 1.0. This makes it possible for unauthenticated attackers to update arbitrary content on the affected WordPress site.	5.3	More Details
CVE-2024-21503	Versions of the package black before 24.3.0 are vulnerable to Regular Expression Denial of Service (ReDoS) via the lines_with_leading_tabs_expanded function in the strings.py file. An attacker could exploit this vulnerability by crafting a malicious input that causes a denial of service. Exploiting this vulnerability is possible when running Black on untrusted input, or if you habitually put thousands of leading tab characters in your docstrings.	5.3	More Details
CVE-2024-1145	User enumeration vulnerability in Devklan's Alma Blog that affects versions 2.1.10 and earlier. This vulnerability could allow a remote user to retrieve all valid users registered in the application just by looking at the request response.	5.3	More Details
CVE-2024-1857	The Ultimate Gift Cards for WooCommerce – Create, Redeem & Manage Digital Gift Certificates with Personalized Templates plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.6.6 via the wps_wgm_preview_email_template(). This makes it possible for unauthenticated attackers to read password protected and draft posts that may contain sensitive data.	5.3	More Details
CVE-2024-2557	A vulnerability was found in kishor-23 Food Waste Management System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/admin.php. The manipulation leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257056. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2024-24867	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Osamaesh WP Visitor Statistics (Real Time Traffic).This issue affects WP Visitor Statistics (Real Time Traffic): from n/a through 6.9.4.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25933	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Pepro Dev. Group PeproDev Ultimate Invoice.This issue affects PeproDev Ultimate Invoice: from n/a through 1.9.7.	5.3	More Details
CVE-2024-25651	User enumeration can occur in the Authentication REST API in Delinea PAM Secret Server 11.4. This allows a remote attacker to determine whether a user is valid because of a difference in responses from the /oauth2/token endpoint.	5.3	More Details
CVE-2023-52618	In the Linux kernel, the following vulnerability has been resolved: block/rnbd-srv: Check for unlikely string overflow Since "dev_search_path" can technically be as large as PATH_MAX, there was a risk of truncation when copying it and a second string into "full_path" since it was also PATH_MAX sized. The W=1 builds were reporting this warning: drivers/block/rnbd/rnbd-srv.c: In function 'process_msg_open.isra': drivers/block/rnbd/rnbd-srv.c:616:51: warning: '%s' directive output may be truncated writing up to 254 bytes into a region of size between 0 and 4095 [-Wformat-truncation=] 616 | snprintf(full_path, PATH_MAX, "%s/%s", | ^~ In function 'rnbd_srv_get_full_path', inlined from 'process_msg_open.isra' at drivers/block/rnbd/rnbd-srv.c:721:14: drivers/block/rnbd/rnbd-srv.c:616:17: note: 'snprintf' output between 2 and 4351 bytes into a destination of size 4096 616 | snprintf(full_path, PATH_MAX, "%s/%s", | ^~~~~~~ 617 | dev_search_path, dev_name); | ~~~~~~~~~~~~~~~~~~~~~~~~~~~ To fix this, unconditionally check for truncation (as was already done for the case where "%SESSNAME%" was present).	5.3	More Details
CVE-2024-0163	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain a TOCTOU race condition vulnerability. A local low privileged attacker could potentially exploit this vulnerability to gain access to otherwise unauthorized resources.	5.3	More Details
CVE-2024-20266	A vulnerability in the DHCP version 4 (DHCPv4) server feature of Cisco IOS XR Software could allow an unauthenticated, remote attacker to trigger a crash of the dhcpd process, resulting in a denial of service (DoS) condition. This vulnerability exists because certain DHCPv4 messages are improperly validated when they are processed by an affected device. An attacker could exploit this vulnerability by sending a malformed DHCPv4 message to an affected device. A successful exploit could allow the attacker to cause a crash of the dhcpd process. While the dhcpd process is restarting, which may take approximately two minutes, DHCPv4 server services are unavailable on the affected device. This could temporarily prevent network access to clients that join the network during that time period and rely on the DHCPv4 server of the affected device. Notes: Only the dhcpd process crashes and eventually restarts automatically. The router does not reload. This vulnerability only applies to DHCPv4. DHCP version 6 (DHCPv6) is not affected.	5.3	More Details
CVE-2024-1176	The HT Easy GA4 – Google Analytics WordPress Plugin plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the login() function in all versions up to, and including, 1.1.5. This makes it possible for unauthenticated attackers to update the email associated through the plugin with GA4.	5.3	More Details
CVE-2024-1321	The EventPrime – Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to payment bypass in all versions up to, and including, 3.4.2. This is due to the plugin allowing unauthenticated users to update the status of order payments. This makes it possible for unauthenticated attackers to book events for free.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-1370	The Maintenance Page plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the subscribe_download function hooked via AJAX action in all versions up to, and including, 1.0.8. This makes it possible for authenticated attackers, with subscriber access or higher, to download a csv containing subscriber emails.	5.3	More Details
CVE-2024-1380	The Relevanssi – A Better Search plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the relevanssi_export_log_check() function in all versions up to, and including, 4.22.0. This makes it possible for unauthenticated attackers to export the query log data. The vendor has indicated that they may look into adding a capability check for proper authorization control, however, this vulnerability is theoretically patched as is.	5.3	More Details
CVE-2024-1462	The Maintenance Page plugin for WordPress is vulnerable to Basic Information Exposure in all versions up to, and including, 1.0.8 via the REST API. This makes it possible for unauthenticated attackers to view post titles and content when the site is in maintenance mode.	5.3	More Details
CVE-2024-1479	The WP Show Posts plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.1.4 via the wpsp_display function. This makes it possible for authenticated attackers with contributor access and above to view the contents of draft, trash, future, private and pending posts and pages.	5.3	More Details
CVE-2024-1640	The Contact Form Builder Plugin: Multi Step Contact Form, Payment Form, Custom Contact Form Plugin by Bit Form plugin for WordPress is vulnerable to unauthorized modification of data due to a insufficient user validation on the bitforms_update_form_entry AJAX action in all versions up to, and including, 2.10.1. This makes it possible for unauthenticated attackers to modify form submissions.	5.3	More Details
CVE-2024-25903	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in N-Media Frontend File Manager.This issue affects Frontend File Manager: from n/a through 22.7.	5.3	More Details
CVE-2024-2106	The MasterStudy LMS WordPress Plugin – for Online Courses and Education plugin for WordPress is vulnerable to Information Exposure in versions up to, and including, 3.2.10. This can allow unauthenticated attackers to extract sensitive data including all registered user's username and email addresses which can be used to help perform future attacks.	5.3	More Details
CVE-2024-0162	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain an Improper SMM communication buffer verification vulnerability. A local low privileged attacker could potentially exploit this vulnerability leading to out-of-bound read/writes to SMRAM.	5.3	More Details
CVE-2024-26119	Adobe Experience Manager versions 6.5.19 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An attacker could leverage this vulnerability to achieve a low-confidentiality impact within the application. Exploitation of this issue does not require user interaction.	5.3	More Details
CVE-2024-24692	Race condition in the installer for Zoom Rooms Client for Windows before version 5.17.5 may allow an authenticated user to conduct a denial of service via local access.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28192	your_spotify is an open source, self hosted Spotify tracking dashboard. YourSpotify version <1.8.0 is vulnerable to NoSQL injection in the public access token processing logic. Attackers can fully bypass the public token authentication mechanism, regardless if a public token has been generated before or not, without any user interaction or prerequisite knowledge. This vulnerability allows an attacker to fully bypass the public token authentication mechanism, regardless if a public token has been generated before or not, without any user interaction or prerequisite knowledge. This issue has been addressed in version 1.8.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2024-2495	Cryptographic key vulnerability encoded in the FriendlyWrt firmware affecting version 2022-11-16.51b3d35. This vulnerability could allow an attacker to compromise the confidentiality and integrity of encrypted data.	5.2	More Details
CVE-2023-43043	IBM Maximo Application Suite - Maximo Mobile for EAM 8.10 and 8.11 could disclose sensitive information to a local user. IBM X-Force ID: 266875.	5.1	More Details
CVE-2024-2496	A NULL pointer dereference flaw was found in the udevConnectListAllInterfaces() function in libvirt. This issue can occur when detaching a host interface while at the same time collecting the list of interfaces via virConnectListAllInterfaces API. This flaw could be used to perform a denial of service attack by causing the libvirt daemon to crash.	5.0	More Details
CVE-2024-0447	The ArtiBot Free Chat Bot for WordPress WebSites plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the artibot_update function in all versions up to, and including, 1.1.6. This makes it possible for authenticated attackers, with subscriber-level access and above, to update plugin settings.	5.0	More Details
CVE-2024-28859	Symfony1 is a community fork of symfony 1.4 with DIC, form enhancements, latest Swiftmailer, better performance, composer compatible and PHP 8 support. Symfony 1 has a gadget chain due to vulnerable Swift Mailer dependency that would enable an attacker to get remote code execution if a developer unserialize user input in his project. This vulnerability present no direct threat but is a vector that will enable remote code execution if a developper deserialize user untrusted data. Symfony 1 depends on Swift Mailer which is bundled by default in vendor directory in the default installation since 1.3.0. Swift Mailer classes implement some `__destruct()` methods. These methods are called when php destroys the object in memory. However, it is possible to include any object type in `$this->_keys` to make PHP access to another array/object properties than intended by the developer. In particular, it is possible to abuse the array access which is triggered on foreach($this->_keys ...) for any class implementing ArrayAccess interface. This may allow an attacker to execute any PHP command which leads to remote code execution. This issue has been addressed in version 1.5.18. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-7248	Certain functionality in OpenText Vertica Management console might be prone to bypass via crafted requests. The vulnerability would affect one of Vertica's authentication functionalities by allowing specially crafted requests and sequences. This issue impacts the following Vertica Management Console versions: 10.x 11.1.1-24 or lower 12.0.4-18 or lower Please upgrade to one of the following Vertica Management Console versions: 10.x to upgrade to latest versions from below. 11.1.1-25 12.0.4-19 23.x 24.x	5.0	More Details
CVE-2023-6957	The Fluent Forms plugin for WordPress by Fluent Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting in all versions up to, and including, 5.1.9 due to insufficient input sanitization and output escaping. This makes it possible for attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. The exploitation level depends on who is granted the right to create forms by an administrator. This level can be as low as contributor, but by default is admin.	4.9	More Details
CVE-2024-22398	An improper Limitation of a Pathname to a Restricted Directory (Path Traversal) vulnerability in SonicWall Email Security Appliance could allow a remote attacker with administrative privileges to conduct a directory traversal attack and delete arbitrary files from the appliance file system.	4.9	More Details
CVE-2024-2294	The Backuply – Backup, Restore, Migrate and Clone plugin for WordPress is vulnerable to Directory Traversal in all versions up to, and including, 1.2.7 via the backup_name parameter in the backuply_download_backup function. This makes it possible for attackers to have an account with only activate_plugins capability to access arbitrary files on the server, which can contain sensitive information. This only impacts sites hosted on Windows servers.	4.9	More Details
CVE-2024-1223	This vulnerability potentially allows unauthorized enumeration of information from the embedded device APIs. An attacker must already have existing knowledge of some combination of valid usernames, device names and an internal system key. For such an attack to be successful the system must be in a specific runtime state.	4.8	More Details
CVE-2024-26050	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an admin attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	4.8	More Details
CVE-2024-27440	The Toyoko Inn official App for iOS versions prior to 1.13.0 and Toyoko Inn official App for Android versions prior 1.3.14 don't properly verify server certificates, which allows a man-in-the-middle attacker to spoof servers and obtain sensitive information via a crafted certificate.	4.8	More Details
CVE-2024-27953	Missing Authorization vulnerability in Cool Plugins Cryptocurrency Widgets – Price Ticker & Coins List.This issue affects Cryptocurrency Widgets – Price Ticker & Coins List: from n/a through 2.6.8.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2568	A vulnerability has been found in heyewei JFinalCMS 5.0.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/div_data/delete?divId=9 of the component Custom Data Page. 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 associated identifier of this vulnerability is VDB-257071.	4.7	More Details
CVE-2024-2497	A vulnerability was found in RaspAP raspap-webgui 3.0.9 and classified as critical. This issue affects some unknown processing of the file includes/provider.php of the component HTTP POST Request Handler. The manipulation of the argument country leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256919. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2023-7236	The Backup Bolt WordPress plugin through 1.3.0 is vulnerable to Information Exposure via the unprotected access of debug logs. This makes it possible for unauthenticated attackers to retrieve the debug log which may contain information like system errors which could contain sensitive information.	4.7	More Details
CVE-2024-1985	The Simple Membership plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Display Name' parameter in all versions up to, and including, 4.4.2 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This vulnerability requires social engineering to successfully exploit, and the impact would be very limited due to the attacker requiring a user to login as the user with the injected payload for execution.	4.7	More Details
CVE-2024-26163	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	4.7	More Details
CVE-2023-38535	Use of Hard-coded Cryptographic Key vulnerability in OpenText™ Exceed Turbo X affecting versions 12.5.1 and 12.5.2. The vulnerability could compromise the cryptographic keys.	4.7	More Details
CVE-2024-1606	Lack of input sanitization in BMC Control-M branches 9.0.20 and 9.0.21 allows logged-in users for manipulation of generated web pages via injection of HTML code. This might lead to a successful phishing attack for example by tricking users into using a hyperlink pointing to a website controlled by an attacker. Fix for 9.0.20 branch was released in version 9.0.20.238. Fix for 9.0.21 branch was released in version 9.0.21.200.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47129	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_ct: skip expectations for confirmed conntrack nft_ct_expect_obj_eval() calls nf_ct_ext_add() for a confirmed conntrack entry. However, nf_ct_ext_add() can only be called for !nf_ct_is_confirmed(). [1825.349056] WARNING: CPU: 0 PID: 1279 at net/netfilter/nf_conntrack_extend.c:48 nf_ct_xt_add+0x18e/0x1a0 [nf_conntrack] [1825.351391] RIP: 0010:nf_ct_ext_add+0x18e/0x1a0 [nf_conntrack] [1825.351493] Code: 41 5c 41 5d 41 5e 41 5f c3 41 bc 0a 00 00 00 e9 15 ff ff ff ba 09 00 00 00 31 f6 4c 89 ff e8 69 6c 3d e9 eb 96 45 31 ed eb cd <0f> 0b e9 b1 fe ff ff e8 86 79 14 e9 eb bf 0f 1f 40 00 0f 1f 44 00 [1825.351721] RSP: 0018:ffffc90002e1f1e8 EFLAGS: 00010202 [1825.351790] RAX: 000000000000000e RBX: ffff88814f5783c0 RCX: ffffffffc0e4f887 [1825.351881] RDX: dfffc0000000000 RSI: 0000000000000008 RDI: ffff88814f578440 [1825.351971] RBP: 0000000000000000 R08: 0000000000000000 R09: ffff88814f578447 [1825.352060] R10: ffffed1029eaf088 R11: 0000000000000001 R12: ffff88814f578440 [1825.352150] R13: ffff8882053f3a00 R14: 0000000000000000 R15: 0000000000000a20 [1825.352240] FS: 00007f992261c900(0000) GS:ffff889faec00000(0000) knlGS:0000000000000000 [1825.352343] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [1825.352417] CR2: 000056070a4d1158 CR3: 000000015efe0000 CR4: 0000000000350ee0 [1825.352508] Call Trace: [1825.352544] nf_ct_helper_ext_add+0x10/0x60 [nf_conntrack] [1825.352641] nft_ct_expect_obj_eval+0x1b8/0x1e0 [nft_ct] [1825.352716] nft_do_chain+0x232/0x850 [nf_tables] Add the ct helper extension only for unconfirmed conntrack. Skip rule evaluation if the ct helper extension does not exist. Thus, you can only create expectations from the first packet. It should be possible to remove this limitation by adding a new action to attach a generic ct helper to the first packet. Then, use this ct helper extension from follow up packets to create the ct expectation. While at it, add a missing check to skip the template conntrack too and remove check for IPCT_UNTRACK which is implicit to !ct.	4.6	More Details
CVE-2024-27104	GLPI is a Free Asset and IT Management Software package, Data center management, ITIL Service Desk, licenses tracking and software auditing. A user with rights to create and share dashboards can build a dashboard containing javascript code. Any user that will open this dashboard will be subject to an XSS attack. This issue has been patched in version 10.0.13.	4.5	More Details
CVE-2024-2432	A privilege escalation (PE) vulnerability in the Palo Alto Networks GlobalProtect app on Windows devices enables a local user to execute programs with elevated privileges. However, execution requires that the local user is able to successfully exploit a race condition.	4.5	More Details
CVE-2024-27265	IBM Integration Bus for z/OS 10.1 through 10.1.0.3 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. IBM X-Force ID: 284564.	4.5	More Details
CVE-2024-25942	Dell PowerEdge Server BIOS contains an Improper SMM communication buffer verification vulnerability. A physical high privileged attacker could potentially exploit this vulnerability leading to arbitrary writes to SMRAM.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4839	The WP Go Maps for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in versions up to, and including, 9.0.32 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-2024-0449	The ArtiBot Free Chat Bot for WordPress WebSites plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 1.1.6 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-2021-47130	In the Linux kernel, the following vulnerability has been resolved: nvmet: fix freeing unallocated p2pmem In case p2p device was found but the p2p pool is empty, the nvme target is still trying to free the sgl from the p2p pool instead of the regular sgl pool and causing a crash (BUG() is called). Instead, assign the p2p_dev for the request only if it was allocated from p2p pool. This is the crash that was caused: [Sun May 30 19:13:53 2021] ------------[cut here]------------ [Sun May 30 19:13:53 2021] kernel BUG at lib/genalloc.c:518! [Sun May 30 19:13:53 2021] invalid opcode: 0000 [#1] SMP PTI ... [Sun May 30 19:13:53 2021] kernel BUG at lib/genalloc.c:518! ... [Sun May 30 19:13:53 2021] RIP: 0010:gen_pool_free_owner+0xa8/0xb0 ... [Sun May 30 19:13:53 2021] Call Trace: [Sun May 30 19:13:53 2021] ------------[cut here]------------ [Sun May 30 19:13:53 2021] pci_free_p2pmem+0x2b/0x70 [Sun May 30 19:13:53 2021] pci_p2pmem_free_sgl+0x4f/0x80 [Sun May 30 19:13:53 2021] nvmet_req_free_sgls+0x1e/0x80 [nvmet] [Sun May 30 19:13:53 2021] kernel BUG at lib/genalloc.c:518! [Sun May 30 19:13:53 2021] nvmet_rdma_release_rsp+0x4e/0x1f0 [nvmet_rdma] [Sun May 30 19:13:53 2021] nvmet_rdma_send_done+0x1c/0x60 [nvmet_rdma]	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26638	In the Linux kernel, the following vulnerability has been resolved: nbd: always initialize struct msghdr completely syzbot complains that msg->msg_get_inq value can be uninitialized [1] struct msghdr got many new fields recently, we should always make sure their values is zero by default. [1] BUG: KMSAN: uninit-value in tcp_recvmsg+0x686/0xac0 net/ipv4/tcp.c:2571 tcp_recvmsg+0x686/0xac0 net/ipv4/tcp.c:2571 inet_recvmsg+0x131/0x580 net/ipv4/af_inet.c:879 sock_recvmsg_nosec net/socket.c:1044 [inline] sock_recvmsg+0x12b/0x1e0 net/socket.c:1066 __sock_xmit+0x236/0x5c0 drivers/block/nbd.c:538 nbd_read_reply drivers/block/nbd.c:732 [inline] recv_work+0x262/0x3100 drivers/block/nbd.c:863 process_one_work kernel/workqueue.c:2627 [inline] process_scheduled_works+0x104e/0x1e70 kernel/workqueue.c:2700 worker_thread+0xf45/0x1490 kernel/workqueue.c:2781 kthread+0x3ed/0x540 kernel/kthread.c:388 ret_from_fork+0x66/0x80 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x11/0x20 arch/x86/entry/entry_64.S:242 Local variable msg created at: __sock_xmit+0x4c/0x5c0 drivers/block/nbd.c:513 nbd_read_reply drivers/block/nbd.c:732 [inline] recv_work+0x262/0x3100 drivers/block/nbd.c:863 CPU: 1 PID: 7465 Comm: kworker/u5:1 Not tainted 6.7.0-rc7-syzkaller-00041-gf016f7547aee #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 11/17/2023 Workqueue: nbd5-recv recv_work	4.4	More Details
CVE-2024-2537	Improper Control of Dynamically-Managed Code Resources vulnerability in Logitech Logi Tune on MacOS allows Local Code Inclusion.	4.4	More Details
CVE-2023-52617	In the Linux kernel, the following vulnerability has been resolved: PCI: switchtec: Fix stdev_release() crash after surprise hot remove A PCI device hot removal may occur while stdev->cdev is held open. The call to stdev_release() then happens during close or exit, at a point way past switchtec_pci_remove(). Otherwise the last ref would vanish with the trailing put_device(), just before return. At that later point in time, the devm cleanup has already removed the stdev->mmio_mrpc mapping. Also, the stdev->pdev reference was not a counted one. Therefore, in DMA mode, the iowrite32() in stdev_release() will cause a fatal page fault, and the subsequent dma_free_coherent(), if reached, would pass a stale &stdev->pdev->dev pointer. Fix by moving MRPC DMA shutdown into switchtec_pci_remove(), after stdev_kill(). Counting the stdev->pdev ref is now optional, but may prevent future accidents. Reproducible via the script at https://lore.kernel.org/r/20231113212150.96410-1-dns@arista.com	4.4	More Details
CVE-2024-0898	The Chat Bubble – Floating Chat with Contact Chat Icons, Messages, Telegram, Email, SMS, Call me back plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 2.3 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 Number	Description	Base Score	Reference
CVE-2024-0614	The Events Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 6.4.6.4 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-2023-39933	Insufficient verification vulnerability exists in Broadcast Mail CGI (pmc.exe) included in A.K.I Software's PMailServer/PMailServer2 products. If this vulnerability is exploited, a user who can upload files through the product may execute an arbitrary executable file with the web server's execution privilege.	4.3	More Details
CVE-2024-1690	The TeraWallet – Best WooCommerce Wallet System With Cashback Rewards, Partial Payment, Wallet Refunds plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the terawallet_export_user_search() function in all versions up to, and including, 1.4.10. This makes it possible for authenticated attackers, with subscriber-level access and above, to export a list of registered users and their emails.	4.3	More Details
CVE-2023-46179	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 269683.	4.3	More Details
CVE-2024-1843	The Auto Affiliate Links plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the aalAddLink function in all versions up to, and including, 6.4.3. This makes it possible for authenticated attackers, with subscriber access or higher, to add arbitrary links to posts.	4.3	More Details
CVE-2023-50861	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 HUSKY – Products Filter for WooCommerce (formerly WOOF).This issue affects HUSKY – Products Filter for WooCommerce (formerly WOOF): from n/a through 1.3.4.3.	4.3	More Details
CVE-2024-2446	Mattermost versions 8.1.x before 8.1.10, 9.2.x before 9.2.6, 9.3.x before 9.3.2, and 9.4.x before 9.4.3 fail to limit the number of @-mentions processed per message, allowing an authenticated attacker to crash the client applications of other users via large, crafted messages.	4.3	More Details
CVE-2024-2483	A vulnerability, which was classified as problematic, has been found in Surya2Developer Hostel Management Service 1.0. This issue affects some unknown processing of the file /change-password.php of the component Password Change Handler. The manipulation of the argument oldpassword leads to cross-site request forgery. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-256889 was assigned to this vulnerability.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2648	A vulnerability, which was classified as problematic, was found in Netentsec NS-ASG Application Security Gateway 6.3. Affected is an unknown function of the file /nac/naccheck.php. The manipulation of the argument username leads to improper neutralization of data within xpath expressions. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257286 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-20319	A vulnerability in the UDP forwarding code of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to bypass configured management plane protection policies and access the Simple Network Management Plane (SNMP) server of an affected device. This vulnerability is due to incorrect UDP forwarding programming when using SNMP with management plane protection. An attacker could exploit this vulnerability by attempting to perform an SNMP operation using broadcast as the destination address that could be processed by an affected device that is configured with an SNMP server. A successful exploit could allow the attacker to communicate to the device on the configured SNMP ports. Although an unauthenticated attacker could send UDP datagrams to the configured SNMP port, only an authenticated user can retrieve or modify data using SNMP requests.	4.3	More Details
CVE-2024-1489	The SMS Alert Order Notifications – WooCommerce plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.6.9. This is due to missing or incorrect nonce validation on the processBulkAction function. This makes it possible for unauthenticated attackers to delete pages and posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-2560	A vulnerability classified as problematic was found in Tenda AC18 15.03.05.05. Affected by this vulnerability is the function fromSysToolRestoreSet of the file /goform/SysToolRestoreSet. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257059. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-2559	A vulnerability classified as problematic has been found in Tenda AC18 15.03.05.05. Affected is the function fromSysToolReboot of the file /goform/SysToolReboot. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-257058 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-2639	A vulnerability was found in Bdtask Wholesale Inventory Management System up to 20240311. It has been declared as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to session fixiation. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-257245 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-25653	Broken Access Control in the Report functionality of Delinea PAM Secret Server 11.4 allows unprivileged users, when Unlimited Admin Mode is enabled, to view system reports and modify custom reports via the Report functionality in the Web UI.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-27097	A user endpoint didn't perform filtering on an incoming parameter, which was added directly to the application log. This could lead to an attacker injecting false log entries or corrupt the log file format. This has been fixed in the CKAN versions 2.9.11 and 2.10.4. Users are advised to upgrade. Users unable to upgrade should override the `/user/reset` endpoint to filter the `id` parameter in order to exclude newlines.	4.3	More Details
CVE-2023-51407	Cross-Site Request Forgery (CSRF) vulnerability in Rocket Elements Split Test For Elementor.This issue affects Split Test For Elementor: from n/a through 1.6.9.	4.3	More Details
CVE-2023-51510	Cross-Site Request Forgery (CSRF) vulnerability in Atlas Gondal Export Media URLs.This issue affects Export Media URLs: from n/a through 1.0.	4.3	More Details
CVE-2024-2433	An improper authorization vulnerability in Palo Alto Networks Panorama software enables an authenticated read-only administrator to upload files using the web interface and completely fill one of the disk partitions with those uploaded files, which prevents the ability to log into the web interface or to download PAN-OS, WildFire, and content images. This issue affects only the web interface of the management plane; the dataplane is unaffected.	4.3	More Details
CVE-2024-1642	The MainWP Dashboard – WordPress Manager for Multiple Websites Maintenance plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 4.6.0.1. This is due to missing or incorrect nonce validation on the 'posting_bulk' function. This makes it possible for unauthenticated attackers to delete arbitrary posts via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-1452	The GenerateBlocks plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.8.2 via Query Loop. This makes it possible for authenticated attackers, with contributor access and above, to see contents of posts and pages in draft or private status as well as those with scheduled publication dates.	4.3	More Details
CVE-2024-0829	The Comments Extra Fields For Post,Pages and CPT plugin for WordPress is vulnerable to Missing Authorization in all versions up to, and including, 5.0. This is due to missing or incorrect capability checks on several ajax actions. This makes it possible for authenticated attackers, with subscriber access or higher, to invoke those actions. As a result, they may modify comment form fields and update plugin settings.	4.3	More Details
CVE-2024-28550	Tenda AC18 V15.03.05.05 has a stack overflow vulnerability in the filePath parameter of formExpandDlnaFile function.	4.3	More Details
CVE-2023-51522	Cross-Site Request Forgery (CSRF) vulnerability in Cozmoslabs Paid Member Subscriptions.This issue affects Paid Member Subscriptions: from n/a through 2.10.4.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2645	A vulnerability classified as problematic has been found in Netentsec NS-ASG Application Security Gateway 6.3. This affects an unknown part of the file /vpnweb/resetpwd/resetpwd.php. The manipulation of the argument UserId leads to improper neutralization of data within xpath expressions. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-257283. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2023-51369	Cross-Site Request Forgery (CSRF) vulnerability in SysBasics Customize My Account for WooCommerce.This issue affects Customize My Account for WooCommerce: from n/a through 1.8.3.	4.3	More Details
CVE-2023-50886	Cross-Site Request Forgery (CSRF), Incorrect Authorization vulnerability in wpWax Legal Pages.This issue affects Legal Pages: from n/a through 1.3.7.	4.3	More Details
CVE-2024-0369	The Bulk Edit Post Titles plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the bulkUpdatePostTitles function in all versions up to, and including, 5.0.0. This makes it possible for authenticated attackers, with subscriber access and above, to modify the titles of arbitrary posts.	4.3	More Details
CVE-2024-0827	The Play.ht – Make Your Blog Posts Accessible With Text to Speech Audio plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.6.4. This is due to missing or incorrect nonce validation on several functions. This makes it possible for unauthenticated attackers to invoke those functions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-0385	The Categorify plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the categorifyAjaxAddCategory function in all versions up to, and including, 1.0.7.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to add categories.	4.3	More Details
CVE-2023-51512	Cross Site Request Forgery (CSRF) vulnerability in WBW Product Table by WBW.This issue affects Product Table by WBW: from n/a through 1.8.6.	4.3	More Details
CVE-2024-0830	The Comments Extra Fields For Post,Pages and CPT plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.0. This is due to missing or incorrect nonce validation on several ajax actions. This makes it possible for unauthenticated attackers to invoke those actions via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. As a result, they may modify comment form fields and update plugin settings.	4.3	More Details
CVE-2024-1158	The Post Form – Registration Form – Profile Form for User Profiles – Frontend Content Forms for User Submissions (UGC) plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the buddyforms_new_page function in all versions up to, and including, 2.8.7. This makes it possible for authenticated attackers, with subscriber access or higher, to create pages with arbitrary titles. These pages are published.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-29093	Cross-Site Request Forgery (CSRF) vulnerability in Tobias Conrad Builder for WooCommerce reviews shortcodes – ReviewShort.This issue affects Builder for WooCommerce reviews shortcodes – ReviewShort: from n/a through 1.01.3.	4.3	More Details
CVE-2024-1127	The EventPrime – Events Calendar, Bookings and Tickets plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the booking_export_all() function in all versions up to, and including, 3.4.1. This makes it possible for authenticated attackers, with subscriber-level access and above, to retrieve all event booking which can contain PII.	4.3	More Details
CVE-2024-23823	vantage6 is an open source framework built to enable, manage and deploy privacy enhancing technologies like Federated Learning and Multi-Party Computation. The vantage6 server has no restrictions on CORS settings. It should be possible for people to set the allowed origins of the server. The impact is limited because v6 does not use session cookies. This issue has been addressed in commit `70bb4e1d8` and is expected to ship in subsequent releases. Users are advised to upgrade as soon as a new release is available. There are no known workarounds for this vulnerability.	4.2	More Details
CVE-2023-46181	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 269686.	4.0	More Details
CVE-2024-28237	OctoPrint provides a web interface for controlling consumer 3D printers. OctoPrint versions up until and including 1.9.3 contain a vulnerability that allows malicious admins to configure or talk a victim with administrator rights into configuring a webcam snapshot URL which when tested through the "Test" button included in the web interface will execute JavaScript code in the victims browser when attempting to render the snapshot image. An attacker who successfully talked a victim with admin rights into performing a snapshot test with such a crafted URL could use this to retrieve or modify sensitive configuration settings, interrupt prints or otherwise interact with the OctoPrint instance in a malicious way. The vulnerability is patched in version 1.10.0rc3. OctoPrint administrators are strongly advised to thoroughly vet who has admin access to their installation and what settings they modify based on instructions by strangers.	4.0	More Details
CVE-2024-28851	The Snowflake Hive metastore connector provides an easy way to query Hive-managed data via Snowflake. Snowflake Hive MetaStore Connector has addressed a potential elevation of privilege vulnerability in a `helper script` for the Hive MetaStore Connector. A malicious insider without admin privileges could, in theory, use the script to download content from a Microsoft domain to the local system and replace the valid content with malicious code. If the attacker then also had local access to the same system where the maliciously modified script is run, they could attempt to manipulate users into executing the attacker-controlled helper script, potentially gaining elevated privileges to the local system. The vulnerability in the script was patched on February 09, 2024, without a version bump to the Connector. User who use the helper script are strongly advised to use the latest version as soon as possible. Users unable to upgrade should avoid using the helper script.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-51699	Fluid is an open source Kubernetes-native Distributed Dataset Orchestrator and Accelerator for data-intensive applications. An OS command injection vulnerability within the Fluid project's JuicefsRuntime can potentially allow an authenticated user, who has the authority to create or update the K8s CRD Dataset/JuicefsRuntime, to execute arbitrary OS commands within the juicefs related containers. This could lead to unauthorized access, modification or deletion of data. Users who're using versions < 0.9.3 with JuicefsRuntime should upgrade to v0.9.3.	4.0	More Details
CVE-2024-26246	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	3.9	More Details
CVE-2024-0173	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain an improper parameter initialization vulnerability. A local low privileged attacker could potentially exploit this vulnerability to read the contents of non-SMM stack memory.	3.8	More Details
CVE-2024-0154	Dell PowerEdge Server BIOS and Dell Precision Rack BIOS contain an improper parameter initialization vulnerability. A local low privileged attacker could potentially exploit this vulnerability to read the contents of non-SMM stack memory.	3.8	More Details
CVE-2024-2482	A vulnerability has been found in Surya2Developer Hostel Management Service 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /check_availability.php of the component HTTP POST Request Handler. The manipulation of the argument oldpassword leads to observable response discrepancy. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256891.	3.7	More Details
CVE-2023-32335	IBM Maximo Application Suite 8.10, 8.11 and IBM Maximo Asset Management 7.6.1.3 stores sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header or browser history. IBM X-Force ID: 255075.	3.7	More Details
CVE-2024-2606	Passing invalid data could have led to invalid wasm values being created, such as arbitrary integers turning into pointer values. This vulnerability affects Firefox < 124.	3.7	More Details
CVE-2024-24975	Uncontrolled Resource Consumption in Mattermost Mobile versions before 2.13.0 fails to limit the size of the code block that will be processed by the syntax highlighter, allowing an attacker to send a very large code block and crash the mobile app.	3.5	More Details
CVE-2024-2479	A vulnerability classified as problematic has been found in MHA Sistemas arMHAzena 9.6.0.0. This affects an unknown part of the component Cadastro Page. The manipulation of the argument Query leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256887. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2526	A vulnerability has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /admin/rooms.php. The manipulation of the argument id leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256963. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-2533	A vulnerability, which was classified as problematic, has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected by this issue is some unknown functionality of the file /admin/update-users.php. The manipulation of the argument id leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-256970 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-2518	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as problematic. This issue affects some unknown processing of the file book_history.php. The manipulation of the argument id leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256955. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-2519	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been classified as problematic. Affected is an unknown function of the file navbar.php. The manipulation of the argument id leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256956. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-1979	A vulnerability was found in Quarkus. In certain conditions related to the CI process, git credentials could be inadvertently published, which could put the git repository at risk.	3.5	More Details
CVE-2024-2521	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /admin/bookdate.php. The manipulation of the argument id leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-256958 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-2553	A vulnerability, which was classified as problematic, was found in SourceCodester Product Review Rating System 1.0. Affected is an unknown function of the component Rate Product Handler. The manipulation of the argument Your Name/Comment leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-257052.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2523	A vulnerability classified as problematic was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. This vulnerability affects unknown code of the file /admin/booktime.php. The manipulation of the argument id leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256960. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-2535	A vulnerability has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0 and classified as problematic. This vulnerability affects unknown code of the file /admin/users.php. The manipulation of the argument id leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256972. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-2525	A vulnerability, which was classified as problematic, was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected is an unknown function of the file /admin/receipt.php. The manipulation of the argument id leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-256962 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-2515	A vulnerability, which was classified as problematic, has been found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. Affected by this issue is some unknown functionality of the file home.php. The manipulation of the argument id leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-256952. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-2530	A vulnerability was found in MAGESH-K21 Online-College-Event-Hall-Reservation-System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/update-rooms.php. The manipulation of the argument id leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-256967. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-27502	Insertion of sensitive information into log file for some Intel(R) Local Manageability Service software before version 2316.5.1.2 may allow an authenticated user to potentially enable information disclosure via local access.	3.3	More Details
CVE-2024-28745	Improper export of Android application components issue exists in 'ABEMA' App for Android prior to 10.65.0 allowing another app installed on the user's device to access an arbitrary URL on 'ABEMA' App for Android via Intent. If this vulnerability is exploited, an arbitrary website may be displayed on the app, and as a result, the user may become a victim of a phishing attack.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28053	Resource Exhaustion in Mattermost Server versions 8.1.x before 8.1.10 fails to limit the size of the payload that can be read and parsed allowing an attacker to send a very large email payload and crash the server.	3.1	More Details
CVE-2024-1221	This vulnerability potentially allows files on a PaperCut NG/MF server to be exposed using a specifically formed payload against the impacted API endpoint. The attacker must carry out some reconnaissance to gain knowledge of a system token. This CVE only affects Linux and macOS PaperCut NG/MF servers.	3.1	More Details
CVE-2024-2616	To harden ICU against exploitation, the behavior for out-of-memory conditions was changed to crash instead of attempt to continue. This vulnerability affects Firefox ESR < 115.9 and Thunderbird < 115.9.	2.7	More Details
CVE-2024-28864	SecureProps is a PHP library designed to simplify the encryption and decryption of property data in objects. A vulnerability in SecureProps version 1.2.0 and 1.2.1 involves a regex failing to detect tags during decryption of encrypted data. This occurs when the encrypted data has been encoded with `NullEncoder` and passed to `TagAwareCipher`, and contains special characters such as `\n`. As a result, the decryption process is skipped since the tags are not detected. This causes the encrypted data to be returned in plain format. The vulnerability affects users who implement `TagAwareCipher` with any base cipher that has `NullEncoder` (not default). The patch for the issue has been released. Users are advised to update to version 1.2.2. As a workaround, one may use the default `Base64Encoder` with the base cipher decorated with `TagAwareCipher` to prevent special characters in the encrypted string from interfering with regex tag detection logic. This workaround is safe but may involve double encoding since `TagAwareCipher` uses `NullEncoder` by default.	2.6	More Details
CVE-2024-22412	ClickHouse is an open-source column-oriented database management system. A bug exists in the cloud ClickHouse offering prior to version 24.0.2.54535 and in github.com/clickhouse/clickhouse version 23.1. Query caching bypasses the role based access controls and the policies being enforced on roles. In affected versions, the query cache only respects separate users, however this is not documented and not expected behavior. People relying on ClickHouse roles can have their access control lists bypassed if they are using query caching. Attackers who have control of a role could guess queries and see data they shouldn't have access to. Version 24.1 of ClickHouse and version 24.0.2.54535 of ClickHouse Cloud contain a patch for this issue. Based on the documentation, role based access control should be enforced regardless if query caching is enabled or not.	2.4	More Details
CVE-2024-2567	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as problematic, was found in jurecapuder AndroidWeatherApp 1.0.0 on Android. Affected is an unknown function of the file androidmanifest.xml of the component Backup File Handler. The manipulation leads to exposure of backup file to an unauthorized control sphere. It is possible to launch the attack on the physical device. The exploit has been disclosed to the public and may be used. VDB-257070 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: The code maintainer was contacted early about this disclosure but did not respond in any way. Instead the GitHub repository got deleted after a few days. We have to assume that the product is not supported anymore.	1.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-2545	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-1730. Reason: This candidate is a duplicate of CVE-2024-1730. Notes: All CVE users should reference CVE-2024-1730 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-4426	Rejected reason: **REJECT** Not a valid security issue - vendor unable to replicate.	N/A	More Details
CVE-2024-21677	This High severity Path Traversal vulnerability was introduced in version 6.13.0 of Confluence Data Center. This Path Traversal vulnerability, with a CVSS Score of 8.3, allows an unauthenticated attacker to exploit an undefinable vulnerability which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Data Center Atlassian recommends that Confluence Data Center customers upgrade to the latest version and that Confluence Server customers upgrade to the latest 8.5.x LTS version. If you are unable to do so, upgrade your instance to one of the specified supported fixed versions See the release notes https://confluence.atlassian.com/doc/confluence-release-notes-327.html You can download the latest version of Confluence Data Center and Server from the download center https://www.atlassian.com/software/confluence/download-archives. This vulnerability was reported via our Bug Bounty program.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26629	In the Linux kernel, the following vulnerability has been resolved: nfsd: fix RELEASE_LOCKOWNER The test on so_count in nfsd4_release_lockowner() is nonsense and harmful. Revert to using check_for_locks(), changing that to not sleep. First: harmful. As is documented in the kdoc comment for nfsd4_release_lockowner(), the test on so_count can transiently return a false positive resulting in a return of NFS4ERR_LOCKS_HELD when in fact no locks are held. This is clearly a protocol violation and with the Linux NFS client it can cause incorrect behaviour. If RELEASE_LOCKOWNER is sent while some other thread is still processing a LOCK request which failed because, at the time that request was received, the given owner held a conflicting lock, then the nfsd thread processing that LOCK request can hold a reference (conflock) to the lock owner that causes nfsd4_release_lockowner() to return an incorrect error. The Linux NFS client ignores that NFS4ERR_LOCKS_HELD error because it never sends NFS4_RELEASE_LOCKOWNER without first releasing any locks, so it knows that the error is impossible. It assumes the lock owner was in fact released so it feels free to use the same lock owner identifier in some later locking request. When it does reuse a lock owner identifier for which a previous RELEASE failed, it will naturally use a lock_seqid of zero. However the server, which didn't release the lock owner, will expect a larger lock_seqid and so will respond with NFS4ERR_BAD_SEQID. So clearly it is harmful to allow a false positive, which testing so_count allows. The test is nonsense because ... well... it doesn't mean anything. so_count is the sum of three different counts. 1/ the set of states listed on so_stateids 2/ the set of active vfs locks owned by any of those states 3/ various transient counts such as for conflicting locks. When it is tested against '2' it is clear that one of these is the transient reference obtained by find_lockowner_str_locked(). It is not clear what the other one is expected to be. In practice, the count is often 2 because there is precisely one state on so_stateids. If there were more, this would fail. In my testing I see two circumstances when RELEASE_LOCKOWNER is called. In one case, CLOSE is called before RELEASE_LOCKOWNER. That results in all the lock states being removed, and so the lockowner being discarded (it is removed when there are no more references which usually happens when the lock state is discarded). When nfsd4_release_lockowner() finds that the lock owner doesn't exist, it returns success. The other case shows an so_count of '2' and precisely one state listed in so_stateid. It appears that the Linux client uses a separate lock owner for each file resulting in one lock state per lock owner, so this test on '2' is safe. For another client it might not be safe. So this patch changes check_for_locks() to use the (newish) find_any_file_locked() so that it doesn't take a reference on the nfs4_file and so never calls nfsd_file_put(), and so never sleeps. With this check is it safe to restore the use of check_for_locks() rather than testing so_count against the mysterious '2'.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52608	In the Linux kernel, the following vulnerability has been resolved: firmware: arm_scmi: Check mailbox/SMT channel for consistency On reception of a completion interrupt the shared memory area is accessed to retrieve the message header at first and then, if the message sequence number identifies a transaction which is still pending, the related payload is fetched too. When an SCMI command times out the channel ownership remains with the platform until eventually a late reply is received and, as a consequence, any further transmission attempt remains pending, waiting for the channel to be relinquished by the platform. Once that late reply is received the channel ownership is given back to the agent and any pending request is then allowed to proceed and overwrite the SMT area of the just delivered late reply; then the wait for the reply to the new request starts. It has been observed that the spurious IRQ related to the late reply can be wrongly associated with the freshly enqueued request: when that happens the SCMI stack in-flight lookup procedure is fooled by the fact that the message header now present in the SMT area is related to the new pending transaction, even though the real reply has still to arrive. This race-condition on the A2P channel can be detected by looking at the channel status bits: a genuine reply from the platform will have set the channel free bit before triggering the completion IRQ. Add a consistency check to validate such condition in the A2P ISR.	N/A	More Details
CVE-2024-27441	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-2024-2403	Improper cleanup in temporary file handling component in Devolutions Remote Desktop Manager 2024.1.12 and earlier on Windows allows an attacker that compromised a user endpoint, under specific circumstances, to access sensitive information via residual files in the temporary directory.	N/A	More Details
CVE-2024-26630	In the Linux kernel, the following vulnerability has been resolved: mm: cachestat: fix folio read-after-free in cache walk In cachestat, we access the folio from the page cache's xarray to compute its page offset, and check for its dirty and writeback flags. However, we do not hold a reference to the folio before performing these actions, which means the folio can concurrently be released and reused as another folio/page/slab. Get around this altogether by just using xarray's existing machinery for the folio page offsets and dirty/writeback states. This changes behavior for tmpfs files to now always report zeroes in their dirty and writeback counters. This is okay as tmpfs doesn't follow conventional writeback cache behavior: its pages get "cleaned" during swapout, after which they're no longer resident etc.	N/A	More Details
CVE-2024-25227	SQL Injection vulnerability in ABO.CMS version 5.8, allows remote attackers to execute arbitrary code, cause a denial of service (DoS), escalate privileges, and obtain sensitive information via the tb_login parameter in admin login page.	N/A	More Details
CVE-2024-26454	A Cross Site Scripting vulnerability in Healthcare-Chatbot through 9b7058a can occur via a crafted payload to the email1 or pwd1 parameter in login.php.	N/A	More Details
CVE-2024-26475	An issue in radareorg radare2 v.0.9.7 through v.5.8.6 and fixed in v.5.8.8 allows a local attacker to cause a denial of service via the grub_sfs_read_extent function.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42286	There is a PHP file inclusion vulnerability in the template configuration of eyoucms v1.6.4, allowing attackers to execute code or system commands through a carefully crafted malicious payload.	N/A	More Details
CVE-2024-1998	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-1795. Reason: This candidate is a reservation duplicate of CVE-2024-1795. Notes: All CVE users should reference CVE-2024-1795 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-2438	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-47851. Reason: This candidate is a reservation duplicate of CVE-2023-47851. Notes: All CVE users should reference CVE-2023-47851 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-2437	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-41728. Reason: This candidate is a reservation duplicate of CVE-2023-41728. Notes: All CVE users should reference CVE-2023-41728 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-22397	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') in the SonicOS SSLVPN portal allows a remote authenticated attacker as a firewall 'admin' user to store and execute arbitrary JavaScript code.	N/A	More Details
CVE-2024-24105	SQL Injection vulnerability in Code-projects Computer Science Time Table System 1.0 allows attackers to run arbitrary code via adminFormvalidation.php.	N/A	More Details
CVE-2024-28319	gpac 2.3-DEV-rev921-g422b78ecf-master was discovered to contain an out of boundary read vulnerability via gf_dash_setup_period media_tools/dash_client.c:6374	N/A	More Details
CVE-2024-28054	Amavis before 2.12.3 and 2.13.x before 2.13.1, in part because of its use of MIME-tools, has an Interpretation Conflict (relative to some mail user agents) when there are multiple boundary parameters in a MIME email message. Consequently, there can be an incorrect check for banned files or malware.	N/A	More Details
CVE-2024-28403	TOTOLINK X2000R before V1.0.0-B20231213.1013 is vulnerable to Cross Site Scripting (XSS) via the VPN Page.	N/A	More Details
CVE-2023-7007	Sciener server does not validate connection requests from the GatewayG2, allowing an impersonation attack that provides the attacker the unlockKey field.	N/A	More Details
CVE-2023-39223	Stored cross-site scripting vulnerability exists in CGIs included in A.K.I Software's PMailServer/PMailServer2 products. If this vulnerability is exploited, an arbitrary script may be executed on a logged-in user's web browser.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40160	Directory traversal vulnerability exists in Mailing List Search CGI (pmmls.exe) included in A.K.I Software's PMailServer/PMailServer2 products. If this vulnerability is exploited, a remote attacker may obtain arbitrary files on the server.	N/A	More Details
CVE-2023-52159	A stack-based buffer overflow vulnerability in gross 0.9.3 through 1.x before 1.0.4 allows remote attackers to trigger a denial of service (grossd daemon crash) or potentially execute arbitrary code in grossd via crafted SMTP transaction parameters that cause an incorrect strncat for a log entry.	N/A	More Details
CVE-2021-47156	The Net::IPAddress::Util module before 5.000 for Perl does not properly consider extraneous zero characters in an IP address string, which (in some situations) allows attackers to bypass access control that is based on IP addresses.	N/A	More Details
CVE-2024-29156	In OpenStack Murano through 16.0.0, when YAQL before 3.0.0 is used, the Murano service's MuranoPL extension to the YAQL language fails to sanitize the supplied environment, leading to potential leakage of sensitive service account information.	N/A	More Details
CVE-2024-23604	Cross-site scripting vulnerability exists in FitNesse all releases, which may allow a remote unauthenticated attacker to execute an arbitrary script on the web browser of the user who is using the product and accessing a link with specially crafted multiple parameters.	N/A	More Details
CVE-2024-28128	Cross-site scripting vulnerability exists in FitNesse releases prior to 20220319, which may allow a remote unauthenticated attacker to execute an arbitrary script on the web browser of the user who is using the product and accessing a link with a specially crafted certain parameter.	N/A	More Details
CVE-2023-52609	In the Linux kernel, the following vulnerability has been resolved: binder: fix race between mmput() and do_exit() Task A calls binder_update_page_range() to allocate and insert pages on a remote address space from Task B. For this, Task A pins the remote mm via mmget_not_zero() first. This can race with Task B do_exit() and the final mmput() refcount decrement will come from Task A. Task A | Task B ----------+---------- mmget_not_zero() | | do_exit() | exit_mm() | mmput() mmput() | exit_mmap() | remove_vma() | fput() | In this case, the work of ____fput() from Task B is queued up in Task A as TWA_RESUME. So in theory, Task A returns to userspace and the cleanup work gets executed. However, Task A instead sleep, waiting for a reply from Task B that never comes (it's dead). This means the binder_deferred_release() is blocked until an unrelated binder event forces Task A to go back to userspace. All the associated death notifications will also be delayed until then. In order to fix this use mmput_async() that will schedule the work in the corresponding mm->async_put_work WQ instead of Task A.	N/A	More Details
	In the Linux kernel, the following vulnerability has been resolved: net/sched: act_ct: fix skb leak and crash on ooo frags act_ct adds skb->users before defragmentation. If frags arrive in order, the last frag's reference is reset in: inet_frag_reasm_prepare skb_morph which is not straightforward. However when frags arrive out of order, nobody unref the last frag, and all frags are leaked. The situation is even worse, as initiating packet capture can lead to a crash[0] when skb has been cloned and shared at the same time. Fix the issue by removing skb_get() before defragmentation. act_ct returns TC_ACT_CONSUMED when defrag failed or in progress. [0]: [843.804823] ----------[cut here]----------- [843.809659] kernel BUG at net/core/skbuff.c:2091! [843.814516] invalid opcode: 0000 [#1] PREEMPT SMP [843.819296] CPU: 7 PID: 0		

CVE Number	Description	Base Score	Reference
CVE-2023-52610	Comm: swapper/7 Kdump: loaded Tainted: G S 6.7.0-rc3 #2 [843.824107] Hardware name: XFUSION 1288H V6/BC13MBSBD, BIOS 1.29 11/25/2022 [843.828953] RIP: 0010:pskb_expand_head+0x2ac/0x300 [843.833805] Code: 8b 70 28 48 85 f6 74 82 48 83 c6 08 bf 01 00 00 00 e8 38 bd ff ff 8b 83 c0 00 00 00 48 03 83 c8 00 00 00 e9 62 ff ff ff 0f 0b <0f> 0b e8 8d d0 ff ff e9 b3 fd ff ff 81 7c 24 14 40 01 00 00 4c 89 [843.843698] RSP: 0018:ffffc9000cce07c0 EFLAGS: 00010202 [843.848524] RAX: 0000000000000002 RBX: ffff88811a211d00 RCX: 0000000000000820 [843.853299] RDX: 0000000000000640 RSI: 0000000000000000 RDI: ffff88811a211d00 [843.857974] RBP: ffff888127d39518 R08: 00000000bee97314 R09: 0000000000000000 [843.862584] R10: 0000000000000000 R11: ffff8881109f0000 R12: 0000000000000880 [843.867147] R13: ffff888127d39580 R14: 0000000000000640 R15: ffff888170f7b900 [843.871680] FS: 0000000000000000(0000) GS:ffff889ffffc0000(0000) knlGS:0000000000000000 [843.876242] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [843.880778] CR2: 00007fa42affcfb8 CR3: 000000011433a002 CR4: 0000000000770ef0 [843.885336] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [843.889809] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [843.894229] PKRU: 55555554 [843.898539] Call Trace: [843.902772] <IRQ> [843.906922] ? __die_body+0x1e/0x60 [843.911032] ? die+0x3c/0x60 [843.915037] ? do_trap+0xe2/0x110 [843.918911] ? pskb_expand_head+0x2ac/0x300 [843.922687] ? do_error_trap+0x65/0x80 [843.926342] ? pskb_expand_head+0x2ac/0x300 [843.929905] ? exc_invalid_op+0x50/0x60 [843.933398] ? pskb_expand_head+0x2ac/0x300 [843.936835] ? asm_exc_invalid_op+0x1a/0x20 [843.940226] ? pskb_expand_head+0x2ac/0x300 [843.943580] inet_frag_reasm_prepare+0xd1/0x240 [843.946904] ip_defrag+0x5d4/0x870 [843.950132] nf_ct_handle_fragments+0xec/0x130 [nf_conntrack] [843.953334] tcf_ct_act+0x252/0xd90 [act_ct] [843.956473] ? tcf_mirred_act+0x516/0x5a0 [act_mirred] [843.959657] tcf_action_exec+0xa1/0x160 [843.962823] fl_classify+0x1db/0x1f0 [cls_flower] [843.966010] ? skb_clone+0x53/0xc0 [843.969173] tcf_classify+0x24d/0x420 [843.972333] tc_run+0x8f/0xf0 [843.975465] __netif_receive_skb_core+0x67a/0x1080 [843.978634] ? dev_gro_receive+0x249/0x730 [843.981759] __netif_receive_skb_list_core+0x12d/0x260 [843.984869] netif_receive_skb_list_internal+0x1cb/0x2f0 [843.987957] ? mlx5e_handle_rx_cqe_mpwrq_rep+0xfa/0x1a0 [mlx5_core] [843.991170] napi_complete_done+0x72/0x1a0 [843.994305] mlx5e_napi_poll+0x28c/0x6d0 [mlx5_core] [843.997501] __napi_poll+0x25/0x1b0 [844.000627] net_rx_action+0x256/0x330 [844.003705] __do_softirq+0xb3/0x29b [844.006718] irq_exit_rcu+0x9e/0xc0 [844.009672] common_interrupt+0x86/0xa0 [844.012537] </IRQ> [844.015285] <TASK> [844.017937] asm_common_interrupt+0x26/0x40 [844.020591] RIP: 0010:acpi_safe_halt+0x1b/0x20 [844.023247] Code: ff 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 65 48 8b 04 25 00 18 03 00 48 8b 00 a8 08 75 0c 66 90 0f 00 2d 81 d0 44 00 fb ---truncated---	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-52611	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw88: sdio: Honor the host max_req_size in the RX path Lukas reports skb_over_panic errors on his Banana Pi BPI-CM4 which comes with an Amlogic A311D (G12B) SoC and a RTL8822CS SDIO wifi/Bluetooth combo card. The error he observed is identical to what has been fixed in commit e967229ead0e ("wifi: rtw88: sdio: Check the HISR RX_REQUEST bit in rtw_sdio_rx_isr()") but that commit didn't fix Lukas' problem. Lukas found that disabling or limiting RX aggregation works around the problem for some time (but does not fully fix it). In the following discussion a few key topics have been discussed which have an impact on this problem: - The Amlogic A311D (G12B) SoC has a hardware bug in the SDIO controller which prevents DMA transfers. Instead all transfers need to go through the controller SRAM which limits transfers to 1536 bytes - rtw88 chips don't split incoming (RX) packets, so if a big packet is received this is forwarded to the host in it's original form - rtw88 chips can do RX aggregation, meaning more multiple incoming packets can be pulled by the host from the card with one MMC/SDIO transfer. This Depends on settings in the REG_RXDMA_AGG_PG_TH register (BIT_RXDMA_AGG_PG_TH limits the number of packets that will be aggregated, BIT_DMA_AGG_TO_V1 configures a timeout for aggregation and BIT_EN_PRE_CALC makes the chip honor the limits more effectively) Use multiple consecutive reads in rtw_sdio_read_port() and limit the number of bytes which are copied by the host from the card in one MMC/SDIO transfer. This allows receiving a buffer that's larger than the hosts max_req_size (number of bytes which can be transferred in one MMC/SDIO transfer). As a result of this the skb_over_panic error is gone as the rtw88 driver is now able to receive more than 1536 bytes from the card (either because the incoming packet is larger than that or because multiple packets have been aggregated). In case of an receive errors (-EILSEQ has been observed by Lukas) we need to drain the remaining data from the card's buffer, otherwise the card will return corrupt data for the next rtw_sdio_read_port() call.	N/A	More Details
CVE-2023-52612	In the Linux kernel, the following vulnerability has been resolved: crypto: scomp - fix req->dst buffer overflow The req->dst buffer size should be checked before copying from the scomp_scratch->dst to avoid req->dst buffer overflow problem.	N/A	More Details
CVE-2023-52616	In the Linux kernel, the following vulnerability has been resolved: crypto: lib/mpi - Fix unexpected pointer access in mpi_ec_init When the mpi_ec_ctx structure is initialized, some fields are not cleared, causing a crash when referencing the field when the structure was released. Initially, this issue was ignored because memory for mpi_ec_ctx is allocated with the __GFP_ZERO flag. For example, this error will be triggered when calculating the Za value for SM2 separately.	N/A	More Details
CVE-2023-52619	In the Linux kernel, the following vulnerability has been resolved: pstore/ram: Fix crash when setting number of cpus to an odd number When the number of cpu cores is adjusted to 7 or other odd numbers, the zone size will become an odd number. The address of the zone will become: addr of zone0 = BASE addr of zone1 = BASE + zone_size addr of zone2 = BASE + zone_size*2 ... The address of zone1/3/5/7 will be mapped to non-alignment va. Eventually crashes will occur when accessing these va. So, use ALIGN_DOWN() to make sure the zone size is even to avoid this bug.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-25654	Insecure permissions for log files of AVSystem Unified Management Platform (UMP) 23.07.0.16567~LTS allow members (with local access to the UMP application server) to access credentials to authenticate to all services, and to decrypt sensitive data stored in the database.	N/A	More Details
CVE-2024-26631	In the Linux kernel, the following vulnerability has been resolved: ipv6: mcast: fix data-race in ipv6_mc_down / mld_ifc_work idev->mc_ifc_count can be written over without proper locking. Originally found by syzbot [1], fix this issue by encapsulating calls to mld_ifc_stop_work() (and mld_gq_stop_work() for good measure) with mutex_lock() and mutex_unlock() accordingly as these functions should only be called with mc_lock per their declarations. [1] BUG: KCSAN: data-race in ipv6_mc_down / mld_ifc_work write to 0xffff88813a80c832 of 1 bytes by task 3771 on cpu 0: mld_ifc_stop_work net/ipv6/mcast.c:1080 [inline] ipv6_mc_down+0x10a/0x280 net/ipv6/mcast.c:2725 addrconf_ifdown+0xe32/0xf10 net/ipv6/addrconf.c:3949 addrconf_notify+0x310/0x980 notifier_call_chain kernel/notifier.c:93 [inline] raw_notifier_call_chain+0x6b/0x1c0 kernel/notifier.c:461 __dev_notify_flags+0x205/0x3d0 dev_change_flags+0xab/0xd0 net/core/dev.c:8685 do_setlink+0x9f6/0x2430 net/core/rtnetlink.c:2916 rtnl_group_changelink net/core/rtnetlink.c:3458 [inline] __rtnl_newlink net/core/rtnetlink.c:3717 [inline] rtnl_newlink+0xbb3/0x1670 net/core/rtnetlink.c:3754 rtnetlink_rcv_msg+0x807/0x8c0 net/core/rtnetlink.c:6558 netlink_rcv_skb+0x126/0x220 net/netlink/af_netlink.c:2545 rtnetlink_rcv+0x1c/0x20 net/core/rtnetlink.c:6576 netlink_unicast_kernel net/netlink/af_netlink.c:1342 [inline] netlink_unicast+0x589/0x650 net/netlink/af_netlink.c:1368 netlink_sendmsg+0x66e/0x770 net/netlink/af_netlink.c:1910 ... write to 0xffff88813a80c832 of 1 bytes by task 22 on cpu 1: mld_ifc_work+0x54c/0x7b0 net/ipv6/mcast.c:2653 process_one_work kernel/workqueue.c:2627 [inline] process_scheduled_works+0x5b8/0xa30 kernel/workqueue.c:2700 worker_thread+0x525/0x730 kernel/workqueue.c:2781 ...	N/A	More Details
CVE-2024-26632	In the Linux kernel, the following vulnerability has been resolved: block: Fix iterating over an empty bio with bio_for_each_folio_all If the bio contains no data, bio_first_folio() calls page_folio() on a NULL pointer and oopses. Move the test that we've reached the end of the bio from bio_next_folio() to bio_first_folio(). [axboe: add unlikely() to error case]	N/A	More Details
CVE-2024-26634	In the Linux kernel, the following vulnerability has been resolved: net: fix removing a namespace with conflicting altnames Mark reports a BUG() when a net namespace is removed. kernel BUG at net/core/dev.c:11520! Physical interfaces moved outside of init_net get "refunded" to init_net when that namespace disappears. The main interface name may get overwritten in the process if it would have conflicted. We need to also discard all conflicting altnames. Recent fixes addressed ensuring that altnames get moved with the main interface, which surfaced this problem.	N/A	More Details
CVE-2024-0951	The Advanced Social Feeds Widget & Shortcode WordPress plugin through 1.7 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)	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26635	In the Linux kernel, the following vulnerability has been resolved: llc: Drop support for ETH_P_TR_802_2. syzbot reported an uninit-value bug below. [0] llc supports ETH_P_802_2 (0x0004) and used to support ETH_P_TR_802_2 (0x0011), and syzbot abused the latter to trigger the bug. write$tun(r0, &(0x7f0000000040)={@val={0x0, 0x11}, @val, @mpls={[], @llc={@snap={0xaa, 0x1, ')', "90e5dd"}}}}, 0x16) llc_conn_handler() initialises local variables {saddr,daddr}.mac based on skb in llc_pdu_decode_sa()/llc_pdu_decode_da() and passes them to __llc_lookup(). However, the initialisation is done only when skb->protocol is htons(ETH_P_802_2), otherwise, __llc_lookup_established() and __llc_lookup_listener() will read garbage. The missing initialisation existed prior to commit 211ed865108e ("net: delete all instances of special processing for token ring"). It removed the part to kick out the token ring stuff but forgot to close the door allowing ETH_P_TR_802_2 packets to sneak into llc_rcv(). Let's remove llc_tr_packet_type and complete the deprecation. [0]: BUG: KMSAN: uninit-value in __llc_lookup_established+0xe9d/0xf90 __llc_lookup_established+0xe9d/0xf90 __llc_lookup net/llc/llc_conn.c:611 [inline] llc_conn_handler+0x4bd/0x1360 net/llc/llc_conn.c:791 llc_rcv+0xfbb/0x14a0 net/llc/llc_input.c:206 __netif_receive_skb_one_core net/core/dev.c:5527 [inline] __netif_receive_skb+0x1a6/0x5a0 net/core/dev.c:5641 netif_receive_skb_internal net/core/dev.c:5727 [inline] netif_receive_skb+0x58/0x660 net/core/dev.c:5786 tun_rx_batched+0x3ee/0x980 drivers/net/tun.c:1555 tun_get_user+0x53af/0x66d0 drivers/net/tun.c:2002 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:2048 call_write_iter include/linux/fs.h:2020 [inline] new_sync_write fs/read_write.c:491 [inline] vfs_write+0x8ef/0x1490 fs/read_write.c:584 ksys_write+0x20f/0x4c0 fs/read_write.c:637 __do_sys_write fs/read_write.c:649 [inline] __se_sys_write fs/read_write.c:646 [inline] __x64_sys_write+0x93/0xd0 fs/read_write.c:646 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x44/0x110 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x63/0x6b Local variable daddr created at: llc_conn_handler+0x53/0x1360 net/llc/llc_conn.c:783 llc_rcv+0xfbb/0x14a0 net/llc/llc_input.c:206 CPU: 1 PID: 5004 Comm: syz-executor994 Not tainted 6.6.0-syzkaller-14500-g1c41041124bd #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 10/09/2023	N/A	More Details
CVE-2024-0820	The Jobs for WordPress plugin before 2.7.4 does not sanitise and escape some parameters, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks	N/A	More Details
CVE-2024-0780	The Enjoy Social Feed plugin for WordPress website WordPress plugin through 6.2.2 does not have authorisation when resetting its database, allowing any authenticated users, such as subscriber to perform such action	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26636	In the Linux kernel, the following vulnerability has been resolved: llc: make llc_ui_sendmsg() more robust against bonding changes syzbot was able to trick llc_ui_sendmsg(), allocating an skb with no headroom, but subsequently trying to push 14 bytes of Ethernet header [1] Like some others, llc_ui_sendmsg() releases the socket lock before calling sock_alloc_send_skb(). Then it acquires it again, but does not redo all the sanity checks that were performed. This fix: - Uses LL_RESERVED_SPACE() to reserve space. - Check all conditions again after socket lock is held again. - Do not account Ethernet header for mtu limitation. [1] skbuff: skb_under_panic: text:ffff800088baa334 len:1514 put:14 head:ffff0000c9c37000 data:ffff0000c9c36ff2 tail:0x5dc end:0x6c0 dev:bond0 kernel BUG at net/core/skbuff.c:193 ! Internal error: Oops - BUG: 00000000f2000800 [#1] PREEMPT SMP Modules linked in: CPU: 0 PID: 6875 Comm: syz-executor.0 Not tainted 6.7.0-rc8-syzkaller-00101-g0802e17d9aca-dirty #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 11/17/2023 pstate: 60400005 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : skb_panic net/core/skbuff.c:189 [inline] pc : skb_under_panic+0x13c/0x140 net/core/skbuff.c:203 lr : skb_panic net/core/skbuff.c:189 [inline] lr : skb_under_panic+0x13c/0x140 net/core/skbuff.c:203 sp : ffff800096f97000 x29: ffff800096f97010 x28: ffff80008cc8d668 x27: dfff800000000000 x26: ffff0000cb970c90 x25: 00000000000005dc x24: ffff0000c9c36ff2 x23: ffff0000c9c37000 x22: 00000000000005ea x21: 00000000000006c0 x20: 000000000000000e x19: ffff800088baa334 x18: 1fffe000368261ce x17: ffff80008e4ed000 x16: ffff80008a8310f8 x15: 0000000000000001 x14: 1ffff00012df2d58 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000001 x10: 0000000000ff0100 x9 : e28a51f1087e8400 x8 : e28a51f1087e8400 x7 : ffff80008028f8d0 x6 : 0000000000000000 x5 : 0000000000000001 x4 : 0000000000000001 x3 : ffff800082b78714 x2 : 0000000000000001 x1 : 0000000100000000 x0 : 0000000000000089 Call trace: skb_panic net/core/skbuff.c:189 [inline] skb_under_panic+0x13c/0x140 net/core/skbuff.c:203 skb_push+0xf0/0x108 net/core/skbuff.c:2451 eth_header+0x44/0x1f8 net/ethernet/eth.c:83 dev_hard_header include/linux/netdevice.h:3188 [inline] llc_mac_hdr_init+0x110/0x17c net/llc/llc_output.c:33 llc_sap_action_send_xid_c+0x170/0x344 net/llc/llc_s_ac.c:85 llc_exec_sap_trans_actions net/llc/llc_sap.c:153 [inline] llc_sap_next_state net/llc/llc_sap.c:182 [inline] llc_sap_state_process+0x1ec/0x774 net/llc/llc_sap.c:209 llc_build_and_send_xid_pkt+0x12c/0x1c0 net/llc/llc_sap.c:270 llc_ui_sendmsg+0x7bc/0xb1c net/llc/af_llc.c:997 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg net/socket.c:745 [inline] sock_sendmsg+0x194/0x274 net/socket.c:767 splice_to_socket+0x7cc/0xd58 fs/splice.c:881 do_splice_from fs/splice.c:933 [inline] direct_splice_actor+0xe4/0x1c0 fs/splice.c:1142 splice_direct_to_actor+0x2a0/0x7e4 fs/splice.c:1088 do_splice_direct+0x20c/0x348 fs/splice.c:1194 do_sendfile+0x4bc/0xc70 fs/read_write.c:1254 __do_sys_sendfile64 fs/read_write.c:1322 [inline] __se_sys_sendfile64 fs/read_write.c:1308 [inline] __arm64_sys_sendfile64+0x160/0x3b4 fs/read_write.c:1308 __invoke_syscall arch/arm64/kernel/syscall.c:37 [inline] invoke_syscall+0x98/0x2b8 arch/arm64/kernel/syscall.c:51 el0_svc_common+0x130/0x23c arch/arm64/kernel/syscall.c:136 do_el0_svc+0x48/0x58 arch/arm64/kernel/syscall.c:155 el0_svc+0x54/0x158 arch/arm64/kernel/entry-common.c:678 el0t_64_sync_handler+0x84/0xfc arch/arm64/kernel/entry-common.c:696 el0t_64_sync+0x190/0x194 arch/arm64/kernel/entry.S:595 Code:	N/A	More Details

CVE Number	Description	Base Score	Reference
	aa1803e6 aa1903e7 a90023f5 94792f6a (d4210000)		
CVE-2024-26637	In the Linux kernel, the following vulnerability has been resolved: wifi: ath11k: rely on mac80211 debugfs handling for vif mac80211 started to delete debugfs entries in certain cases, causing a ath11k to crash when it tried to delete the entries later. Fix this by relying on mac80211 to delete the entries when appropriate and adding them from the vif_add_debugfs handler.	N/A	More Details
CVE-2024-26639	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2024-26640	In the Linux kernel, the following vulnerability has been resolved: tcp: add sanity checks to rx zerocopy TCP rx zerocopy intent is to map pages initially allocated from NIC drivers, not pages owned by a fs. This patch adds to can_map_frag() these additional checks: - Page must not be a compound one. - page->mapping must be NULL. This fixes the panic reported by ZhangPeng. syzbot was able to loopback packets built with sendfile(), mapping pages owned by an ext4 file to TCP rx zerocopy. r3 = socket$inet_tcp(0x2, 0x1, 0x0) mmap(&(0x7f0000ff9000/0x4000)=nil, 0x4000, 0x0, 0x12, r3, 0x0) r4 = socket$inet_tcp(0x2, 0x1, 0x0) bind$inet(r4, &(0x7f0000000000)={0x2, 0x4e24, @multicast1}, 0x10) connect$inet(r4, &(0x7f00000006c0)={0x2, 0x4e24, @empty}, 0x10) r5 = openat$dir(0xffffffffffffff9c, &(0x7f00000000c0)='./file0\x00', 0x181e42, 0x0) fallocate(r5, 0x0, 0x0, 0x85b8) sendfile(r4, r5, 0x0, 0x8ba0) getsockopt$inet_tcp_TCP_ZEROCOPY_RECEIVE(r4, 0x6, 0x23, &(0x7f00000001c0)={&(0x7f0000ffb000/0x3000)=nil, 0x3000, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0, 0x0}, &(0x7f0000000440)=0x40) r6 = openat$dir(0xffffffffffffff9c, &(0x7f00000000c0)='./file0\x00', 0x181e42, 0x0)	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-26641	In the Linux kernel, the following vulnerability has been resolved: ip6_tunnel: make sure to pull inner header in __ip6_tnl_rcv() syzbot found __ip6_tnl_rcv() could access unitiliazed data [1]. Call pskb_inet_may_pull() to fix this, and initialize ipv6h variable after this call as it can change skb->head. [1] BUG: KMSAN: uninit-value in __INET_ECN_decapsulate include/net/inet_ecn.h:253 [inline] BUG: KMSAN: uninit-value in INET_ECN_decapsulate include/net/inet_ecn.h:275 [inline] BUG: KMSAN: uninit-value in IP6_ECN_decapsulate+0x7df/0x1e50 include/net/inet_ecn.h:321 __INET_ECN_decapsulate include/net/inet_ecn.h:253 [inline] INET_ECN_decapsulate include/net/inet_ecn.h:275 [inline] IP6_ECN_decapsulate+0x7df/0x1e50 include/net/inet_ecn.h:321 ip6ip6_dscp_ecn_decapsulate+0x178/0x1b0 net/ipv6/ip6_tunnel.c:727 __ip6_tnl_rcv+0xd4e/0x1590 net/ipv6/ip6_tunnel.c:845 ip6_tnl_rcv+0xce/0x100 net/ipv6/ip6_tunnel.c:888 gre_rcv+0x143f/0x1870 ip6_protocol_deliver_rcu+0xda6/0x2a60 net/ipv6/ip6_input.c:438 ip6_input_finish net/ipv6/ip6_input.c:483 [inline] NF_HOOK include/linux/netfilter.h:314 [inline] ip6_input+0x15d/0x430 net/ipv6/ip6_input.c:492 ip6_mc_input+0xa7e/0xc80 net/ipv6/ip6_input.c:586 dst_input include/net/dst.h:461 [inline] ip6_rcv_finish+0x5db/0x870 net/ipv6/ip6_input.c:79 NF_HOOK include/linux/netfilter.h:314 [inline] ipv6_rcv+0xda/0x390 net/ipv6/ip6_input.c:310 __netif_receive_skb_one_core net/core/dev.c:5532 [inline] __netif_receive_skb+0x1a6/0x5a0 net/core/dev.c:5646 netif_receive_skb_internal net/core/dev.c:5732 [inline] netif_receive_skb+0x58/0x660 net/core/dev.c:5791 tun_rx_batched+0x3ee/0x980 drivers/net/tun.c:1555 tun_get_user+0x53af/0x66d0 drivers/net/tun.c:2002 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:2048 call_write_iter include/linux/fs.h:2084 [inline] new_sync_write fs/read_write.c:497 [inline] vfs_write+0x786/0x1200 fs/read_write.c:590 ksys_write+0x20f/0x4c0 fs/read_write.c:643 __do_sys_write fs/read_write.c:655 [inline] __se_sys_write fs/read_write.c:652 [inline] __x64_sys_write+0x93/0xd0 fs/read_write.c:652 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0x6d/0x140 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b Uninit was created at: slab_post_alloc_hook+0x129/0xa70 mm/slab.h:768 slab_alloc_node mm/slub.c:3478 [inline] kmem_cache_alloc_node+0x5e9/0xb10 mm/slub.c:3523 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:560 __alloc_skb+0x318/0x740 net/core/skbuff.c:651 alloc_skb include/linux/skbuff.h:1286 [inline] alloc_skb_with_frags+0xc8/0xbd0 net/core/skbuff.c:6334 sock_alloc_send_pskb+0xa80/0xbf0 net/core/sock.c:2787 tun_alloc_skb drivers/net/tun.c:1531 [inline] tun_get_user+0x1e8a/0x66d0 drivers/net/tun.c:1846 tun_chr_write_iter+0x3af/0x5d0 drivers/net/tun.c:2048 call_write_iter include/linux/fs.h:2084 [inline] new_sync_write fs/read_write.c:497 [inline] vfs_write+0x786/0x1200 fs/read_write.c:590 ksys_write+0x20f/0x4c0 fs/read_write.c:643 __do_sys_write fs/read_write.c:655 [inline] __se_sys_write fs/read_write.c:652 [inline] __x64_sys_write+0x93/0xd0 fs/read_write.c:652 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0x6d/0x140 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b CPU: 0 PID: 5034 Comm: syz-executor331 Not tainted 6.7.0-syzkaller-00562-g9f8413c4a66f #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 11/17/2023	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-6821	The Error Log Viewer by BestWebSoft WordPress plugin before 1.1.3 is affected by a Directory Listing issue, allowing users to read and download PHP logs without authorization	N/A	More Details
CVE-2024-22017	setuid() does not affect libuv's internal io_uring operations if initialized before the call to setuid(). This allows the process to perform privileged operations despite presumably having dropped such privileges through a call to setuid(). This vulnerability affects all users using version greater or equal than Node.js 18.18.0, Node.js 20.4.0 and Node.js 21.	N/A	More Details
CVE-2024-22025	A vulnerability in Node.js has been identified, allowing for a Denial of Service (DoS) attack through resource exhaustion when using the fetch() function to retrieve content from an untrusted URL. The vulnerability stems from the fact that the fetch() function in Node.js always decodes Brotli, making it possible for an attacker to cause resource exhaustion when fetching content from an untrusted URL. An attacker controlling the URL passed into fetch() can exploit this vulnerability to exhaust memory, potentially leading to process termination, depending on the system configuration.	N/A	More Details
CVE-2024-28070	A vulnerability in the legacy chat component of Mitel MiContact Center Business through 10.0.0.4 could allow an unauthenticated attacker to conduct a reflected cross-site scripting (XSS) attack due to insufficient input validation. A successful exploit could allow an attacker to access sensitive information and gain unauthorized access.	N/A	More Details
CVE-2021-47120	In the Linux kernel, the following vulnerability has been resolved: HID: magicmouse: fix NULL-deref on disconnect Commit 9d7b18668956 ("HID: magicmouse: add support for Apple Magic Trackpad 2") added a sanity check for an Apple trackpad but returned success instead of -ENODEV when the check failed. This means that the remove callback will dereference the never-initialised driver data pointer when the driver is later unbound (e.g. on USB disconnect).	N/A	More Details
CVE-2024-28401	TOTOLINK X2000R before v1.0.0-B20231213.1013 contains a Store Cross-site scripting (XSS) vulnerability in Root Access Control under the Wireless Page.	N/A	More Details
CVE-2024-1401	The Profile Box Shortcode And Widget WordPress plugin before 1.2.1 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)	N/A	More Details
CVE-2021-47109	In the Linux kernel, the following vulnerability has been resolved: neighbour: allow NUD_NOARP entries to be forced GCed IFF_POINTOPOINT interfaces use NUD_NOARP entries for IPv6. It's possible to fill up the neighbour table with enough entries that it will overflow for valid connections after that. This behaviour is more prevalent after commit 58956317c8de ("neighbor: Improve garbage collection") is applied, as it prevents removal from entries that are not NUD_FAILED, unless they are more than 5s old.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47110	In the Linux kernel, the following vulnerability has been resolved: x86/kvm: Disable kvmclock on all CPUs on shutdown Currenly, we disable kvmclock from machine_shutdown() hook and this only happens for boot CPU. We need to disable it for all CPUs to guard against memory corruption e.g. on restore from hibernate. Note, writing '0' to kvmclock MSR doesn't clear memory location, it just prevents hypervisor from updating the location so for the short while after write and while CPU is still alive, the clock remains usable and correct so we don't need to switch to some other clocksource.	N/A	More Details
CVE-2021-47111	In the Linux kernel, the following vulnerability has been resolved: xen-netback: take a reference to the RX task thread Do this in order to prevent the task from being freed if the thread returns (which can be triggered by the frontend) before the call to kthread_stop done as part of the backend tear down. Not taking the reference will lead to a use-after-free in that scenario. Such reference was taken before but dropped as part of the rework done in 2ac061ce97f4. Reintroduce the reference taking and add a comment this time explaining why it's needed. This is XSA-374 / CVE-2021-28691.	N/A	More Details
CVE-2021-47112	In the Linux kernel, the following vulnerability has been resolved: x86/kvm: Teardown PV features on boot CPU as well Various PV features (Async PF, PV EOI, steal time) work through memory shared with hypervisor and when we restore from hibernation we must properly teardown all these features to make sure hypervisor doesn't write to stale locations after we jump to the previously hibernated kernel (which can try to place anything there). For secondary CPUs the job is already done by kvm_cpu_down_prepare(), register syscore ops to do the same for boot CPU.	N/A	More Details
CVE-2021-47113	In the Linux kernel, the following vulnerability has been resolved: btrfs: abort in rename_exchange if we fail to insert the second ref Error injection stress uncovered a problem where we'd leave a dangling inode ref if we failed during a rename_exchange. This happens because we insert the inode ref for one side of the rename, and then for the other side. If this second inode ref insert fails we'll leave the first one dangling and leave a corrupt file system behind. Fix this by aborting if we did the insert for the first inode ref.	N/A	More Details
CVE-2021-47115	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.	N/A	More Details
CVE-2021-47116	In the Linux kernel, the following vulnerability has been resolved: ext4: fix memory leak in ext4_mb_init_backend on error path. Fix a memory leak discovered by syzbot when a file system is corrupted with an illegally large s_log_groups_per_flex.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47117	In the Linux kernel, the following vulnerability has been resolved: ext4: fix bug on in ext4_es_cache_extent as ext4_split_extent_at failed We got follow bug_on when run fsstress with injecting IO fault: [130747.323114] kernel BUG at fs/ext4/extents_status.c:762! [130747.323117] Internal error: Oops - BUG: 0 [#1] SMP ..... [130747.334329] Call trace: [130747.334553] ext4_es_cache_extent+0x150/0x168 [ext4] [130747.334975] ext4_cache_extents+0x64/0xe8 [ext4] [130747.335368] ext4_find_extent+0x300/0x330 [ext4] [130747.335759] ext4_ext_map_blocks+0x74/0x1178 [ext4] [130747.336179] ext4_map_blocks+0x2f4/0x5f0 [ext4] [130747.336567] ext4_mpage_readpages+0x4a8/0x7a8 [ext4] [130747.336995] ext4_readpage+0x54/0x100 [ext4] [130747.337359] generic_file_buffered_read+0x410/0xae8 [130747.337767] generic_file_read_iter+0x114/0x190 [130747.338152] ext4_file_read_iter+0x5c/0x140 [ext4] [130747.338556] __vfs_read+0x11c/0x188 [130747.338851] vfs_read+0x94/0x150 [130747.339110] ksys_read+0x74/0xf0 This patch's modification is according to Jan Kara's suggestion in: https://patchwork.ozlabs.org/project/linux-ext4/patch/20210428085158.3728201-1-yebin10@huawei.com/ "I see. Now I understand your patch. Honestly, seeing how fragile is trying to fix extent tree after split has failed in the middle, I would probably go even further and make sure we fix the tree properly in case of ENOSPC and EDQUOT (those are easily user triggerable). Anything else indicates a HW problem or fs corruption so I'd rather leave the extent tree as is and don't try to fix it (which also means we will not create overlapping extents)."	N/A	More Details
CVE-2024-1658	The Grid Shortcodes WordPress plugin before 1.1.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where the shortcode is embed, which could allow users with the contributor role and above to perform Stored Cross-Site Scripting attacks	N/A	More Details
CVE-2021-47119	In the Linux kernel, the following vulnerability has been resolved: ext4: fix memory leak in ext4_fill_super Buffer head references must be released before calling kill_bdev(); otherwise the buffer head (and its page referenced by b_data) will not be freed by kill_bdev, and subsequently that bh will be leaked. If blocksizes differ, sb_set_blocksize() will kill current buffers and page cache by using kill_bdev(). And then super block will be reread again but using correct blocksize this time. sb_set_blocksize() didn't fully free superblock page and buffer head, and being busy, they were not freed and instead leaked. This can easily be reproduced by calling an infinite loop of: systemctl start <ext4_on_lvm>.mount, and systemctl stop <ext4_on_lvm>.mount ... since systemd creates a cgroup for each slice which it mounts, and the bh leak get amplified by a dying memory cgroup that also never gets freed, and memory consumption is much more easily noticed.	N/A	More Details
CVE-2021-47121	In the Linux kernel, the following vulnerability has been resolved: net: caif: fix memory leak in cfusbl_device_notify In case of caif_enroll_dev() fail, allocated link_support won't be assigned to the corresponding structure. So simply free allocated pointer in case of error.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-28069	A vulnerability in the legacy chat component of Mitel MiContact Center Business through 10.0.0.4 could allow an unauthenticated attacker to conduct an information disclosure attack due to improper configuration. A successful exploit could allow an attacker to access sensitive information and potentially conduct unauthorized actions within the vulnerable component.	N/A	More Details
CVE-2021-47122	In the Linux kernel, the following vulnerability has been resolved: net: caif: fix memory leak in caif_device_notify In case of caif_enroll_dev() fail, allocated link_support won't be assigned to the corresponding structure. So simply free allocated pointer in case of error	N/A	More Details
CVE-2021-47123	In the Linux kernel, the following vulnerability has been resolved: io_uring: fix ltout double free on completion race Always remove linked timeout on io_link_timeout_fn() from the master request link list, otherwise we may get use-after-free when first io_link_timeout_fn() puts linked timeout in the fail path, and then will be found and put on master's free.	N/A	More Details
CVE-2021-47124	In the Linux kernel, the following vulnerability has been resolved: io_uring: fix link timeout refs WARNING: CPU: 0 PID: 10242 at lib/refcount.c:28 refcount_warn_saturate+0x15b/0x1a0 lib/refcount.c:28 RIP: 0010:refcount_warn_saturate+0x15b/0x1a0 lib/refcount.c:28 Call Trace: __refcount_sub_and_test include/linux/refcount.h:283 [inline] __refcount_dec_and_test include/linux/refcount.h:315 [inline] refcount_dec_and_test include/linux/refcount.h:333 [inline] io_put_req fs/io_uring.c:2140 [inline] io_queue_linked_timeout fs/io_uring.c:6300 [inline] __io_queue_sqe+0xbef/0xec0 fs/io_uring.c:6354 io_submit_sqe fs/io_uring.c:6534 [inline] io_submit_sqes+0x2bbd/0x7c50 fs/io_uring.c:6660 __do_sys_io_uring_enter fs/io_uring.c:9240 [inline] __se_sys_io_uring_enter+0x256/0x1d60 fs/io_uring.c:9182 io_link_timeout_fn() should put only one reference of the linked timeout request, however in case of racing with the master request's completion first io_req_complete() puts one and then io_put_req_deferred() is called.	N/A	More Details
CVE-2021-47125	In the Linux kernel, the following vulnerability has been resolved: sch_htb: fix refcount leak in htb_parent_to_leaf_offload The commit ae81feb7338c ("sch_htb: fix null pointer dereference on a null new_q") fixes a NULL pointer dereference bug, but it is not correct. Because htb_graft_helper properly handles the case when new_q is NULL, and after the previous patch by skipping this call which creates an inconsistency : dev_queue->qdisc will still point to the old qdisc, but cl->parent->leaf.q will point to the new one (which will be noop_qdisc, because new_q was NULL). The code is based on an assumption that these two pointers are the same, so it can lead to refcount leaks. The correct fix is to add a NULL pointer check to protect qdisc_refcount_inc inside htb_parent_to_leaf_offload.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47127	In the Linux kernel, the following vulnerability has been resolved: ice: track AF_XDP ZC enabled queues in bitmap Commit c7a219048e45 ("ice: Remove xsk_buff_pool from VSI structure") silently introduced a regression and broke the Tx side of AF_XDP in copy mode. xsk_pool on ice_ring is set only based on the existence of the XDP prog on the VSI which in turn picks ice_clean_tx_irq_zc to be executed. That is not something that should happen for copy mode as it should use the regular data path ice_clean_tx_irq. This results in a following splat when xdpsock is run in txonly or l2fwd scenarios in copy mode: <snip> [106.050195] BUG: kernel NULL pointer dereference, address: 0000000000000030 [106.057269] #PF: supervisor read access in kernel mode [106.062493] #PF: error_code(0x0000) - not-present page [106.067709] PGD 0 P4D 0 [106.070293] Oops: 0000 [#1] PREEMPT SMP NOPTI [106.074721] CPU: 61 PID: 0 Comm: swapper/61 Not tainted 5.12.0-rc2+ #45 [106.081436] Hardware name: Intel Corporation S2600WFT/S2600WFT, BIOS SE5C620.86B.02.01.0008.031920191559 03/19/2019 [106.092027] RIP: 0010:xp_raw_get_dma+0x36/0x50 [106.096551] Code: 74 14 48 b8 ff ff ff ff ff ff 00 00 48 21 f0 48 c1 ee 30 48 01 c6 48 8b 87 90 00 00 00 48 89 f2 81 e6 ff 0f 00 00 48 c1 ea 0c <48> 8b 04 d0 48 83 e0 fe 48 01 f0 c3 66 66 2e 0f 1f 84 00 00 00 00 [106.115588] RSP: 0018:ffffc9000d694e50 EFLAGS: 00010206 [106.120893] RAX: 0000000000000000 RBX: ffff88984b8c8a00 RCX: ffff889852581800 [106.128137] RDX: 0000000000000006 RSI: 0000000000000000 RDI: ffff88984cd8b800 [106.135383] RBP: ffff888123b50001 R08: ffff889896800000 R09: 0000000000000800 [106.142628] R10: 0000000000000000 R11: ffffffff826060c0 R12: 00000000000000ff [106.149872] R13: 0000000000000000 R14: 0000000000000040 R15: ffff888123b50018 [106.157117] FS: 0000000000000000(0000) GS:ffff8897e0f40000(0000) knlGS:0000000000000000 [106.165332] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [106.171163] CR2: 0000000000000030 CR3: 000000000560a004 CR4: 00000000007706e0 [106.178408] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [106.185653] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [106.192898] PKRU: 55555554 [106.195653] Call Trace: [106.198143] <IRQ> [106.200196] ice_clean_tx_irq_zc+0x183/0x2a0 [ice] [106.205087] ice_napi_poll+0x3e/0x590 [ice] [106.209356] __napi_poll+0x2a/0x160 [106.212911] net_rx_action+0xd6/0x200 [106.216634] __do_softirq+0xbf/0x29b [106.220274] irq_exit_rcu+0x88/0xc0 [106.223819] common_interrupt+0x7b/0xa0 [106.227719] </IRQ> [106.229857] asm_common_interrupt+0x1e/0x40 </snip> Fix this by introducing the bitmap of queues that are zero-copy enabled, where each bit, corresponding to a queue id that xsk pool is being configured on, will be set/cleared within ice_xsk_pool_{en,dis}able and checked within ice_xsk_pool(). The latter is a function used for deciding which napi poll routine is executed. Idea is being taken from our other drivers such as i40e and ixgbe.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47128	In the Linux kernel, the following vulnerability has been resolved: bpf, lockdown, audit: Fix buggy SELinux lockdown permission checks Commit 59438b46471a ("security,lockdown,selinux: implement SELinux lockdown") added an implementation of the locked_down LSM hook to SELinux, with the aim to restrict which domains are allowed to perform operations that would breach lockdown. This is indirectly also getting audit subsystem involved to report events. The latter is problematic, as reported by Ondrej and Serhei, since it can bring down the whole system via audit: 1) The audit events that are triggered due to calls to security_locked_down() can OOM kill a machine, see below details [0]. 2) It also seems to be causing a deadlock via avc_has_perm()/slow_avc_audit() when trying to wake up kauditd, for example, when using trace_sched_switch() tracepoint, see details in [1]. Triggering this was not via some hypothetical corner case, but with existing tools like runqlat & runqslower from bcc, for example, which make use of this tracepoint. Rough call sequence goes like: rq_lock(rq) -> ------------------------+ trace_sched_switch() ->	bpf_prog_xyz() -> +-> deadlock selinux_lockdown() ->	audit_log_end() ->	wake_up_interruptible() ->	try_to_wake_up() ->	rq_lock(rq) ----------+ What's worse is that the intention of 59438b46471a to further restrict lockdown settings for specific applications in respect to the global lockdown policy is completely broken for BPF. The SELinux policy rule for the current lockdown check looks something like this: allow <who> <who> : lockdown { <reason> }; However, this doesn't match with the 'current' task where the security_locked_down() is executed, example: httpd does a syscall. There is a tracing program attached to the syscall which triggers a BPF program to run, which ends up doing a bpf_probe_read_kernel{,_str}() helper call. The selinux_lockdown() hook does the permission check against 'current', that is, httpd in this example. httpd has literally zero relation to this tracing program, and it would be nonsensical having to write an SELinux policy rule against httpd to let the tracing helper pass. The policy in this case needs to be against the entity that is installing the BPF program. For example, if bpftrace would generate a histogram of syscall counts by user space application: bpftrace -e 'tracepoint:raw_syscalls:sys_enter { @[comm] = count(); }' bpftrace would then go and generate a BPF program from this internally. One way of doing it [for the sake of the example] could be to call bpf_get_current_task() helper and then access current->comm via one of bpf_probe_read_kernel{,_str}() helpers. So the program itself has nothing to do with httpd or any other random app doing a syscall here. The BPF program _explicitly initiated_ the lockdown check. The allow/deny policy belongs in the context of bpftrace: meaning, you want to grant bpftrace access to use these helpers, but other tracers on the system like my_random_tracer _not_. Therefore fix all three issues at the same time by taking a completely different approach for the security_locked_down() hook, that is, move the check into the program verification phase where we actually retrieve the BPF func proto. This also reliably gets the task (current) that is trying to install the BPF tracing program, e.g. bpftrace/bcc/perf/systemtap/etc, and it also fixes the OOM since we're moving this out of the BPF helper's fast-path which can be called several millions of times per second. The check is then also in line with other security_locked_down() hooks in the system where the enforcement is performed at open/load time, for example, open_kcore() for /proc/kcore access or module_sig_check() for module signatures just to pick f ---truncated---	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47131	In the Linux kernel, the following vulnerability has been resolved: net/tls: Fix use-after-free after the TLS device goes down and up When a netdev with active TLS offload goes down, tls_device_down is called to stop the offload and tear down the TLS context. However, the socket stays alive, and it still points to the TLS context, which is now deallocated. If a netdev goes up, while the connection is still active, and the data flow resumes after a number of TCP retransmissions, it will lead to a use-after-free of the TLS context. This commit addresses this bug by keeping the context alive until its normal destruction, and implements the necessary fallbacks, so that the connection can resume in software (non-offloaded) kTLS mode. On the TX side tls_sw_fallback is used to encrypt all packets. The RX side already has all the necessary fallbacks, because receiving non-decrypted packets is supported. The thing needed on the RX side is to block resync requests, which are normally produced after receiving non-decrypted packets. The necessary synchronization is implemented for a graceful teardown: first the fallbacks are deployed, then the driver resources are released (it used to be possible to have a tls_dev_resync after tls_dev_del). A new flag called TLS_RX_DEV_DEGRADED is added to indicate the fallback mode. It's used to skip the RX resync logic completely, as it becomes useless, and some objects may be released (for example, resync_async, which is allocated and freed by the driver).	N/A	More Details
CVE-2021-47132	In the Linux kernel, the following vulnerability has been resolved: mptcp: fix sk_forward_memory corruption on retransmission MPTCP sk_forward_memory handling is a bit special, as such field is protected by the msk socket spin_lock, instead of the plain socket lock. Currently we have a code path updating such field without handling the relevant lock: __mptcp_retrans() -> __mptcp_clean_una_wakeup() Several helpers in __mptcp_clean_una_wakeup() will update sk_forward_alloc, possibly causing such field corruption, as reported by Matthieu. Address the issue providing and using a new variant of blamed function which explicitly acquires the msk spin lock.	N/A	More Details
CVE-2021-47133	In the Linux kernel, the following vulnerability has been resolved: HID: amd_sfh: Fix memory leak in amd_sfh_work Kmemleak tool detected a memory leak in the amd_sfh driver. ========== unreferenced object 0xffff88810228ada0 (size 32): comm "insmod", pid 3968, jiffies 4295056001 (age 775.792s) hex dump (first 32 bytes): 00 20 73 1f 81 88 ff ff 00 01 00 00 00 00 ad de . s..... 22 01 00 00 00 00 ad de 01 00 02 00 00 00 00 00 "..... backtrace: [<000000007b4c8799>] kmem_cache_alloc_trace+0x163/0x4f0 [<0000000005326893>] amd_sfh_get_report+0xa4/0x1d0 [amd_sfh] [<000000002a9e5ec4>] amdtp_hid_request+0x62/0x80 [amd_sfh] [<00000000b8a95807>] sensor_hub_get_feature+0x145/0x270 [hid_sensor_hub] [<00000000fda054ee>] hid_sensor_parse_common_attributes+0x215/0x460 [hid_sensor_iio_common] [<0000000021279ecf>] hid_accel_3d_probe+0xff/0x4a0 [hid_sensor_accel_3d] [<00000000915760ce>] platform_probe+0x6a/0xd0 [<0000000060258a1f>] really_probe+0x192/0x620 [<00000000fa812f2d>] driver_probe_device+0x14a/0x1d0 [<000000005e79f7fd>] __device_attach_driver+0xbd/0x110 [<0000000070d15018>] bus_for_each_drv+0xfd/0x160 [<0000000013a3c312>] __device_attach+0x18b/0x220 [<000000008c7b4afc>] device_initial_probe+0x13/0x20 [<00000000e6e99665>] bus_probe_device+0xfe/0x120 [<00000000833fa90b>] device_add+0x6a6/0xe00 [<00000000fa901078>] platform_device_add+0x180/0x380 ========== The fix is to freeing request_list entry once the processed entry is removed from the request_list.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47134	In the Linux kernel, the following vulnerability has been resolved: efi/fdt: fix panic when no valid fdt found setup_arch() would invoke efi_init()->efi_get_fdt_params(). If no valid fdt found then initial_boot_params will be null. So we should stop further fdt processing here. I encountered this issue on risc-v.	N/A	More Details
CVE-2021-47135	In the Linux kernel, the following vulnerability has been resolved: mt76: mt7921: fix possible AOOB issue in mt7921_mcu_tx_rate_report Fix possible array out of bound access in mt7921_mcu_tx_rate_report. Remove unnecessary varibable in mt7921_mcu_tx_rate_report	N/A	More Details
CVE-2024-2608	`AppendEncodedAttributeValue(), ExtraSpaceNeededForAttrEncoding()` and `AppendEncodedCharacters()` could have experienced integer overflows, causing underallocation of an output buffer leading to an out of bounds write. This vulnerability affects Firefox < 124, Firefox ESR < 115.9, and Thunderbird < 115.9.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-47118	In the Linux kernel, the following vulnerability has been resolved: pid: take a reference when initializing `cad_pid` During boot, kernel_init_freeable() initializes `cad_pid` to the init task's struct pid. Later on, we may change `cad_pid` via a sysctl, and when this happens proc_do_cad_pid() will increment the refcount on the new pid via get_pid(), and will decrement the refcount on the old pid via put_pid(). As we never called get_pid() when we initialized `cad_pid`, we decrement a reference we never incremented, can therefore free the init task's struct pid early. As there can be dangling references to the struct pid, we can later encounter a use-after-free (e.g. when delivering signals). This was spotted when fuzzing v5.13-rc3 with Syzkaller, but seems to have been around since the conversion of `cad_pid` to struct pid in commit 9ec52099e4b8 ("[PATCH] replace cad_pid by a struct pid") from the pre-KASAN stone age of v2.6.19. Fix this by getting a reference to the init task's struct pid when we assign it to `cad_pid`. Full KASAN splat below. == BUG: KASAN: use-after-free in ns_of_pid include/linux/pid.h:153 [inline] BUG: KASAN: use-after-free in task_active_pid_ns+0xc0/0xc8 kernel/pid.c:509 Read of size 4 at addr ffff23794dda0004 by task syz-executor.0/273 CPU: 1 PID: 273 Comm: syz-executor.0 Not tainted 5.12.0-00001-g9aef892b2d15 #1 Hardware name: linux,dummy-virt (DT) Call trace: ns_of_pid include/linux/pid.h:153 [inline] task_active_pid_ns+0xc0/0xc8 kernel/pid.c:509 do_notify_parent+0x308/0xe60 kernel/signal.c:1950 exit_notify kernel/exit.c:682 [inline] do_exit+0x2334/0x2bd0 kernel/exit.c:845 do_group_exit+0x108/0x2c8 kernel/exit.c:922 get_signal+0x4e4/0x2a88 kernel/signal.c:2781 do_signal arch/arm64/kernel/signal.c:882 [inline] do_notify_resume+0x300/0x970 arch/arm64/kernel/signal.c:936 work_pending+0xc/0x2dc Allocated by task 0: slab_post_alloc_hook+0x50/0x5c0 mm/slab.h:516 slab_alloc_node mm/slub.c:2907 [inline] slab_alloc mm/slub.c:2915 [inline] kmem_cache_alloc+0x1f4/0x4c0 mm/slub.c:2920 alloc_pid+0xdc/0xc00 kernel/pid.c:180 copy_process+0x2794/0x5e18 kernel/fork.c:2129 kernel_clone+0x194/0x13c8 kernel/fork.c:2500 kernel_thread+0xd4/0x110 kernel/fork.c:2552 rest_init+0x44/0x4a0 init/main.c:687 arch_call_rest_init+0x1c/0x28 start_kernel+0x520/0x554 init/main.c:1064 0x0 Freed by task 270: slab_free_hook mm/slub.c:1562 [inline] slab_free_freelist_hook+0x98/0x260 mm/slub.c:1600 slab_free mm/slub.c:3161 [inline] kmem_cache_free+0x224/0x8e0 mm/slub.c:3177 put_pid.part.4+0xe0/0x1a8 kernel/pid.c:114 put_pid+0x30/0x48 kernel/pid.c:109 proc_do_cad_pid+0x190/0x1b0 kernel/sysctl.c:1401 proc_sys_call_handler+0x338/0x4b0 fs/proc/proc_sysctl.c:591 proc_sys_write+0x34/0x48 fs/proc/proc_sysctl.c:617 call_write_iter include/linux/fs.h:1977 [inline] new_sync_write+0x3ac/0x510 fs/read_write.c:518 vfs_write fs/read_write.c:605 [inline] vfs_write+0x9c4/0x1018 fs/read_write.c:585 ksys_write+0x124/0x240 fs/read_write.c:658 __do_sys_write fs/read_write.c:670 [inline] __se_sys_write fs/read_write.c:667 [inline] __arm64_sys_write+0x78/0xb0 fs/read_write.c:667 __invoke_syscall arch/arm64/kernel/syscall.c:37 [inline] invoke_syscall arch/arm64/kernel/syscall.c:49 [inline] el0_svc_common.constprop.1+0x16c/0x388 arch/arm64/kernel/syscall.c:129 do_el0_svc+0xf8/0x150 arch/arm64/kernel/syscall.c:168 el0_svc+0x28/0x38 arch/arm64/kernel/entry-common.c:416 el0_sync_handler+0x134/0x180 arch/arm64/kernel/entry-common.c:432 el0_sync+0x154/0x180 arch/arm64/kernel/entry.S:701 The buggy address belongs to the object at ffff23794dda0000 which belongs to the cache pid of size 224 The buggy address is located 4 bytes inside of 224-byte region [ff ---truncated---	N/A	More Details

CVE Number	Description	Base Score	Reference