SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 16 October 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-2024-47875	DOMPurify is a DOM-only, super-fast, uber-tolerant XSS sanitizer for HTML, MathML and SVG. DOMpurify was vulnerable to nesting-based mXSS. This vulnerability is fixed in 2.5.0 and 3.1.3.	10.0	More Details
CVE-2024-9985	Enterprise Cloud Database from Ragic does not properly validate the file type for uploads. Attackers with regular privileges can upload a webshell and use it to execute arbitrary code on the remote server.	10.0	More Details
CVE-2024-9924	The fix for CVE-2024-26261 was incomplete, and and the specific package for OAKlouds from Hgiga remains at risk. Unauthenticated remote attackers still can download arbitrary system files, which may be deleted subsequently .	9.8	More Details
CVE-2024-46088	An arbitrary file upload vulnerability in the ProductAction.entphone interface of Zhejiang University Entersoft Customer Resource Management System v2002 to v2024 allows attackers to execute arbitrary code via uploading a crafted file.	9.8	More Details
CVE-2024-46532	SQL Injection vulnerability in OpenHIS v.1.0 allows an attacker to execute arbitrary code via the refund function in the PayController.class.php component.	9.8	More Details
CVE-2024-48033	Deserialization of Untrusted Data vulnerability in Elie Burstein, Baptiste Gourdin Talkback allows Object Injection.This issue affects Talkback: from n/a through 1.0.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48283	Phpgurukul User Registration & Login and User Management System 3.2 is vulnerable to SQL Injection in /admin//search-result.php via the searchkey parameter.	9.8	More Details
CVE-2024-48784	An Incorrect Access Control issue in SAMPMAX com.sampmax.homemax 2.1.2.7 allows a remote attacker to obtain sensitive information via the firmware update process.	9.8	More Details
CVE-2024-45275	The devices contain two hard coded user accounts with hardcoded passwords that allow an unauthenticated remote attacker for full control of the affected devices.	9.8	More Details
CVE-2024-45274	An unauthenticated remote attacker can execute OS commands via UDP on the device due to missing authentication.	9.8	More Details
CVE-2024-47945	The devices are vulnerable to session hijacking due to insufficient entropy in its session ID generation algorithm. The session IDs are predictable, with only 32,768 possible values per user, which allows attackers to pre-generate valid session IDs, leading to unauthorized access to user sessions. This is not only due to the use of an (insecure) rand() function call but also because of missing initialization via srand(). As a result only the PIDs are effectively used as seed.	9.8	More Details
CVE-2024-9047	The WordPress File Upload plugin for WordPress is vulnerable to Path Traversal in all versions up to, and including, 4.24.11 via wfu_file_downloader.php. This makes it possible for unauthenticated attackers to read or delete files outside of the originally intended directory. Successful exploitation requires the targeted WordPress installation to be using PHP 7.4 or earlier.	9.8	More Details
CVE-2024-9921	The Team+ from TEAMPLUS TECHNOLOGY does not properly validate specific page parameter, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify and delete database contents.	9.8	More Details
CVE-2024-32608	HDF5 library through 1.14.3 has memory corruption in H5A__close resulting in the corruption of the instruction pointer and causing denial of service or potential code execution.	9.8	More Details
CVE-2024-9984	Enterprise Cloud Database from Ragic does not authenticate access to specific functionality, allowing unauthenticated remote attackers to use this functionality to obtain any user's session cookie.	9.8	More Details
CVE-2024-48255	Cloudlog 2.6.15 allows Oqrs.php get_station_info station_id SQL injection.	9.8	More Details
CVE-2024-48251	Wavelog 1.8.5 allows Activated_gridmap_model.php get_band_confirmed SQL injection via band, sat, propagation, or mode.	9.8	More Details
CVE-2024-48257	Wavelog 1.8.5 allows Oqrs_model.php get_worked_modes station_id SQL injectioin.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48150	D-Link DIR-820L 1.05B03 has a stack overflow vulnerability in the sub_451208 function.	9.8	More Details
CVE-2024-48153	DrayTek Vigor3900 1.5.1.3 allows attackers to inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the get_subconfig function.	9.8	More Details
CVE-2024-46535	Jepaas v7.2.8 was discovered to contain a SQL injection vulnerability via the orderSQL parameter at /homePortal/loadUserMsg.	9.8	More Details
CVE-2024-48168	A stack overflow vulnerability exists in the sub_402280 function of the HNAP service of D-Link DCS-960L 1.09, allowing an attacker to execute arbitrary code.	9.8	More Details
CVE-2024-48823	Local file inclusion in Automatic Systems Maintenance SlimLane 29565_d74ecce0c1081d50546db573a499941b10799fb7 allows a remote attacker to escalate privileges via the PassageAutoServer.php page.	9.8	More Details
CVE-2024-9972	Property Management System from ChanGate has a SQL Injection vulnerability, allowing unauthenticated remote attackers to inject arbitrary SQL commands to read, modify, and delete database contents.	9.8	More Details
CVE-2024-9982	AIM LINE Marketing Platform from Esi Technology does not properly validate a specific query parameter. When the LINE Campaign Module is enabled, unauthenticated remote attackers can inject arbitrary FetchXml commands to read, modify, and delete database content.	9.8	More Details
CVE-2024-48253	Cloudlog 2.6.15 allows Oqrs.php delete_oqrs_line id SQL injection.	9.8	More Details
CVE-2024-9925	SQL injection vulnerability in TAI Smart Factory's QPLANT SF version 1.0. Exploitation of this vulnerability could allow a remote attacker to retrieve all database information by sending a specially crafted SQL query to the ‘email’ parameter on the ‘RequestPasswordChange’ endpoint.	9.8	More Details
CVE-2024-42640	angular-base64-upload prior to v0.1.21 is vulnerable to unauthenticated remote code execution via demo/server.php. Exploiting this vulnerability allows an attacker to upload arbitrary content to the server, which can subsequently be accessed through demo/uploads. This leads to the execution of previously uploaded content and enables the attacker to achieve code execution on the server. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2024-45746	An issue was discovered in Trusted Firmware-M through 2.1.0. User provided (and controlled) mailbox messages contain a pointer to a list of input arguments (in_vec) and output arguments (out_vec). These list pointers are never validated. Each argument list contains a buffer pointer and a buffer length field. After a PSA call, the length of the output arguments behind the unchecked pointer is updated in mailbox_direct_reply, regardless of the call result. This allows an attacker to write anywhere in the secure firmware, which can be used to take over the control flow, leading to remote code execution (RCE).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48779	An issue in Wanxing Technology's Yitu project Management Software 3.2.2 allows a remote attacker to execute arbitrary code via the platformpluginpath parameter to specify that the qt plugin loads the directory.	9.8	More Details
CVE-2024-9518	The UserPlus plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 2.0 due to insufficient restriction on the 'form_actions' and 'userplus_update_user_profile' functions. This makes it possible for unauthenticated attackers to specify their user role by supplying the 'role' parameter during a registration.	9.8	More Details
CVE-2024-9796	The WP-Advanced-Search WordPress plugin before 3.3.9.2 does not sanitize and escape the t parameter before using it in a SQL statement, allowing unauthenticated users to perform SQL injection attacks	9.8	More Details
CVE-2024-48411	itsourcecode Online Tours and Travels Management System v1.0 is vulnerable to SQL Injection (SQLI) via a crafted payload to the val-email parameter in forget_password.php.	9.8	More Details
CVE-2024-45115	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in privilege escalation. An attacker could exploit this vulnerability to gain unauthorized access or elevated privileges within the application. Exploitation of this issue does not require user interaction.	9.8	More Details
CVE-2024-25825	FydeOS for PC 17.1 R114, FydeOS for VMware 17.0 R114, FydeOS for You 17.1 R114, and OpenFyde R114 were discovered to be configured with the root password saved as a wildcard. This allows attackers to gain root access without a password.	9.8	More Details
CVE-2024-48782	File Upload vulnerability in DYCMS Open-Source Version v2.0.9.41 allows a remote attacker to execute arbitrary code via the application only detecting the extension of image files in the front-end.	9.8	More Details
CVE-2024-47636	Deserialization of Untrusted Data vulnerability in Eyecix JobSearch allows Object Injection.This issue affects JobSearch: from n/a through 2.5.9.	9.8	More Details
CVE-2024-47167	Gradio is an open-source Python package designed for quick prototyping. This vulnerability relates to **Server-Side Request Forgery (SSRF)** in the `/queue/join` endpoint. Gradio's `async_save_url_to_cache` function allows attackers to force the Gradio server to send HTTP requests to user-controlled URLs. This could enable attackers to target internal servers or services within a local network and possibly exfiltrate data or cause unwanted internal requests. Additionally, the content from these URLs is stored locally, making it easier for attackers to upload potentially malicious files to the server. This impacts users deploying Gradio servers that use components like the Video component which involve URL fetching. Users are advised to upgrade to `gradio>=5` to address this issue. As a workaround, users can disable or heavily restrict URL-based inputs in their Gradio applications to trusted domains only. Additionally, implementing stricter URL validation (such as allowinglist-based validation) and ensuring that local or internal network addresses cannot be requested via the `/queue/join` endpoint can help mitigate the risk of SSRF attacks.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-49195	Mbed TLS 3.5.x through 3.6.x before 3.6.2 has a buffer underrun in pkwrite when writing an opaque key pair	9.8	More Details
CVE-2024-21216	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	9.8	More Details
CVE-2024-9822	The Pedalo Connector plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.0.5. This is due to insufficient restriction on the 'login_admin_user' function. This makes it possible for unauthenticated attackers to log to the first user, who is usually the administrator, or if it does not exist, then to the first administrator.	9.8	More Details
CVE-2024-21534	All versions of the package jsonpath-plus are vulnerable to Remote Code Execution (RCE) due to improper input sanitization. An attacker can execute aribitrary code on the system by exploiting the unsafe default usage of vm in Node. **Note:** There were several attempts to fix it in versions [10.0.0-10.1.0](https://github.com/JSONPath-Plus/JSONPath/compare/v9.0.0...v10.1.0) but it could still be exploited using [different payloads](https://github.com/JSONPath-Plus/JSONPath/issues/226).	9.8	More Details
CVE-2024-9680	An attacker was able to achieve code execution in the content process by exploiting a use-after-free in Animation timelines. We have had reports of this vulnerability being exploited in the wild. This vulnerability affects Firefox < 131.0.2, Firefox ESR < 128.3.1, Firefox ESR < 115.16.1, Thunderbird < 131.0.1, Thunderbird < 128.3.1, and Thunderbird < 115.16.0.	9.8	More Details
CVE-2024-9234	The GutenKit – Page Builder Blocks, Patterns, and Templates for Gutenberg Block Editor plugin for WordPress is vulnerable to arbitrary file uploads due to a missing capability check on the install_and_activate_plugin_from_external() function (install-active-plugin REST API endpoint) in all versions up to, and including, 2.1.0. This makes it possible for unauthenticated attackers to install and activate arbitrary plugins, or utilize the functionality to upload arbitrary files spoofed like plugins.	9.8	More Details
CVE-2024-9707	The Hunk Companion plugin for WordPress is vulnerable to unauthorized plugin installation/activation due to a missing capability check on the /wp-json/hc/v1/themehunk-import REST API endpoint in all versions up to, and including, 1.8.4. This makes it possible for unauthenticated attackers to install and activate arbitrary plugins which can be leveraged to achieve remote code execution if another vulnerable plugin is installed and activated.	9.8	More Details
CVE-2024-9486	A security issue was discovered in the Kubernetes Image Builder versions <= v0.1.37 where default credentials are enabled during the image build process. Virtual machine images built using the Proxmox provider do not disable these default credentials, and nodes using the resulting images may be accessible via these default credentials. The credentials can be used to gain root access. Kubernetes clusters are only affected if their nodes use VM images created via the Image Builder project with its Proxmox provider.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47074	DataEase is an open source data visualization analysis tool. In Dataease, the PostgreSQL data source in the data source function can customize the JDBC connection parameters and the PG server target to be connected. In backend/src/main/java/io/dataease/provider/datasource/JdbcProvider.java, PgConfiguration class don't filter any parameters, directly concat user input. So, if the attacker adds some parameters in JDBC url, and connect to evil PG server, the attacker can trigger the PG jdbc deserialization vulnerability, and eventually the attacker can execute through the deserialization vulnerability system commands and obtain server privileges. The vulnerability has been fixed in v1.18.25.	9.8	More Details
CVE-2024-48781	An issue in Wanxing Technology Yitu Project Management Kirin Edition 2.3.6 allows a remote attacker to execute arbitrary code via a specially constructed so file/opt/EdrawProj-2/plugins/imageformat.	9.8	More Details
CVE-2024-9164	An issue was discovered in GitLab EE affecting all versions starting from 12.5 prior to 17.2.9, starting from 17.3, prior to 17.3.5, and starting from 17.4 prior to 17.4.2, which allows running pipelines on arbitrary branches.	9.6	More Details
CVE-2024-9137	The affected product lacks an authentication check when sending commands to the server via the Moxa service. This vulnerability allows an attacker to execute specified commands, potentially leading to unauthorized downloads or uploads of configuration files and system compromise.	9.4	More Details
CVE-2024-9201	The SEUR plugin, in its versions prior to 2.5.11, is vulnerable to time-based SQL injection through the use of the ‘id_order’ parameter of the ‘/modules/seur/ajax/saveCodFee.php’ endpoint.	9.4	More Details
CVE-2024-47830	Plane is an open-source project management tool. Plane uses the ** wildcard support to retrieve the image from any hostname as in /web/next.config.js. This may permit an attacker to induce the server side into performing requests to unintended locations. This vulnerability is fixed in 0.23.0.	9.3	More Details
CVE-2024-47331	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in NinjaTeam Multi Step for Contact Form allows SQL Injection.This issue affects Multi Step for Contact Form: from n/a through 2.7.7.	9.3	More Details
CVE-2024-49388	Sensitive information manipulation due to improper authorization. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 38690.	9.1	More Details
CVE-2024-48914	Vendure is an open-source headless commerce platform. Prior to versions 3.0.5 and 2.3.3, a vulnerability in Vendure's asset server plugin allows an attacker to craft a request which is able to traverse the server file system and retrieve the contents of arbitrary files, including sensitive data such as configuration files, environment variables, and other critical data stored on the server. In the same code path is an additional vector for crashing the server via a malformed URI. Patches are available in versions 3.0.5 and 2.3.3. Some workarounds are also available. One may use object storage rather than the local file system, e.g. MinIO or S3, or define middleware which detects and blocks requests with urls containing `/../`.	9.1	More Details
CVE-2024-48787	An issue in Revic Optics Revic Ops (us.revic.revicops) 1.12.5 allows a remote attacker to obtain sensitive information via the firmware update process.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-48082	Nagios XI before 2024R1 was discovered to improperly handle API keys generation (randomly-generated), allowing attackers to possibly generate the same set of API keys for all users and utilize them to authenticate.	9.1	More Details
CVE-2024-48772	An issue in C-CHIP (com.cchip.cchipamaota) v.1.2.8 allows a remote attacker to obtain sensitive information via the firmware update process.	9.1	More Details
CVE-2024-45160	Incorrect credential validation in LemonLDAP::NG 2.18.x and 2.19.x before 2.19.2 allows attackers to bypass OAuth2 client authentication via an empty client_password parameter (client secret).	9.1	More Details
CVE-2024-48786	An issue in SWITCHBOT INC SwitchBot (com.theswitchbot.switchbot) 5.0.4 allows a remote attacker to obtain sensitive information via the firmware update process.	9.1	More Details
CVE-2024-48778	An issue in GIANT MANUFACTURING CO., LTD RideLink (tw.giant.ridelink) 2.0.7 allows a remote attacker to obtain sensitive information via the firmware update process.	9.1	More Details
CVE-2024-48769	An issue in BURG-WCHTER KG de.burgwachter.keyapp.app 4.5.0 allows a remote attacker to obtain sensitve information via the firmware update process.	9.1	More Details
CVE-2024-44730	Incorrect access control in the function handleDataChannelChat(dataMessage) of Mirotalk before commit c21d58 allows attackers to forge chat messages using an arbitrary sender name.	9.1	More Details
CVE-2024-47871	Gradio is an open-source Python package designed for quick prototyping. This vulnerability involves **insecure communication** between the FRP (Fast Reverse Proxy) client and server when Gradio's `share=True` option is used. HTTPS is not enforced on the connection, allowing attackers to intercept and read files uploaded to the Gradio server, as well as modify responses or data sent between the client and server. This impacts users who are sharing Gradio demos publicly over the internet using `share=True` without proper encryption, exposing sensitive data to potential eavesdroppers. Users are advised to upgrade to `gradio>=5` to address this issue. As a workaround, users can avoid using `share=True` in production environments and instead host their Gradio applications on servers with HTTPS enabled to ensure secure communication.	9.1	More Details
CVE-2024-9487	An improper verification of cryptographic signature vulnerability was identified in GitHub Enterprise Server that allowed SAML SSO authentication to be bypassed resulting in unauthorized provisioning of users and access to the instance. Exploitation required the encrypted assertions feature to be enabled, and the attacker would require direct network access as well as a signed SAML response or metadata document. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.15 and was fixed in versions 3.11.16, 3.12.10, 3.13.5, and 3.14.2. This vulnerability was reported via the GitHub Bug Bounty program.	9.1	More Details
CVE-2024-48949	The verify function in lib/elliptic/eddsa/index.js in the Elliptic package before 6.5.6 for Node.js omits "sig.S().gte(sig.eddsa.curve.n) ll sig.S().isNeg()" validation.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9465	An SQL injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to reveal Expedition database contents, such as password hashes, usernames, device configurations, and device API keys. With this, attackers can also create and read arbitrary files on the Expedition system.	9.1	More Details
CVE-2024-8015	In Progress Telerik Report Server versions prior to 2024 Q3 (10.2.24.924), a remote code execution attack is possible through object injection via an insecure type resolution vulnerability.	9.1	More Details
CVE-2023-46586	cgi.c in weborf .0.17, 0.18, 0.19, and 0.20 (before 1.0) lacks '\0' termination of the path for CGI scripts because strncpy is misused.	9.1	More Details
CVE-2024-10004	Opening an external link to an HTTP website when Firefox iOS was previously closed and had an HTTPS tab open could in some cases result in the padlock icon showing an HTTPS indicator incorrectly This vulnerability affects Firefox for iOS < 131.2.	9.1	More Details
CVE-2024-21172	Vulnerability in the Oracle Hospitality OPERA 5 product of Oracle Hospitality Applications (component: Opera Servlet). Supported versions that are affected are 5.6.19.19, 5.6.25.8 and 5.6.26.4. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality OPERA 5. While the vulnerability is in Oracle Hospitality OPERA 5, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Hospitality OPERA 5. CVSS 3.1 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).	9.0	More Details
CVE-2024-9798	The health endpoint is public so everybody can see a list of all services. It is potentially valuable information for attackers.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-9783	A vulnerability was found in D-Link DIR-619L B1 2.06. It has been rated as critical. This issue affects the function formLogDnsquery of the file /goform/formLogDnsquery. The manipulation of the argument curTime leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9971	The specific query functionality in the FlowMaster BPM Plus from NewType does not properly restrict user input, allowing remote attackers with regular privileges to inject SQL commands to read, modify, or delete database contents.	8.8	More Details
CVE-2024-9981	The ee-class from FormosaSoft does not properly validate a specific page parameter, allowing remote attackers with regular privileges to upload a malicious PHP file first and then exploit this vulnerability to include the file, resulting in arbitrary code execution on the server.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9915	A vulnerability classified as critical was found in D-Link DIR-619L B1 2.06. Affected by this vulnerability is the function formVirtualServ of the file /goform/formVirtualServ. The manipulation of the argument curTime leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9914	A vulnerability classified as critical has been found in D-Link DIR-619L B1 2.06. Affected is the function formSetWizardSelectMode of the file /goform/formSetWizardSelectMode. The manipulation of the argument curTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9913	A vulnerability was found in D-Link DIR-619L B1 2.06. It has been rated as critical. This issue affects the function formSetRoute of the file /goform/formSetRoute. The manipulation of the argument curTime leads to buffer overflow. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9912	A vulnerability was found in D-Link DIR-619L B1 2.06. It has been declared as critical. This vulnerability affects the function formSetQoS of the file /goform/formSetQoS. The manipulation of the argument curTime leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9522	The WP Users Masquerade plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.0.0. This is due to incorrect authentication and capability checking in the 'ajax_masq_login' function. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to log in as any existing user on the site, such as an administrator.	8.8	More Details
CVE-2024-9911	A vulnerability was found in D-Link DIR-619L B1 2.06. It has been classified as critical. This affects the function formSetPortTr of the file /goform/formSetPortTr. The manipulation of the argument curTime leads to buffer overflow. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9910	A vulnerability was found in D-Link DIR-619L B1 2.06 and classified as critical. Affected by this issue is the function formSetPassword of the file /goform/formSetPassword. The manipulation of the argument curTime leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9909	A vulnerability has been found in D-Link DIR-619L B1 2.06 and classified as critical. Affected by this vulnerability is the function formSetMuti of the file /goform/formSetMuti. The manipulation of the argument curTime leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-9821	The Bot for Telegram on WooCommerce plugin for WordPress is vulnerable to sensitive information disclosure due to missing authorization checks on the 'stm_wpcfto_get_settings' AJAX action in all versions up to, and including, 1.2.4. This makes it possible for authenticated attackers, with subscriber-level access and above, to view the Telegram Bot Token, a secret token used to control the bot, which can then be used to log in as any existing user on the site, such as an administrator, if they know the username, due to the Login with Telegram feature.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35584	SQL injection vulnerabilities were discovered in Ajax.php, ForWindow.php, ForExport.php, Modules.php, functions/HackingLogFnc.php in OpenSis Community Edition 9.1 to 8.0, and possibly earlier versions. It is possible for an authenticated user to perform SQL Injection due to the lack to sanitisation. The application takes arbitrary value from "X-Forwarded-For" header and appends it to a SQL INSERT statement directly, leading to SQL Injection.	8.8	More Details
CVE-2024-21254	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Web Server). Supported versions that are affected are 7.0.0.0.0, 7.6.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in takeover of Oracle BI Publisher. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2024-21255	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: XMLPublisher). Supported versions that are affected are 8.59, 8.60 and 8.61. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).	8.8	More Details
CVE-2024-9859	Type confusion in WebAssembly in Google Chrome prior to 126.0.6478.126 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-9782	A vulnerability was found in D-Link DIR-619L B1 2.06. It has been declared as critical. This vulnerability affects the function formEasySetupWWConfig of the file /goform/formEasySetupWWConfig. The manipulation of the argument curTime leads to buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-44414	A vulnerability was discovered in FBM_292W-21.03.10V, which has been classified as critical. This issue affects the sub_4901E0 function in the msp_info.htm file. Manipulation of the path parameter can lead to command injection.	8.8	More Details
CVE-2024-8014	In Progress Telerik Reporting versions prior to 2024 Q3 (18.2.24.924), a code execution attack is possible through object injection via an insecure type resolution vulnerability.	8.8	More Details
CVE-2024-9980	The ee-class from FormosaSoft does not properly validate a specific page parameter, allowing remote attackers with regular privileges to inject arbitrary SQL commands to read, modify and delete database contents.	8.8	More Details
CVE-2024-9954	Use after free in AI in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47659	In the Linux kernel, the following vulnerability has been resolved: smack: tcp: ipv4, fix incorrect labeling Currently, Smack mirrors the label of incoming tcp/ipv4 connections: when a label 'foo' connects to a label 'bar' with tcp/ipv4, 'foo' always gets 'foo' in returned ipv4 packets. So, 1) returned packets are incorrectly labeled ('foo' instead of 'bar') 2) 'bar' can write to 'foo' without being authorized to write. Here is a scenario how to see this: * Take two machines, let's call them C and S, with active Smack in the default state (no settings, no rules, no labeled hosts, only builtin labels) * At S, add Smack rule 'foo bar w' (labels 'foo' and 'bar' are instantiated at S at this moment) * At S, at label 'bar', launch a program that listens for incoming tcp/ipv4 connections * From C, at label 'foo', connect to the listener at S. (label 'foo' is instantiated at C at this moment) Connection succeedes and works. * Send some data in both directions. * Collect network traffic of this connection. All packets in both directions are labeled with the CIPSO of the label 'foo'. Hence, label 'bar' writes to 'foo' without being authorized, and even without ever being known at C. If anybody cares: exactly the same happens with DCCP. This behavior 1st manifested in release 2.6.29.4 (see Fixes below) and it looks unintentional. At least, no explanation was provided. I changed returned packes label into the 'bar', to bring it into line with the Smack documentation claims.	8.8	More Details
CVE-2024-9955	Use after free in WebAuthentication in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-45733	In Splunk Enterprise for Windows versions below 9.2.3 and 9.1.6, a low-privileged user that does not hold the "admin" or "power" Splunk roles could perform a Remote Code Execution (RCE) due to an insecure session storage configuration.	8.8	More Details
CVE-2024-9965	Insufficient data validation in DevTools in Google Chrome on Windows prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2024-9961	Use after free in ParcelTracking in Google Chrome on iOS prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-9784	A vulnerability classified as critical has been found in D-Link DIR-619L B1 2.06. Affected is the function formResetStatistic of the file /goform/formResetStatistic. The manipulation of the argument curTime leads to buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-48813	SQL injection vulnerability in employee-management-system-php-and-mysql-free-download.html taskmatic 1.0 allows a remote attacker to execute arbitrary code via the admin_id parameter of the /update-employee.php component.	8.8	More Details
CVE-2024-45148	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authentication vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to gain unauthorized access without proper credentials. Exploitation of this issue does not require user interaction.	8.8	More Details
CVE-2024-9785	A vulnerability classified as critical was found in D-Link DIR-619L B1 2.06. Affected by this vulnerability is the function formSetDDNS of the file /goform/formSetDDNS. The manipulation of the argument curTime leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9959	Use after free in DevTools in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-9786	A vulnerability, which was classified as critical, has been found in D-Link DIR-619L B1 2.06. Affected by this issue is the function formSetLog of the file /goform/formSetLog. The manipulation of the argument curTime leads to buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	8.8	More Details
CVE-2024-48827	An issue in sbondCo Watcharr v.1.43.0 allows a remote attacker to execute arbitrary code and escalate privileges via the Change Password function.	8.8	More Details
CVE-2024-9957	Use after free in UI in Google Chrome on iOS prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-50780	Apache ActiveMQ Artemis allows access to diagnostic information and controls through MBeans, which are also exposed through the authenticated Jolokia endpoint. Before version 2.29.0, this also included the Log4J2 MBean. This MBean is not meant for exposure to non-administrative users. This could eventually allow an authenticated attacker to write arbitrary files to the filesystem and indirectly achieve RCE. Users are recommended to upgrade to version 2.29.0 or later, which fixes the issue.	8.8	More Details
CVE-2024-48822	Privilege escalation in Automatic Systems Maintenance SlimLane 29565_d74ecce0c1081d50546db573a499941b10799fb7 allows a remote attacker to escalate privileges via the FtpConfig.php page.	8.8	More Details
CVE-2024-9687	The WP 2FA with Telegram plugin for WordPress is vulnerable to Authentication Bypass in versions up to, and including, 3.0. This is due to insufficient validation of the user-controlled key on the 'validate_tg' action. This makes it possible for authenticated attackers, with subscriber-level permissions and above, to log in as any existing user on the site, such as an administrator.	8.8	More Details
CVE-2024-9968	WebEIP v3.0 from NewType does not properly validate user input, allowing remote attackers with regular privilege to inject SQL commands to read, modify, and delete data stored in database. The affected product is no longer maintained. It is recommended to upgrade to the new product.	8.8	More Details
CVE-2024-9970	The FlowMaster BPM Plus system from NewType has a privilege escalation vulnerability. Remote attackers with regular privileges can elevate their privileges to administrator by tampering with a specific cookie.	8.8	More Details
CVE-2024-44413	A vulnerability was discovered in DI_8200-16.07.26A1, which has been classified as critical. This issue affects the upgrade_filter_asp function in the upgrade_filter.asp file. Manipulation of the path parameter can lead to command injection.	8.8	More Details
CVE-2024-38139	Improper authentication in Microsoft Dataverse allows an authorized attacker to elevate privileges over a network.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45402	Picotls is a TLS protocol library that allows users select different crypto backends based on their use case. When parsing a spoofed TLS handshake message, picotls (specifically, bindings within picotls that call the crypto libraries) may attempt to free the same memory twice. This double free occurs during the disposal of multiple objects without any intervening calls to malloc Typically, this triggers the malloc implementation to detect the error and abort the process. However, depending on the internals of malloc and the crypto backend being used, the flaw could potentially lead to a use-after-free scenario, which might allow for arbitrary code execution. The vulnerability is addressed with commit 9b88159ce763d680e4a13b6e8f3171ae923a535d.	8.6	More Details
CVE-2024-38190	Missing authorization in Power Platform allows an unauthenticated attacker to view sensitive information through a network attack vector.	8.6	More Details
CVE-2024-48020	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Revmakx Backup and Staging by WP Time Capsule allows SQL Injection.This issue affects Backup and Staging by WP Time Capsule: from n/a through 1.22.21.	8.5	More Details
CVE-2024-48040	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Tainacan.Org Tainacan allows SQL Injection.This issue affects Tainacan: from n/a through 0.21.8.	8.5	More Details
CVE-2024-8070	CWE-312: Cleartext Storage of Sensitive Information vulnerability exists that exposes test credentials in the firmware binary	8.5	More Details
CVE-2024-35522	Netgear EX3700 ' AC750 WiFi Range Extender Essentials Edition before 1.0.0.98 contains an authenticated command injection in operating_mode.cgi via the ap_mode parameter with ap_24g_manual set to 1 and ap_24g_manual_sec set to NotNone.	8.4	More Details
CVE-2023-37154	check_by_ssh in Nagios nagios-plugins 2.4.5 allows arbitrary command execution via ProxyCommand, LocalCommand, and PermitLocalCommand with \${IFS}. This has been categorized both as fixed in e8810de, and as intended behavior.	8.4	More Details
CVE-2024-8755	Improper Input Validation vulnerability of Authenticated User in Progress LoadMaster allows : OS Command Injection.This issue affects: Product Affected Versions LoadMaster From 7.2.55.0 to 7.2.60.1 (inclusive) From 7.2.49.0 to 7.2.54.12 (inclusive) 7.2.48.12 and all prior versions Multi-Tenant Hypervisor 7.1.35.12 and all prior versions ECS All prior versions to 7.2.60.1 (inclusive)	8.4	More Details
CVE-2024-35520	Netgear R7000 1.0.11.136 is vulnerable to Command Injection in RMT_invite.cgi via device_name2 parameter.	8.4	More Details
CVE-2024-45273	An unauthenticated local attacker can decrypt the devices config file and therefore compromise the device due to a weak implementation of the encryption used.	8.4	More Details
CVE-2024-45271	An unauthenticated local attacker can gain admin privileges by deploying a config file due to improper input validation.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35518	Netgear EX6120 v1.0.0.68 is vulnerable to Command Injection in genie_fix2.cgi via the wan_dns1_pri parameter.	8.4	More Details
CVE-2024-35519	Netgear EX6120 v1.0.0.68, Netgear EX6100 v1.0.2.28, and Netgear EX3700 v1.0.0.96 are vulnerable to command injection in operating_mode.cgi via the ap_mode parameter.	8.4	More Details
CVE-2024-35517	Netgear XR1000 v1.0.0.64 is vulnerable to command injection in usb_remote_smb_conf.cgi via the share_name parameter.	8.4	More Details
CVE-2024-47084	Gradio is an open-source Python package designed for quick prototyping. This vulnerability is related to **CORS origin validation**, where the Gradio server fails to validate the request origin when a cookie is present. This allows an attacker's website to make unauthorized requests to a local Gradio server. Potentially, attackers can upload files, steal authentication tokens, and access user data if the victim visits a malicious website while logged into Gradio. This impacts users who have deployed Gradio locally and use basic authentication. Users are advised to upgrade to `gradio>4.44` to address this issue. As a workaround, users can manually enforce stricter CORS origin validation by modifying the `CustomCORSMiddleware` class in their local Gradio server code. Specifically, they can bypass the condition that skips CORS validation for requests containing cookies to prevent potential exploitation.	8.3	More Details
CVE-2024-8970	An issue was discovered in GitLab CE/EE affecting all versions starting from 11.6 prior to 17.2.9, starting from 17.3 prior to 17.3.5, and starting from 17.4 prior to 17.4.2, which allows an attacker to trigger a pipeline as another user under certain circumstances.	8.2	More Details
CVE-2024-48770	An issue in Plug n Play Camera com.wisdomcity.zwave 1.1.0 allows a remote attacker to obtain sensitive information via the firmware update process.	8.2	More Details
CVE-2024-47490	An Improper Restriction of Communication Channel to Intended Endpoints vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved on ACX 7000 Series allows an unauthenticated, network based attacker to cause increased consumption of resources, ultimately resulting in a Denial of Service (DoS). When specific transit MPLS packets are received by the PFE, these packets are internally forwarded to the Routing Engine (RE), rather than being handled appropriately. Continuous receipt of these MPLS packets causes resources to be exhausted. MPLS config is not required to be affected by this issue. This issue affects Junos OS Evolved ACX 7000 Series: * All versions before 21.4R3-S9-EVO, * 22.2-EVO before 22.2R3-S4-EVO, * 22.3-EVO before 22.3R3-S3-EVO, * 22.4-EVO before 22.4R3-S2-EVO, * 23.2-EVO before 23.2R2-EVO, * 23.4-EVO before 23.4R1-S1-EVO, 23.4R2-EVO.	8.2	More Details
CVE-2024-8977	An issue has been discovered in GitLab EE affecting all versions starting from 15.10 prior to 17.2.9, from 17.3 prior to 17.3.5, and from 17.4 prior to 17.4.2. Instances with Product Analytics Dashboard configured and enabled could be vulnerable to SSRF attacks.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45720	On Windows platforms, a "best fit" character encoding conversion of command line arguments to Subversion's executables (e.g., svn.exe, etc.) may lead to unexpected command line argument interpretation, including argument injection and execution of other programs, if a specially crafted command line argument string is processed. All versions of Subversion up to and including Subversion 1.14.3 are affected on Windows platforms only. Users are recommended to upgrade to version Subversion 1.14.4, which fixes this issue. Subversion is not affected on UNIX-like platforms.	8.2	More Details
CVE-2024-21265	Vulnerability in the Oracle Site Hub product of Oracle E-Business Suite (component: Site Hierarchy Flows). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Site Hub. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Site Hub accessible data as well as unauthorized access to critical data or complete access to all Oracle Site Hub accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-21269	Vulnerability in the Oracle Incentive Compensation product of Oracle E-Business Suite (component: Compensation Plan). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Incentive Compensation. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Incentive Compensation accessible data as well as unauthorized access to critical data or complete access to all Oracle Incentive Compensation accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-21252	Vulnerability in the Oracle Product Hub product of Oracle E-Business Suite (component: Item Catalog). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Product Hub. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Product Hub accessible data as well as unauthorized access to critical data or complete access to all Oracle Product Hub accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-21250	Vulnerability in the Oracle Process Manufacturing Product Development product of Oracle E-Business Suite (component: Quality Manager Specification). Supported versions that are affected are 12.2.13-12.2.14. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Process Manufacturing Product Development. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Process Manufacturing Product Development accessible data as well as unauthorized access to critical data or complete access to all Oracle Process Manufacturing Product Development accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-3656	A flaw was found in Keycloak. Certain endpoints in Keycloak's admin REST API allow low-privilege users to access administrative functionalities. This flaw allows users to perform actions reserved for administrators, potentially leading to data breaches or system compromise.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41311	In Libheif 1.17.6, insufficient checks in ImageOverlay::parse() decoding a heif file containing an overlay image with forged offsets can lead to an out-of-bounds read and write.	8.1	More Details
CVE-2024-21283	Vulnerability in the PeopleSoft Enterprise HCM Global Payroll Core product of Oracle PeopleSoft (component: Global Payroll for Core). Supported versions that are affected are 9.2.48-9.2.50. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise HCM Global Payroll Core. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise HCM Global Payroll Core accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise HCM Global Payroll Core accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-21266	Vulnerability in the Oracle Advanced Pricing product of Oracle E-Business Suite (component: Price List). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Advanced Pricing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Advanced Pricing accessible data as well as unauthorized access to critical data or complete access to all Oracle Advanced Pricing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-9575	Local File Inclusion vulnerability in pretix Widget WordPress plugin pretix-widget on Windows allows PHP Local File Inclusion. This issue affects pretix Widget WordPress plugin: from 1.0.0 through 1.0.5.	8.1	More Details
CVE-2024-21214	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Query). Supported versions that are affected are 8.59, 8.60 and 8.61. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized access to critical data or complete access to all PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-21282	Vulnerability in the Oracle Financials product of Oracle E-Business Suite (component: Common Components). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Financials. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Financials accessible data as well as unauthorized access to critical data or complete access to all Oracle Financials accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47870	Gradio is an open-source Python package designed for quick prototyping. This vulnerability involves a **race condition** in the `update_root_in_config` function, allowing an attacker to modify the `root` URL used by the Gradio frontend to communicate with the backend. By exploiting this flaw, an attacker can redirect user traffic to a malicious server. This could lead to the interception of sensitive data such as authentication credentials or uploaded files. This impacts all users who connect to a Gradio server, especially those exposed to the internet, where malicious actors could exploit this race condition. Users are advised to upgrade to `gradio>=5` to address this issue. There are no known workarounds for this issue.	8.1	More Details
CVE-2024-21267	Vulnerability in the Oracle Cost Management product of Oracle E-Business Suite (component: Cost Planning). Supported versions that are affected are 12.2.12-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Cost Management. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Cost Management accessible data as well as unauthorized access to critical data or complete access to all Oracle Cost Management accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-21268	Vulnerability in the Oracle Applications Manager product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are 12.2.11-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Applications Manager. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Applications Manager accessible data as well as unauthorized access to critical data or complete access to all Oracle Applications Manager accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-21280	Vulnerability in the Oracle Service Contracts product of Oracle E-Business Suite (component: Authoring). Supported versions that are affected are 12.2.5-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Service Contracts. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Service Contracts accessible data as well as unauthorized access to critical data or complete access to all Oracle Service Contracts accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-21277	Vulnerability in the Oracle MES for Process Manufacturing product of Oracle E-Business Suite (component: Device Integration). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle MES for Process Manufacturing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle MES for Process Manufacturing accessible data as well as unauthorized access to critical data or complete access to all Oracle MES for Process Manufacturing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21271	Vulnerability in the Oracle Field Service product of Oracle E-Business Suite (component: Field Service Engineer Portal). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Field Service. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Field Service accessible data as well as unauthorized access to critical data or complete access to all Oracle Field Service accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-45116	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could be exploited to execute arbitrary code. If an admin attacker can trick a user into clicking a specially crafted link or submitting a form, malicious scripts may be executed within the context of the victim's browser and have high impact on confidentiality and integrity. Exploitation of this issue requires user interaction.	8.1	More Details
CVE-2024-21275	Vulnerability in the Oracle Quoting product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.2.7-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Quoting. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Quoting accessible data as well as unauthorized access to critical data or complete access to all Oracle Quoting accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-21276	Vulnerability in the Oracle Work in Process product of Oracle E-Business Suite (component: Messages). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Work in Process. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Work in Process accessible data as well as unauthorized access to critical data or complete access to all Oracle Work in Process accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-21270	Vulnerability in the Oracle Common Applications Calendar product of Oracle E-Business Suite (component: Tasks). Supported versions that are affected are 12.2.6-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Common Applications Calendar. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Common Applications Calendar accessible data as well as unauthorized access to critical data or complete access to all Oracle Common Applications Calendar accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21278	Vulnerability in the Oracle Contract Lifecycle Management for Public Sector product of Oracle E-Business Suite (component: Award Processes). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Contract Lifecycle Management for Public Sector. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Contract Lifecycle Management for Public Sector accessible data as well as unauthorized access to critical data or complete access to all Oracle Contract Lifecycle Management for Public Sector accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-21279	Vulnerability in the Oracle Sourcing product of Oracle E-Business Suite (component: Auctions). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Sourcing. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Sourcing accessible data as well as unauthorized access to critical data or complete access to all Oracle Sourcing accessible data. CVSS 3.1 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).	8.1	More Details
CVE-2024-46316	DrayTek Vigor3900 v1.5.1.6 was discovered to contain a command injection vulnerability via the sub_2C920 function at /cgi-bin/mainfunction.cgi. This vulnerability allows attackers to execute arbitrary commands via supplying a crafted HTTP message.	8.0	More Details
CVE-2024-45731	In Splunk Enterprise for Windows versions below 9.3.1, 9.2.3, and 9.1.6, a low-privileged user that does not hold the "admin" or "power" Splunk roles could write a file to the Windows system root directory, which has a default location in the Windows System32 folder, when Splunk Enterprise for Windows is installed on a separate drive.	8.0	More Details
CVE-2024-47414	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47411	Animate versions 23.0.7, 24.0.4 and earlier are affected by an Access of Uninitialized Pointer 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-2024-47412	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-45142	Substance3D - Stager versions 3.0.3 and earlier are affected by a Write-what-where Condition vulnerability that could allow an attacker to execute arbitrary code in the context of the current user. This vulnerability allows an attacker to write a controlled value to an arbitrary memory location, potentially leading to code execution. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-45316	The Improper link resolution before file access ('Link Following') vulnerability in SonicWall Connect Tunnel (version 12.4.3.271 and earlier of Windows client) allows users with standard privileges to delete arbitrary folders and files, potentially leading to local privilege escalation attack.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48958	execute_filter_delta in archive_read_support_format_rar.c in libarchive before 3.7.5 allows out-of-bounds access via a crafted archive file because src can move beyond dst.	7.8	More Details
CVE-2024-47413	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-45143	Substance3D - Stager versions 3.0.3 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-2024-45144	Substance3D - Stager versions 3.0.3 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-2024-48957	execute_filter_audio in archive_read_support_format_rar.c in libarchive before 3.7.5 allows out-of-bounds access via a crafted archive file because src can move beyond dst.	7.8	More Details
CVE-2024-48911	OpenCanary, a multi-protocol network honeypot, directly executed commands taken from its config file. Prior to version 0.9.4, where the config file is stored in an unprivileged user directory but the daemon is executed by root, it’s possible for the unprivileged user to change the config file and escalate permissions when root later runs the daemon. Version 0.9.4 contains a fix for the issue.	7.8	More Details
CVE-2024-47422	Adobe Framemaker versions 2020.6, 2022.4 and earlier are affected by an Untrusted Search Path vulnerability that could lead to arbitrary code execution. An attacker could exploit this vulnerability by inserting a malicious path into the search directories, which the application could unknowingly execute. This could allow the attacker to execute arbitrary code in the context of the current user. Exploitation of this issue requires user interaction.	7.8	More Details
CVE-2024-47410	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Stack-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-2024-9780	ITS dissector crash in Wireshark 4.4.0 allows denial of service via packet injection or crafted capture file	7.8	More Details
CVE-2024-47962	Delta Electronics CNCSoft-G2 lacks proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can manipulate an insider to visit a malicious page or file to leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2024-47963	Delta Electronics CNCSoft-G2 lacks proper validation of user-supplied data, which can result in a write past the end of an allocated object. An attacker can manipulate users to visit a malicious page or file to leverage this vulnerability to execute code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-4089	A DLL hijack vulnerability was reported in Lenovo Super File that could allow a local attacker to execute code with elevated privileges.	7.8	More Details
CVE-2024-4130	A DLL hijack vulnerability was reported in Lenovo App Store that could allow a local attacker to execute code with elevated privileges.	7.8	More Details
CVE-2024-4131	A DLL hijack vulnerability was reported in Lenovo Emulator that could allow a local attacker to execute code with elevated privileges.	7.8	More Details
CVE-2024-47964	Delta Electronics CNCSoft-G2 lacks proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can manipulate users to visit a malicious page or file to leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2024-9781	AppleTalk and RELOAD Framing dissector crash in Wireshark 4.4.0 and 4.2.0 to 4.2.7 allows denial of service via packet injection or crafted capture file	7.8	More Details
CVE-2024-47965	Delta Electronics CNCSoft-G2 lacks proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can manipulate users to visit a malicious page or file to leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2024-45141	Substance3D - Stager versions 3.0.3 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-2024-47966	Delta Electronics CNCSoft-G2 lacks proper initialization of memory prior to accessing it. An attacker can manipulate users to visit a malicious page or file to leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2024-45139	Substance3D - Stager versions 3.0.3 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-2024-45152	Substance3D - Stager versions 3.0.3 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-2024-4132	A DLL hijack vulnerability was reported in Lenovo Lock Screen that could allow a local attacker to execute code with elevated privileges.	7.8	More Details
CVE-2024-45140	Substance3D - Stager versions 3.0.3 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 Number	Description	Base Score	Reference
CVE-2024-45146	Dimension versions 4.0.3 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-45150	Dimension versions 4.0.3 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-2024-47415	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-9473	A privilege escalation vulnerability in the Palo Alto Networks GlobalProtect app on Windows allows a locally authenticated non-administrative Windows user to escalate their privileges to NT AUTHORITY/SYSTEM through the use of the repair functionality offered by the .msi file used to install GlobalProtect.	7.8	More Details
CVE-2024-47417	Animate versions 23.0.7, 24.0.4 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-2024-8048	In Progress Telerik Reporting versions prior to 2024 Q3 (18.2.24.924), a code execution attack is possible using object injection via insecure expression evaluation.	7.8	More Details
CVE-2024-47421	Adobe Framemaker versions 2020.6, 2022.4 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2024-45137	InDesign Desktop versions 19.4, 18.5.3 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution. An attacker could exploit this vulnerability by uploading a malicious file which, when executed, could run arbitrary code in the context of the server. Exploitation of this issue requires user interaction.	7.8	More Details
CVE-2024-35288	Nitro PDF Pro before 13.70.8.82 and 14.x before 14.26.1.0 allows Local Privilege Escalation in the MSI Installer because custom actions occur unsafely in repair mode. CertUtil is run in a conhost.exe window, and there is a mechanism allowing CTRL+o to launch cmd.exe as NT AUTHORITY\SYSTEM.	7.8	More Details
CVE-2024-7840	In Progress Telerik Reporting versions prior to 2024 Q3 (18.2.24.924), a command injection attack is possible through improper neutralization of hyperlink elements.	7.8	More Details
CVE-2024-9002	CWE-269: Improper Privilege Management vulnerability exists that could cause unauthorized access, loss of confidentiality, integrity, and availability of the workstation when non-admin authenticated user tries to perform privilege escalation by tampering with the binaries	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45136	InCopy versions 19.4, 18.5.3 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue requires user interaction.	7.8	More Details
CVE-2024-47418	Animate versions 23.0.7, 24.0.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47416	Animate versions 23.0.7, 24.0.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-9046	A DLL hijack vulnerability was reported in Lenovo stARstudio that could allow a local attacker to execute code with elevated privileges.	7.8	More Details
CVE-2024-33578	A DLL hijack vulnerability was reported in Lenovo Leyun that could allow a local attacker to execute code with elevated privileges.	7.8	More Details
CVE-2024-33579	A DLL hijack vulnerability was reported in Lenovo Baiying that could allow a local attacker to execute code with elevated privileges.	7.8	More Details
CVE-2024-46871	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Correct the defined value for AMDGPU_DMUB_NOTIFICATION_MAX [Why & How] It actually exposes '6' types in enum dmub_notification_type. Not 5. Using smaller number to create array dmub_callback & dmub_thread_offload has potential to access item out of array bound. Fix it.	7.8	More Details
CVE-2024-47670	In the Linux kernel, the following vulnerability has been resolved: ocfs2: add bounds checking to ocfs2_xattr_find_entry() Add a paranoia check to make sure it doesn't stray beyond valid memory region containing ocfs2 xattr entries when scanning for a match. It will prevent out-of-bound access in case of crafted images.	7.8	More Details
CVE-2024-33580	A DLL hijack vulnerability was reported in Lenovo Personal Cloud that could allow a local attacker to execute code with elevated privileges.	7.8	More Details
CVE-2024-33581	A DLL hijack vulnerability was reported in Lenovo PC Manager AI intelligent scenario that could allow a local attacker to execute code with elevated privileges.	7.8	More Details
CVE-2024-47423	Adobe Framemaker versions 2020.6, 2022.4 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution. An attacker could exploit this vulnerability by uploading a malicious file which can be automatically processed or executed by the system. Exploitation of this issue requires user interaction.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45138	Substance3D - Stager versions 3.0.3 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47425	Adobe Framemaker versions 2020.6, 2022.4 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-47424	Adobe Framemaker versions 2020.6, 2022.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	7.8	More Details
CVE-2024-33582	A DLL hijack vulnerability was reported in Lenovo Service Framework that could allow a local attacker to execute code with elevated privileges.	7.8	More Details
CVE-2024-43701	Software installed and run as a non-privileged user may conduct GPU system calls to read and write freed physical memory from the GPU.	7.8	More Details
CVE-2024-9956	Inappropriate implementation in WebAuthentication in Google Chrome on Android prior to 130.0.6723.58 allowed a local attacker to perform privilege escalation via a crafted HTML page. (Chromium security severity: Medium)	7.8	More Details
CVE-2024-9675	A vulnerability was found in Buildah. Cache mounts do not properly validate that user-specified paths for the cache are within our cache directory, allowing a `RUN` instruction in a Container file to mount an arbitrary directory from the host (read/write) into the container as long as those files can be accessed by the user running Buildah.	7.8	More Details
CVE-2024-42018	An issue was discovered in Atos Eviden SMC xScale before 1.6.6. During initialization of nodes, some configuration parameters are retrieved from management nodes. These parameters embed credentials whose integrity and confidentiality may be important to the security of the HPC configuration. Because these parameters are needed for initialization, there is no available mechanism to ensure access control on the management node, and a mitigation measure is normally put in place to prevent access to unprivileged users. It was discovered that this mitigation measure does not survive a reboot of diskful nodes. (Diskless nodes are not at risk.) The mistake lies in the cloudinit configuration: the iptables configuration should have been in the bootcmd instead of the runcmd section.	7.7	More Details
CVE-2024-7847	VULNERABILITY DETAILS Rockwell Automation used the latest versions of the CVSS scoring system to assess the following vulnerabilities. The following vulnerabilities were reported to us by Sharon Brizinov of Claroty Research - Team82. A feature in the affected products enables users to prepare a project file with an embedded VBA script and can be configured to run once the project file has been opened without user intervention. This feature can be abused to trick a legitimate user into executing malicious code upon opening an infected RSP/RSS project file. If exploited, a threat actor may be able to perform a remote code execution. Connected devices may also be impacted by exploitation of this vulnerability.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47334	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Zoho Flow Zoho Flow for WordPress allows SQL Injection.This issue affects Zoho Flow for WordPress: from n/a through 2.7.1.	7.6	More Details
CVE-2024-45117	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An admin attacker could exploit this vulnerability to read files from the system outside of the intended directories via PHP filter chain and also can have a low-availability impact on the service. Exploitation of this issue does not require user interaction and scope is changed.	7.6	More Details
CVE-2024-21191	Vulnerability in the Oracle Enterprise Manager Fusion Middleware Control product of Oracle Fusion Middleware (component: FMW Control Plugin). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Manager Fusion Middleware Control. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle Enterprise Manager Fusion Middleware Control, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Manager Fusion Middleware Control accessible data as well as unauthorized update, insert or delete access to some of Oracle Enterprise Manager Fusion Middleware Control accessible data. CVSS 3.1 Base Score 7.6 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:L/A:N).	7.6	More Details
CVE-2024-48279	A HTML Injection vulnerability was found in /search-result.php of PHPGurukul User Registration & Login and User Management System 3.2. This vulnerability allows remote attackers to execute arbitrary HTML code via the searchkey parameter in a POST HTTP request.	7.6	More Details
CVE-2024-48280	A SQL Injection vulnerability was found in /search-result.php of PHPGurukul User Registration & Login and User Management System 3.2, which allows remote attackers to execute arbitrary SQL command via the fromdate parameter in a POST HTTP request.	7.6	More Details
CVE-2024-48282	A SQL Injection vulnerability was found in /password-recovery.php of PHPGurukul User Registration & Login and User Management System 3.2, which allows remote attackers to execute arbitrary SQL commands to get unauthorized database access via the femail parameter in a POST HTTP request.	7.6	More Details
CVE-2024-21195	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Layout Templates). Supported versions that are affected are 7.0.0.0.0, 7.6.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle BI Publisher. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle BI Publisher accessible data as well as unauthorized update, insert or delete access to some of Oracle BI Publisher accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle BI Publisher. CVSS 3.1 Base Score 7.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:L).	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-35202	Bitcoin Core before 25.0 allows remote attackers to cause a denial of service (blocktxn message-handling assertion and node exit) by including transactions in a blocktxn message that are not committed to in a block's merkle root. FillBlock can be called twice for one PartiallyDownloadedBlock instance.	7.5	More Details
CVE-2024-47504	An Improper Validation of Specified Type of Input vulnerability in the packet forwarding engine (pfe) Juniper Networks Junos OS on SRX5000 Series allows an unauthenticated, network based attacker to cause a Denial of Service (Dos). When a non-clustered SRX5000 device receives a specifically malformed packet this will cause a flowd crash and restart. This issue affects Junos OS: * 22.1 releases 22.1R1 and later before 22.2R3-S5, * 22.3 releases before 22.3R3-S4, * 22.4 releases before 22.4R3-S4, * 23.2 releases before 23.2R2-S2, * 23.4 releases before 23.4R2-S1, * 24.2 releases before 24.2R1-S1, 24.2R2. Please note that the PR does indicate that earlier versions have been fixed as well, but these won't be adversely impacted by this.	7.5	More Details
CVE-2024-47502	An Allocation of Resources Without Limits or Throttling vulnerability in the kernel of Juniper Networks Junos OS Evolved allows an unauthenticated, network based attacker to cause a Denial of Service (DoS). In specific cases the state of TCP sessions that are terminated is not cleared, which over time leads to an exhaustion of resources, preventing new connections to the control plane from being established. A continuously increasing number of connections shown by: user@host > show system connections is indicative of the problem. To recover the respective RE needs to be restarted manually. This issue only affects IPv4 but does not affect IPv6. This issue only affects TCP sessions established in-band (over an interface on an FPC) but not out-of-band (over the management ethernet port on the routing-engine). This issue affects Junos OS Evolved: * All versions before 21.4R3-S9-EVO, * 22.2 versions before 22.2R3-S4-EVO, * 22.4 version before 22.4R3-S3-EVO, * 23.2 versions before 23.2R2-S1-EVO, * 23.4 versions before 23.4R2-EVO.	7.5	More Details
CVE-2024-9922	The Team+ from TEAMPLUS TECHNOLOGY does not properly validate a specific page parameter, allowing unauthenticated remote attackers to exploit this vulnerability to read arbitrary system files.	7.5	More Details
CVE-2024-38863	Exposure of CSRF tokens in query parameters on specific requests in Checkmk GmbH's Checkmk versions <2.3.0p18, <2.2.0p35 and <2.1.0p48 could lead to a leak of the token to facilitate targeted phishing attacks.	7.5	More Details
CVE-2024-9312	Authd, through version 0.3.6, did not sufficiently randomize user IDs to prevent collisions. A local attacker who can register user names could spoof another user's ID and gain their privileges.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47499	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (RPD) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network based attacker to cause a Denial of Service (DoS). In a scenario where BGP Monitoring Protocol (BMP) is configured with rib-in pre-policy monitoring, receiving a BGP update with a specifically malformed AS PATH attribute over an established BGP session, can cause an RPD crash and restart. This issue affects: Junos OS: * All versions before 21.2R3-S8, * 21.4 versions before 21.4R3-S8, * 22.2 versions before 22.2R3-S4, * 22.3 versions before 22.3R3-S3, * 22.4 versions before 22.4R3-S2, * 23.2 versions before 23.2R2-S1, * 23.4 versions before 23.4R1-S2, 23.4R2; Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * 21.4 versions before 21.4R3-S8-EVO, * 22.2 versions before 22.2R3-S4-EVO, * 22.3 versions before 22.3R3-S3-EVO, * 22.4 versions before 22.4R3-S2-EVO, * 23.2 versions before 23.2R2-S1-EVO, * 23.4 versions before 23.4R1-S2-EVO, 23.4R2-EVO.	7.5	More Details
CVE-2024-48776	An issue in Shelly com.home.shelly 1.0.4 allows a remote attacker to obtain sensitive information via the firmware update process	7.5	More Details
CVE-2024-47497	An Uncontrolled Resource Consumption vulnerability in the http daemon (httpd) of Juniper Networks Junos OS on SRX Series, QFX Series, MX Series and EX Series allows an unauthenticated, network-based attacker to cause Denial-of-Service (DoS). An attacker can send specific HTTPS connection requests to the device, triggering the creation of processes that are not properly terminated. Over time, this leads to resource exhaustion, ultimately causing the device to crash and restart. The following command can be used to monitor the resource usage: user@host> show system processes extensive | match mgd | count This issue affects Junos OS on SRX Series and EX Series: All versions before 21.4R3-S7, from 22.2 before 22.2R3-S4, from 22.3 before 22.3R3-S3, from 22.4 before 22.4R3-S2, from 23.2 before 23.2R2-S1, from 23.4 before 23.4R1-S2, 23.4R2.	7.5	More Details
CVE-2024-44729	Incorrect access control in the component app/src/server.js of Mirotalk before commit 9de226 allows unauthenticated attackers without presenter privileges to arbitrarily eject users from a meeting.	7.5	More Details
CVE-2024-8376	In Eclipse Mosquitto up to version 2.0.18a, an attacker can achieve memory leaking, segmentation fault or heap-use-after-free by sending specific sequences of "CONNECT", "DISCONNECT", "SUBSCRIBE", "UNSUBSCRIBE" and "PUBLISH" packets.	7.5	More Details
CVE-2024-45396	Quicly is an IETF QUIC protocol implementation. Quicly up to commtit d720707 is susceptible to a denial-of-service attack. A remote attacker can exploit these bugs to trigger an assertion failure that crashes process using quicly. The vulnerability is addressed with commit 2a95896104901589c495bc41460262e64ffcad5c.	7.5	More Details
CVE-2024-44734	Incorrect access control in Mirotalk before commit 9de226 allows attackers to arbitrarily change usernames via sending a crafted roomAction request to the server.	7.5	More Details
CVE-2024-47877	Extract is aA Go library to extract archives in zip, tar.gz or tar.bz2 formats. A maliciously crafted archive may allow an attacker to create a symlink outside the extraction target directory. This vulnerability is fixed in 4.0.0. If you're using the Extractor.FS interface, then upgrading to /v4 will require to implement the new methods that have been added.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-48768	An issue in almaodo GmbH appinventor.ai_google.almando_control 2.3.1 allows a remote attacker to obtain sensitive information via the firmware update process	7.5	More Details
CVE-2024-48771	An issue in almando GmbH Almando Play APP (com.almando.play) 1.8.2 allows a remote attacker to obtain sensitive information via the firmware update process	7.5	More Details
CVE-2024-48773	An issue in WoFit v.7.2.3 allows a remote attacker to obtain sensitive information via the firmware update process	7.5	More Details
CVE-2024-48774	An issue in Fermax Asia Pacific Pte Ltd com.fermax.vida 2.4.6 allows a remote attacker to obtain sensitve information via the firmware update process.	7.5	More Details
CVE-2024-48775	An issue in Plug n Play Camera com.ezset.delaney 1.2.0 allows a remote attacker to obtain sensitive information via the firmware update process.	7.5	More Details
CVE-2024-48777	LEDVANCE com.ledvance.smartplus.eu 2.1.10 allows a remote attacker to obtain sensitive information via the firmware update process.	7.5	More Details
CVE-2024-46468	A Server-Side Request Forgery (SSRF) vulnerability exists in the jpress <= v5.1.1, which can be exploited by an attacker to obtain sensitive information, resulting in an information disclosure.	7.5	More Details
CVE-2024-48788	An issue in YESCAM (com.yescom.YesCam.zwave) 1.0.2 allows a remote attacker to obtain sensitive information via the firmware update process.	7.5	More Details
CVE-2024-48938	Znuny before LTS 6.5.1 through 6.5.10 and 7.0.1 through 7.0.16 allows DoS/ReDos via email. Parsing the content of emails where HTML code is copied from Microsoft Word could lead to high CPU usage and block the parsing process.	7.5	More Details
CVE-2024-47868	Gradio is an open-source Python package designed for quick prototyping. This is a **data validation vulnerability** affecting several Gradio components, which allows arbitrary file leaks through the post-processing step. Attackers can exploit these components by crafting requests that bypass expected input constraints. This issue could lead to sensitive files being exposed to unauthorized users, especially when combined with other vulnerabilities, such as issue TOB-GRADIO-15. The components most at risk are those that return or handle file data. Vulnerable Components: 1. **String to FileData:** DownloadButton, Audio, ImageEditor, Video, Model3D, File, UploadButton. 2. **Complex data to FileData:** Chatbot, MultimodalTextbox. 3. **Direct file read in preprocess:** Code. 4. **Dictionary converted to FileData:** ParamViewer, Dataset. Exploit Scenarios: 1. A developer creates a Dropdown list that passes values to a DownloadButton. An attacker bypasses the allowed inputs, sends an arbitrary file path (like `/etc/passwd`), and downloads sensitive files. 2. An attacker crafts a malicious payload in a ParamViewer component, leaking sensitive files from a server through the arbitrary file leak. This issue has been resolved in `gradio>5.0`. Upgrading to the latest version will mitigate this vulnerability. There are no known workarounds for this vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47867	Gradio is an open-source Python package designed for quick prototyping. This vulnerability is a **lack of integrity check** on the downloaded FRP client, which could potentially allow attackers to introduce malicious code. If an attacker gains access to the remote URL from which the FRP client is downloaded, they could modify the binary without detection, as the Gradio server does not verify the file's checksum or signature. Any users utilizing the Gradio server's sharing mechanism that downloads the FRP client could be affected by this vulnerability, especially those relying on the executable binary for secure data tunneling. There is no direct workaround for this issue without upgrading. However, users can manually validate the integrity of the downloaded FRP client by implementing checksum or signature verification in their own environment to ensure the binary hasn't been tampered with.	7.5	More Details
CVE-2024-49193	Zendesk before 2024-07-02 allows remote attackers to read ticket history via e-mail spoofing, because Cc fields are extracted from incoming e-mail messages and used to grant additional authorization for ticket viewing, the mechanism for detecting spoofed e-mail messages is insufficient, and the support e-mail addresses associated with individual tickets are predictable.	7.5	More Details
CVE-2024-39547	An Improper Handling of Exceptional Conditions vulnerability in the rpd-server of Juniper Networks Junos OS and Junos OS Evolved within cRPD allows an unauthenticated network-based attacker sending crafted TCP traffic to the routing engine (RE) to cause a CPU-based Denial of Service (DoS). If specially crafted TCP traffic is received by the control plane, or a TCP session terminates unexpectedly, it will cause increased control plane CPU utilization by the rpd-server process. While not explicitly required, the impact is more severe when RIB sharding is enabled. Task accounting shows unexpected reads by the RPD Server jobs for shards: user@junos> show task accounting detail ... read:RPD Server.0.0.0.0+780.192.168.0.78+48886 TOT:00000003.00379787 MAX:00000000.00080516 RUNS: 233888\ read:RPD Server.0.0.0.0+780.192.168.0.78+49144 TOT:00000004.00007565 MAX:00000000.00080360 RUNS: 233888\ read:RPD Server.0.0.0.0+780.192.168.0.78+49694 TOT:00000003.00600584 MAX:00000000.00080463 RUNS: 233888\ read:RPD Server.0.0.0.0+780.192.168.0.78+50246 TOT:00000004.00346998 MAX:00000000.00080338 RUNS: 233888\ This issue affects: Junos OS with cRPD: * All versions before 21.2R3-S8, * 21.4 before 21.4R3-S7, * 22.1 before 22.1R3-S6, * 22.2 before 22.2R3-S4, * 22.3 before 22.3R3-S3, * 22.4 before 22.4R3-S2, * 23.2 before 23.2R2-S2, * 24.2 before 24.2R2; Junos OS Evolved with cRPD: * All versions before 21.4R3-S7-EVO, * 22.2 before 22.2R3-S4-EVO, * 22.3 before 22.3R3-S3-EVO, * 22.4 before 22.4R3-S2-EVO, * 23.2 before 23.2R2-EVO.	7.5	More Details
CVE-2024-38204	Improper access control in Imagine Cup allows an authorized attacker to elevate privileges over a network.	7.5	More Details
CVE-2024-46898	SHIRASAGI prior to v1.19.1 processes URLs in HTTP requests improperly, resulting in a path traversal vulnerability. If this vulnerability is exploited, arbitrary files on the server may be retrieved when processing crafted HTTP requests.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39525	An Improper Handling of Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker sending a specific BGP packet to cause rpd to crash and restart, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects systems with BGP traceoptions enabled and requires a BGP session to be already established. Systems without BGP traceoptions enabled are not affected by this issue. This issue affects iBGP and eBGP, and both IPv4 and IPv6 are affected by this vulnerability. This issue affects: Junos OS: * All versions before 21.2R3-S8, * from 21.4 before 21.4R3-S8, * from 22.2 before 22.2R3-S4, * from 22.3 before 22.3R3-S4, * from 22.4 before 22.4R3-S3, * from 23.2 before 23.2R2-S1, * from 23.4 before 23.4R2; Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * from 21.4-EVO before 21.4R3-S8-EVO, * from 22.2-EVO before 22.2R3-S4-EVO, * from 22.3-EVO before 22.3R3-S4-EVO, * from 22.4-EVO before 22.4R3-S3-EVO, * from 23.2-EVO before 23.2R2-S1-EVO, * from 23.4-EVO before 23.4R2-EVO.	7.5	More Details
CVE-2024-7294	In Progress® Telerik® Report Server versions prior to 2024 Q3 (10.2.24.806), an HTTP DoS attack is possible on anonymous endpoints without rate limiting.	7.5	More Details
CVE-2024-9156	The TI WooCommerce Wishlist WordPress plugin through 2.8.2 is vulnerable to SQL Injection due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for unauthenticated attackers to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	7.5	More Details
CVE-2024-46307	A loop hole in the payment logic of Sparkshop v1.16 allows attackers to arbitrarily modify the number of products.	7.5	More Details
CVE-2024-9463	An OS command injection vulnerability in Palo Alto Networks Expedition allows an unauthenticated attacker to run arbitrary OS commands as root in Expedition, resulting in disclosure of usernames, cleartext passwords, device configurations, and device API keys of PAN-OS firewalls.	7.5	More Details
CVE-2024-21260	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2024-21259	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22 and prior to 7.1.2. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:H/A:H).	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21246	Vulnerability in the Oracle Service Bus product of Oracle Fusion Middleware (component: OSB Core Functionality). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Service Bus. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Service Bus accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2024-9983	Enterprise Cloud Database from Ragic does not properly validate a specific page parameter, allowing unauthenticated remote attackers to exploit this vulnerability to read arbitrary system files.	7.5	More Details
CVE-2024-45272	An unauthenticated remote attacker can perform a brute-force attack on the credentials of the remote service portal with a high chance of success, resulting in connection lost.	7.5	More Details
CVE-2024-21234	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).	7.5	More Details
CVE-2024-45276	An unauthenticated remote attacker can get read access to files in the "/tmp" directory due to missing authentication.	7.5	More Details
CVE-2024-21215	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2024-39515	An Improper Validation of Consistency within Input vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker sending a specifically malformed BGP packet to cause rpd to crash and restart, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. In some cases, rpd fails to restart requiring a manual restart via the 'restart routing' CLI command. This issue only affects systems with BGP traceoptions enabled and requires a BGP session to be already established. Systems without BGP traceoptions enabled are not affected by this issue. This issue affects iBGP and eBGP, and both IPv4 and IPv6 are affected by this vulnerability. This issue affects: Junos OS: * All versions before 21.4R3-S8, * 22.2 before 22.2R3-S5, * 22.3 before 22.3R3-S4, * 22.4 before 22.4R3-S3, * 23.2 before 23.2R2-S2, * 23.4 before 23.4R2; Junos OS Evolved: * All versions before 21.4R3-S8-EVO, * 22.2-EVO before 22.2R3-S5-EVO, * 22.3-EVO before 22.3R3-S4-EVO, * 22.4-EVO before 22.4R3-S3-EVO, * 23.2-EVO before 23.2R2-S2-EVO, * 23.4-EVO before 23.4R2-EVO.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39516	An Out-of-Bounds Read vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker sending a specifically malformed BGP packet to cause rpd to crash and restart, resulting in a Denial of Service (DoS). Continued receipt and processing of this packet will create a sustained Denial of Service (DoS) condition. This issue only affects systems configured in either of two ways: * systems with BGP traceoptions enabled * systems with BGP traffic engineering configured This issue can affect iBGP and eBGP with any address family configured. The specific attribute involved is non-transitive, and will not propagate across a network. This issue affects: Junos OS: * All versions before 21.4R3-S8, * 22.2 before 22.2R3-S5, * 22.3 before 22.3R3-S4, * 22.4 before 22.4R3-S3, * 23.2 before 23.2R2-S2, * 23.4 before 23.4R2; Junos OS Evolved: * All versions before 21.4R3-S8-EVO, * 22.2-EVO before 22.2R3-S5-EVO, * 22.3-EVO before 22.3R3-S4-EVO, * 22.4-EVO before 22.4R3-S3-EVO, * 23.2-EVO before 23.2R2-S2-EVO, * 23.4-EVO before 23.4R2-EVO.	7.5	More Details
CVE-2024-21190	Vulnerability in the Oracle Global Lifecycle Management FMW Installer product of Oracle Fusion Middleware (component: Cloning). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via SFTP to compromise Oracle Global Lifecycle Management FMW Installer. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Global Lifecycle Management FMW Installer accessible data. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).	7.5	More Details
CVE-2024-49387	Cleartext transmission of sensitive information in acep-collector service. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 38690.	7.5	More Details
CVE-2024-41344	A Cross-Site Request Forgery (CSRF) in Codeigniter 3.1.13 allows attackers to arbitrarily change the Administrator password and escalate privileges.	7.5	More Details
CVE-2024-5749	Certain HP DesignJet products may be vulnerable to credential reflection which allow viewing SMTP server credentials.	7.5	More Details
CVE-2024-46292	A buffer overflow in modsecurity v3.0.12 allows attackers to cause a Denial of Service (DoS) via a crafted input inserted into the name parameter. NOTE: this is disputed by the Supplier because it cannot be reproduced. Also, the product's documentation indicates that it is not guaranteed to be usable with very large values of SecRequestBodyNoFilesLimit (which are required by the claimed issue).	7.5	More Details
CVE-2024-46304	A NULL pointer dereference in libcoap v4.3.5-rc2 and below allows a remote attacker to cause a denial of service via the coap_handle_request_put_block function in src/coap_block.c.	7.5	More Details
CVE-2024-7293	In Progress® Telerik® Report Server versions prior to 2024 Q3 (10.2.24.806), a password brute forcing attack is possible through weak password requirements.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21274	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).	7.5	More Details
CVE-2024-48796	An issue in EQUES com.eques.plug 1.0.1 allows a remote attacker to obtain sensitive information via the firmware update process.	7.5	More Details
CVE-2024-9960	Use after free in Dawn in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	7.5	More Details
CVE-2024-48797	An issue in PCS Engineering Preston Cinema (com.prestoncinema.app) 0.2.0 allows a remote attacker to obtain sensitive information via the firmware update process.	7.5	More Details
CVE-2024-48798	An issue in Hubble Connected (com.hubbleconnected.vervelife) 2.00.81 allows a remote attacker to obtain sensitive information via the firmware update process.	7.5	More Details
CVE-2024-48799	An issue in LOREX TECHNOLOGY INC com.lorexcorp.lorexping 1.4.22 allows a remote attacker to obtain sensitive information via the firmware update process.	7.5	More Details
CVE-2024-48783	An issue in Ruijie NBR3000D-E Gateway allows a remote attacker to obtain sensitive information via the /tool/shell/postgresql.conf component.	7.5	More Details
CVE-2024-48789	An issue in INATRONIC com.inatronic.drivedeck.home 2.6.23 allows a remote attacker to obtain sensitve information via the firmware update process.	7.5	More Details
CVE-2024-44775	An issue in kmqtt v0.2.7 allows attackers to cause a Denial of Service(DoS) via a crafted request.	7.5	More Details
CVE-2024-28168	Improper Restriction of XML External Entity Reference ('XXE') vulnerability in Apache XML Graphics FOP. This issue affects Apache XML Graphics FOP: 2.9. Users are recommended to upgrade to version 2.10, which fixes the issue.	7.5	More Details
CVE-2024-48791	An issue in Plug n Play Camera com.starvedia.mCamView.zwave 5.5.1 allows a remote attacker to obtain sensitive information via the firmware update process	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21272	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/Python). Supported versions that are affected are 9.0.0 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in takeover of MySQL Connectors. CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).	7.5	More Details
CVE-2024-48792	An issue in Hideez com.hideez 2.7.8.3 allows a remote attacker to obtain sensitive information via the firmware update process.	7.5	More Details
CVE-2024-48824	An issue in Automatic Systems Maintenance SlimLane 29565_d74ecce0c1081d50546db573a499941b10799fb7 allows a remote attacker to obtain sensitive information via the Racine & FileName parameters in the download-file.php component.	7.5	More Details
CVE-2024-6207	CVE 2021-22681 https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1550.html and send a specially crafted CIP message to the device. If exploited, a threat actor could help prevent access to the legitimate user and end connections to connected devices including the workstation. To recover the controllers, a download is required which ends any process that the controller is running.	7.5	More Details
CVE-2024-7292	In Progress® Telerik® Report Server versions prior to 2024 Q3 (10.2.24.806), a credential stuffing attack is possible through improper restriction of excessive login attempts.	7.5	More Details
CVE-2024-38365	btcd is an alternative full node bitcoin implementation written in Go (golang). The btcd Bitcoin client (versions 0.10 to 0.24) did not correctly re-implement Bitcoin Core's "FindAndDelete()" functionality. This logic is consensus-critical: the difference in behavior with the other Bitcoin clients can lead to btcd clients accepting an invalid Bitcoin block (or rejecting a valid one). This consensus failure can be leveraged to cause a chain split (accepting an invalid Bitcoin block) or be exploited to DoS the btcd nodes (rejecting a valid Bitcoin block). An attacker can create a standard transaction where FindAndDelete doesn't return a match but removeOpCodeByData does making btcd get a different sighash, leading to a chain split. Importantly, this vulnerability can be exploited remotely by any Bitcoin user and does not require any hash power. This is because the difference in behavior can be triggered by a "standard" Bitcoin transaction, that is a transaction which gets relayed through the P2P network before it gets included in a Bitcoin block. `removeOpcodeByData(script []byte, dataToRemove []byte)` removes any data pushes from `script` that contain `dataToRemove`. However, `FindAndDelete` only removes exact matches. So for example, with `script = "<data> <data|foo>"` and `dataToRemove = "data"` btcd will remove both data pushes but Bitcoin Core's `FindAndDelete` only removes the first `<data>` push. This has been patched in btcd version v0.24.2. Users are advised to upgrade. There are no known workarounds for this issue.	7.4	More Details
CVE-2024-43610	Exposure of Sensitive Information to an Unauthorized Actor in Copilot Studio allows a unauthenticated attacker to view sensitive information through network attack vector	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9814	A vulnerability, which was classified as critical, was found in Codezips Pharmacy Management System 1.0. Affected is an unknown function of the file product/update.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-39563	A Command Injection vulnerability in Juniper Networks Junos Space allows an unauthenticated, network-based attacker sending a specially crafted request to execute arbitrary shell commands on the Junos Space Appliance, leading to remote command execution by the web application, gaining complete control of the device. A specific script in the Junos Space web application allows attacker-controlled input from a GET request without sufficient input sanitization. A specially crafted request can exploit this vulnerability to execute arbitrary shell commands on the Junos Space Appliance. This issue affects Junos Space 24.1R1. Previous versions of Junos Space are unaffected by this vulnerability.	7.3	More Details
CVE-2024-9818	A vulnerability classified as critical has been found in SourceCodester Online Veterinary Appointment System 1.0. Affected is an unknown function of the file /admin/categories/manage_category.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-9986	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file member_register.php. The manipulation of the argument fullname/username/password/email leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "password" to be affected. But it must be assumed that other parameters are affected as well.	7.3	More Details
CVE-2024-6530	A cross-site scripting issue has been discovered in GitLab affecting all versions starting from 17.1 prior 17.2.9, starting from 17.3 prior to 17.3.5, and starting from 17.4 prior to 17.4.2. When adding a authorizing an application, it can be made to render as HTML under specific circumstances.	7.3	More Details
CVE-2024-9797	A vulnerability, which was classified as critical, was found in code-projects Blood Bank System 1.0. Affected is an unknown function of the file register.php. The manipulation of the argument user leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-9813	A vulnerability, which was classified as critical, has been found in Codezips Pharmacy Management System 1.0. This issue affects some unknown processing of the file product/register.php. The manipulation of the argument category leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-9916	A vulnerability, which was classified as critical, has been found in HuangDou UTCMS V9. Affected by this issue is some unknown functionality of the file app/modules/ut-cac/admin/cli.php. The manipulation of the argument o leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9837	The The AADMY – Add Auto Date Month Year Into Posts plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 2.0.1. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-48249	Wavelog 1.8.5 allows Gridmap_model.php get_band_confirmed SQL injection via band, sat, propagation, or mode.	7.3	More Details
CVE-2024-48259	Cloudlog 2.6.15 allows Oqrs.php request_form SQL injection via station_id or callsign.	7.3	More Details
CVE-2024-9581	The Shortcodes AnyWhere plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.0.1. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-9811	A vulnerability classified as critical has been found in code-projects Restaurant Reservation System 1.0. This affects an unknown part of the file filter3.php. The manipulation of the argument company leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-9812	A vulnerability classified as critical was found in code-projects Crud Operation System 1.0. This vulnerability affects unknown code of the file delete.php. The manipulation of the argument sid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-9548	The SlimStat Analytics plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the resource parameter in all versions up to, and including, 5.2.6 due to insufficient input sanitization and output escaping when logging visitor requests. 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-2024-9022	The TS Poll – Survey, Versus Poll, Image Poll, Video Poll plugin for WordPress is vulnerable to SQL Injection via the ‘orderby’ parameter in all versions up to, and including, 2.3.9 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-2024-9519	The UserPlus plugin for WordPress is vulnerable to unauthorized modification of data due to an improper capability check on the 'save_metabox_form' function in versions up to, and including, 2.0. This makes it possible for authenticated attackers, with editor-level permissions or above, to update the registration form role to administrator, which leads to privilege escalation.	7.2	More Details
CVE-2024-9139	The affected product permits OS command injection through improperly restricted commands, potentially allowing attackers to execute arbitrary code.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8531	CWE-347: Improper Verification of Cryptographic Signature vulnerability exists that could compromise the Data Center Expert software when an upgrade bundle is manipulated to include arbitrary bash scripts that are executed as root.	7.2	More Details
CVE-2024-9180	A privileged Vault operator with write permissions to the root namespace's identity endpoint could escalate their own or another user's privileges to Vault's root policy. Fixed in Vault Community Edition 1.18.0 and Vault Enterprise 1.18.0, 1.17.7, 1.16.11, and 1.15.16.	7.2	More Details
CVE-2024-45179	An issue was discovered in za-internet C-MOR Video Surveillance 5.2401 and 6.00PL01. Due to insufficient input validation, the C-MOR web interface is vulnerable to OS command injection attacks. It was found out that different functionality is vulnerable to OS command injection attacks, for example for generating new X.509 certificates, or setting the time zone. These OS command injection vulnerabilities in the script generatesslreq.pml can be exploited as a low-privileged authenticated user to execute commands in the context of the Linux user www-data via shell metacharacters in HTTP POST data (e.g., the city parameter). The OS command injection vulnerability in the script settimezone.pml or setdatetime.pml (e.g., via the year parameter) requires an administrative user for the C-MOR web interface. By also exploiting a privilege-escalation vulnerability, it is possible to execute commands on the C-MOR system with root privileges.	7.2	More Details
CVE-2024-8757	The WP Post Author – Boost Your Blog's Engagement with Author Box, Social Links, Co-Authors, Guest Authors, Post Rating System, and Custom User Registration Form Builder plugin for WordPress is vulnerable to time-based SQL Injection via the linked_user_id parameter in all versions up to, and including, 3.8.1 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 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-2024-45754	An issue was discovered in the centreon-bi-server component in Centreon BI Server 24.04.x before 24.04.3, 23.10.x before 23.10.8, 23.04.x before 23.04.11, and 22.10.x before 22.10.11. SQL injection can occur in the listing of configured reporting jobs. Exploitation is only accessible to authenticated users with high-privileged access.	7.2	More Details
CVE-2024-21284	Vulnerability in the Oracle Banking Liquidity Management product of Oracle Financial Services Applications (component: Reports). The supported version that is affected is 14.5.0.12.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Liquidity Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Banking Liquidity Management. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H).	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21285	Vulnerability in the Oracle Banking Liquidity Management product of Oracle Financial Services Applications (component: Reports). The supported version that is affected is 14.5.0.12.0. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Banking Liquidity Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Oracle Banking Liquidity Management. CVSS 3.1 Base Score 7.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H).	7.1	More Details
CVE-2024-6959	A vulnerability in parisneo/lollms-webui version 9.8 allows for a Denial of Service (DOS) attack when uploading an audio file. If an attacker appends a large number of characters to the end of a multipart boundary, the system will continuously process each character, rendering lollms-webui inaccessible. This issue is exacerbated by the lack of Cross-Site Request Forgery (CSRF) protection, enabling remote exploitation. The vulnerability leads to service disruption, resource exhaustion, and extended downtime.	7.1	More Details
CVE-2024-45732	In Splunk Enterprise versions below 9.3.1, and 9.2.0 versions below 9.2.3, and Splunk Cloud Platform versions below 9.2.2403.103, 9.1.2312.200, 9.1.2312.110 and 9.1.2308.208, a low-privileged user that does not hold the "admin" or "power" Splunk roles could run a search as the "nobody" Splunk user in the SplunkDeploymentServerConfig app. This could let the low-privileged user access potentially restricted data.	7.1	More Details
CVE-2024-47191	pam_oath.so in oath-toolkit 2.6.7 through 2.6.11 before 2.6.12 allows root privilege escalation because, in the context of PAM code running as root, it mishandles usersfile access, such as by calling fchown in the presence of a symlink.	7.1	More Details
CVE-2024-47944	The device directly executes .patch firmware upgrade files on a USB stick without any prior authentication in the admin interface. This leads to an unauthenticated code execution via the firmware upgrade function.	6.8	More Details
CVE-2024-38818	VMware NSX contains a local privilege escalation vulnerability. An authenticated malicious actor may exploit this vulnerability to obtain permissions from a separate group role than previously assigned.	6.7	More Details
CVE-2024-38817	VMware NSX contains a command injection vulnerability. A malicious actor with access to the NSX Edge CLI terminal may be able to craft malicious payloads to execute arbitrary commands on the operating system as root.	6.7	More Details
CVE-2024-47495	An Authorization Bypass Through User-Controlled Key vulnerability allows a locally authenticated attacker with shell access to gain full control of the device when Dual Routing Engines (REs) are in use on Juniper Networks Junos OS Evolved devices. This issue affects: Juniper Networks Junos OS Evolved with dual-REs: * All versions before 21.2R3-S8-EVO, * from 21.4-EVO before 21.4R3-S8-EVO, * from 22.2-EVO before 22.2R3-S4-EVO, * from 22.3-EVO before 22.3R3-S4-EVO, * from 22.4-EVO before 22.4R3-S3-EVO, * from 23.2-EVO before 23.2R2-S1-EVO, * from 23.4-EVO before 23.4R2-S1-EVO. This issue does not affect Juniper Networks Junos OS.	6.7	More Details
CVE-2023-42133	PAX Android based POS devices allow for escalation of privilege via improperly configured scripts. An attacker must have shell access with system account privileges in order to exploit this vulnerability. A patch addressing this issue was included in firmware version PayDroid_8.1.0_Sagittarius_V11.1.61_20240226.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31493	RCE (Remote Code Execution) exists in ZoneMinder through 1.36.33 as an attacker can create a new .php log file in language folder, while executing a crafted payload and escalate privileges allowing execution of any commands on the remote system.	6.6	More Details
CVE-2024-48622	A cross-site scripting (XSS) issue in DomainMOD below v4.12.0 allows remote attackers to inject JavaScript code via admin/domain-fields/edit.php and the cdfid parameter.	6.6	More Details
CVE-2024-48987	Snipe-IT before 7.0.10 allows remote code execution (associated with cookie serialization) when an attacker knows the APP_KEY. This is exacerbated by .env files, available from the product's repository, that have default APP_KEY values.	6.6	More Details
CVE-2024-41997	An issue was discovered in version of Warp Terminal prior to 2024.07.18 (v0.2024.07.16.08.02). A command injection vulnerability exists in the Docker integration functionality. An attacker can create a specially crafted hyperlink using the `warp://action/docker/open_subshell` intent that when clicked by the victim results in command execution on the victim's machine.	6.6	More Details
CVE-2023-45872	An issue was discovered in Qt before 6.2.11 and 6.3.x through 6.6.x before 6.6.1. When a QML image refers to an image whose content is not known yet, there is an assumption that it is an SVG document, leading to a denial of service (application crash) if it is not actually an SVG document.	6.5	More Details
CVE-2024-47505	An Allocation of Resources Without Limits or Throttling vulnerability in the PFE management daemon (evo-pfemand) of Juniper Networks Junos OS Evolved allows an authenticated, network-based attacker to cause an FPC crash leading to a Denial of Service (DoS).When specific SNMP GET operations or specific low-priviledged CLI commands are executed, a GUID resource leak will occur, eventually leading to exhaustion and resulting in FPCs to hang. Affected FPCs need to be manually restarted to recover. GUID exhaustion will trigger a syslog message like one of the following: evo-pfemand[<pid>]: get_next_guid: Ran out of Guid Space ... evo-aftmand-zx[<pid>]: get_next_guid: Ran out of Guid Space ... The leak can be monitored by running the following command and taking note of the values in the rightmost column labeled Guids: user@host> show platform application-info allocations app evo-pfemand/evo-pfemand In case one or more of these values are constantly increasing the leak is happening. This issue affects Junos OS Evolved: * All versions before 21.4R3-S7-EVO, * 22.1 versions before 22.1R3-S6-EVO, * 22.2 versions before 22.2R3-EVO, * 22.3 versions before 22.3R3-EVO, * 22.4 versions before 22.4R2-EVO. Please note that this issue is similar to, but different from CVE-2024-47508 and CVE-2024-47509.	6.5	More Details
CVE-2024-47498	An Unimplemented or Unsupported Feature in UI vulnerability in the CLI of Juniper Networks Junos OS Evolved on QFX5000 Series allows an unauthenticated, adjacent attacker to cause a Denial-of-Service (DoS). Several configuration statements meant to enforce limits on MAC learning and moves can be configured but do not take effect. This can lead to control plane overload situations which will severely impact the ability of the device to processes legitimate traffic. This issue affects Junos OS Evolved on QFX5000 Series: * All versions before 21.4R3-S8-EVO, * 22.2-EVO versions before 22.2R3-S5-EVO, * 22.4-EVO versions before 22.4R3-EVO, * 23.2-EVO versions before 23.2R2-EVO.	6.5	More Details
CVE-2023-45359	An issue was discovered in the Vector Skin component for MediaWiki before 1.39.5 and 1.40.x before 1.40.1. vector-toc-toggle-button-label is not escaped, but should be, because the line param can have markup.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9936	When manipulating the selection node cache, an attacker may have been able to cause unexpected behavior, potentially leading to an exploitable crash. This vulnerability affects Firefox < 131.0.3.	6.5	More Details
CVE-2024-39436	In linkturbonative service, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed.	6.5	More Details
CVE-2024-39526	An Improper Handling of Exceptional Conditions vulnerability in packet processing of Juniper Networks Junos OS on MX Series with MPC10/MPC11/LC9600 line cards, EX9200 with EX9200-15C lines cards, MX304 devices, and Juniper Networks Junos OS Evolved on PTX Series, allows an attacker sending malformed DHCP packets to cause ingress packet processing to stop, leading to a Denial of Service (DoS). Continued receipt and processing of these packets will create a sustained Denial of Service (DoS) condition. This issue only occurs if DHCP snooping is enabled. See configuration below. This issue can be detected using following commands. Their output will display the interface status going down: user@device>show interfaces <if--x/x/x> user@device>show log messages | match <if--x/x/x> user@device>show log messages ==> will display the "[Error] Wedge-Detect : Host Loopback Wedge Detected: PFE: no," logs. This issue affects: Junos OS on MX Series with MPC10/MPC11/LC9600 line cards, EX9200 with EX9200-15C line cards, and MX304: * All versions before 21.2R3-S7, * from 21.4 before 21.4R3-S6, * from 22.2 before 22.2R3-S3, * all versions of 22.3, * from 22.4 before 22.4R3, * from 23.2 before 23.2R2; Junos OS Evolved on PTX Series: * from 19.3R1-EVO before 21.2R3-S8-EVO, * from 21.4-EVO before 21.4R3-S7-EVO, * from 22.1-EVO before 22.1R3-S6-EVO, * from 22.2-EVO before 22.2R3-S5-EVO, * from 22.3-EVO before 22.3R3-S3-EVO, * from 22.4-EVO before 22.4R3-S1-EVO, * from 23.2-EVO before 23.2R2-S2-EVO, * from 23.4-EVO before 23.4R2-EVO. Junos OS Evolved releases prior to 19.3R1-EVO are unaffected by this vulnerability	6.5	More Details
CVE-2024-39437	In linkturbonative service, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed.	6.5	More Details
CVE-2024-39438	In linkturbonative service, there is a possible command injection due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed.	6.5	More Details
CVE-2024-47493	A Missing Release of Memory after Effective Lifetime vulnerability in the Packet Forwarding Engine (PFE) of the Juniper Networks Junos OS on the MX Series platforms with Trio-based FPCs allows an unauthenticated, adjacent attacker to cause a Denial of Service (DoS). In case of channelized Modular Interface Cards (MICs), every physical interface flap operation will leak heap memory. Over a period of time, continuous physical interface flap operations causes local FPC to eventually run out of memory and crash. Below CLI command can be used to check the memory usage over a period of time: user@host> show chassis fpc Temp CPU Utilization (%) CPU Utilization (%) Memory Utilization (%) Slot State (C) Total Interrupt 1min 5min 15min DRAM (MB) Heap Buffer 0 Online 43 41 2 2048 49 14 1 Online 43 41 2 2048 49 14 2 Online 43 41 2 2048 49 14 This issue affects Junos OS on MX Series: * All versions before 21.2R3-S7, * from 21.4 before 21.4R3-S6, * from 22.1 before 22.1R3-S5, * from 22.2 before 22.2R3-S3, * from 22.3 before 22.3R3-S2, * from 22.4 before 22.4R3, * from 23.2 before 23.2R2, * from 23.4 before 23.4R2.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47503	An Improper Check for Unusual or Exceptional Conditions vulnerability in the flow processing daemon (flowd) of Juniper Networks Junos OS on SRX4600 and SRX5000 Series allows an unauthenticated and logically adjacent attacker to cause a Denial-of-Service (DoS). If in a multicast scenario a sequence of specific PIM packets is received, this will cause a flowd crash and restart, which leads to momentary service interruption. This issue affects Junos OS on SRX 4600 and SRX 5000 Series: * All versions before 21.4R3-S9, * 22.2 versions before 22.2R3-S5, * 22.3 versions before 22.3R3-S4, * 22.4 versions before 22.4R3-S4, * 23.2 versions before 23.2R2-S2, * 23.4 versions before 23.4R2, * 24.2 versions before 24.2R1-S1, 24.2R2.	6.5	More Details
CVE-2024-48710	In TP-Link TL-WDR7660 1.0, the wlanTimerRuleJsonToBin function handles the parameter string name without checking it, which can lead to stack overflow vulnerabilities.	6.5	More Details
CVE-2024-45132	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and affect confidentiality. Exploitation of this issue does not require user interaction.	6.5	More Details
CVE-2024-48712	In TP-Link TL-WDR7660 1.0, the rtRuleJsonToBin function handles the parameter string name without checking it, which can lead to stack overflow vulnerabilities.	6.5	More Details
CVE-2024-48713	In TP-Link TL-WDR7660 1.0, the wacWhitelistJsonToBin function handles the parameter string name without checking it, which can lead to stack overflow vulnerabilities.	6.5	More Details
CVE-2024-48714	In TP-Link TL-WDR7660 v1.0, the guestRuleJsonToBin function handles the parameter string name without checking it, which can lead to stack overflow vulnerabilities.	6.5	More Details
CVE-2024-47509	An Allocation of Resources Without Limits or Throttling vulnerability in the PFE management daemon (evo-pfemand) of Juniper Networks Junos OS Evolved allows an authenticated, network-based attacker to cause an FPC crash leading to a Denial of Service (DoS).When specific SNMP GET operations or specific low-priviledged CLI commands are executed, a GUID resource leak will occur, eventually leading to exhaustion and resulting in FPCs to hang. Affected FPCs need to be manually restarted to recover. GUID exhaustion will trigger a syslog message like one of the following: evo-pfemand[<pid>]: get_next_guid: Ran out of Guid Space ... evo-aftmand-zx[<pid>]: get_next_guid: Ran out of Guid Space ... The leak can be monitored by running the following command and taking note of the values in the rightmost column labeled Guids: user@host> show platform application-info allocations app evo-pfemand/evo-pfemand In case one or more of these values are constantly increasing the leak is happening. This issue affects Junos OS Evolved: * All versions before 21.4R2-EVO, * 22.1 versions before 22.1R2-EVO. Please note that this issue is similar to, but different from CVE-2024-47505 and CVE-2024-47508.	6.5	More Details
CVE-2024-9820	The WP 2FA with Telegram plugin for WordPress is vulnerable to Two-Factor Authentication Bypass in versions up to, and including, 3.0. This is due to the two-factor code being stored in a cookie, which makes it possible to bypass two-factor authentication.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9586	The Linkz.ai plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'check_auth' and 'check_logout' functions in versions up to, and including, 1.1.8. This makes it possible for unauthenticated attackers to update plugin settings.	6.5	More Details
CVE-2024-9860	The Bridge Core plugin for WordPress is vulnerable to unauthorized modification of data or loss of data due to a missing capability check on the 'import_action' and 'install_plugin_per_demo' functions in versions up to, and including, 3.3. This makes it possible for authenticated attackers with subscriber-level permissions or above, to delete or change plugin settings, import demo data, and install limited plugins.	6.5	More Details
CVE-2024-9676	A vulnerability was found in Podman, Buildah, and CRI-O. A symlink traversal vulnerability in the containers/storage library can cause Podman, Buildah, and CRI-O to hang and result in a denial of service via OOM kill when running a malicious image using an automatically assigned user namespace (`--userns=auto` in Podman and Buildah). The containers/storage library will read /etc/passwd inside the container, but does not properly validate if that file is a symlink, which can be used to cause the library to read an arbitrary file on the host.	6.5	More Details
CVE-2024-47164	Gradio is an open-source Python package designed for quick prototyping. This vulnerability relates to the **bypass of directory traversal checks** within the `is_in_or_equal` function. This function, intended to check if a file resides within a given directory, can be bypassed with certain payloads that manipulate file paths using `..` (parent directory) sequences. Attackers could potentially access restricted files if they are able to exploit this flaw, although the difficulty is high. This primarily impacts users relying on Gradio's blocklist or directory access validation, particularly when handling file uploads. Users are advised to upgrade to `gradio>=5.0` to address this issue. As a workaround, users can manually sanitize and normalize file paths in their Gradio deployment before passing them to the `is_in_or_equal` function. Ensuring that all file paths are properly resolved and absolute can help mitigate the bypass vulnerabilities caused by the improper handling of `..` sequences or malformed paths.	6.5	More Details
CVE-2024-45736	In Splunk Enterprise versions below 9.3.1, 9.2.3, and 9.1.6 and Splunk Cloud Platform versions below 9.2.2403.107, 9.1.2312.204, and 9.1.2312.111, a low-privileged user that does not hold the "admin" or "power" Splunk roles could craft a search query with an improperly formatted "INGEST_EVAL" parameter as part of a [Field Transformation](https://docs.splunk.com/Documentation/Splunk/latest/Knowledge/Managefieldtransforms) which could crash the Splunk daemon (splunkd).	6.5	More Details
CVE-2024-7514	The WordPress Comments Import & Export plugin for WordPress is vulnerable to to arbitrary file read due to insufficient file path validation during the comments import process, in versions up to, and including, 2.3.7. This makes it possible for authenticated attackers, with Author-level access and above, to read the contents of arbitrary files on the server, which can contain sensitive information. The issue was partially fixed in version 2.3.8 and fully fixed in 2.3.9	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21196	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: X Plugin). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2024-21205	Vulnerability in the Oracle Service Bus product of Oracle Fusion Middleware (component: OSB Core Functionality). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Service Bus. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Service Bus accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).	6.5	More Details
CVE-2024-47833	Taipy is an open-source Python library for easy, end-to-end application development for data scientists and machine learning engineers. In affected versions session cookies are served without Secure and HTTPOnly flags. This issue has been addressed in release version 4.0.0 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2024-45118	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have high impact on integrity. Exploitation of this issue does not require user interaction.	6.5	More Details
CVE-2024-21230	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	6.5	More Details
CVE-2024-48041	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CreativeMindsSolutions CM Tooltip Glossary allows Stored XSS.This issue affects CM Tooltip Glossary: from n/a through 4.3.9.	6.5	More Details
CVE-2024-21262	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/ODBC). Supported versions that are affected are 9.0.0 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Connectors accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Connectors. CVSS 3.1 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L).	6.5	More Details
CVE-2024-9466	A cleartext storage of sensitive information vulnerability in Palo Alto Networks Expedition allows an authenticated attacker to reveal firewall usernames, passwords, and API keys generated using those credentials.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6657	A denial of service may be caused to a single peripheral device in a BLE network when multiple central devices continuously connect and disconnect to the peripheral. A hard reset is required to recover the peripheral device.	6.5	More Details
CVE-2024-46215	A vulnerability was discovered in KM08-708H-v1.1, There is a buffer overflow in the sub_445BDC() function within the /usr/sbin/goahead program; The strcpy function is executed without checking the length of the string, leading to a buffer overflow.	6.5	More Details
CVE-2024-9464	An OS command injection vulnerability in Palo Alto Networks Expedition allows an authenticated attacker to run arbitrary OS commands as root in Expedition, resulting in disclosure of usernames, cleartext passwords, device configurations, and device API keys of PAN-OS firewalls.	6.5	More Details
CVE-2024-44415	A vulnerability was discovered in DI_8200-16.07.26A1, There is a buffer overflow in the dbsrv_asp function; The strcpy function is executed without checking the length of the string, leading to a buffer overflow.	6.5	More Details
CVE-2024-47508	An Allocation of Resources Without Limits or Throttling vulnerability in the PFE management daemon (evo-pfemand) of Juniper Networks Junos OS Evolved allows an authenticated, network-based attacker to cause an FPC crash leading to a Denial of Service (DoS).When specific SNMP GET operations or specific low-priviledged CLI commands are executed, a GUID resource leak will occur, eventually leading to exhaustion and resulting in FPCs to hang. Affected FPCs need to be manually restarted to recover. GUID exhaustion will trigger a syslog message like one of the following: evo-pfemand[<pid>]: get_next_guid: Ran out of Guid Space ... evo-aftmand-zx[<pid>]: get_next_guid: Ran out of Guid Space ... The leak can be monitored by running the following command and taking note of the values in the rightmost column labeled Guids: user@host> show platform application-info allocations app evo-pfemand/evo-pfemand In case one or more of these values are constantly increasing the leak is happening. This issue affects Junos OS Evolved: * All versions before 21.2R3-S8-EVO, * 21.3 versions before 21.3R3-EVO; * 21.4 versions before 22.1R2-EVO, * 22.1 versions before 22.1R1-S1-EVO, 22.1R2-EVO. Please note that this issue is similar to, but different from CVE-2024-47505 and CVE-2024-47509.	6.5	More Details
CVE-2024-9895	The Smart Online Order for Clover plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's moo_receipt_link shortcode in all versions up to, and including, 1.5.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9704	The Social Sharing (by Danny) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'dvk_social_sharing' shortcode in all versions up to, and including, 1.3.7 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9696	The Rescue Shortcodes plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'rescue_tab' shortcode in all versions up to, and including, 2.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9656	The Mynx Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 0.27.8 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-9595	The TablePress – Tables in WordPress made easy plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the table cell content in all versions up to, and including, 2.4.2 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-2024-8915	The Category Icon plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-7963	The CMSMasters Content Composer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's multiple shortcodes in all versions up to, and including, 1.8.8 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-47816	ImportDump is a mediawiki extension designed to automate user import requests. A user's local actor ID is stored in the database to tell who made what requests. Therefore, if a user on another wiki happens to have the same actor ID as someone on the central wiki, the user on the other wiki can act as if they're the original wiki requester. This can be abused to create new comments, edit the request, and view the request if it's marked private. This issue has been addressed in commit `5c91dfc` and all users are advised to update. Users unable to update may disable the special page outside of their global wiki. See `miraheze/mw-config@e566499` for details on that.	6.4	More Details
CVE-2024-9451	The Embed PDF Viewer plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'height' and 'width' parameters in all versions up to, and including, 2.4.4 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-2024-9066	The Marketing and SEO Booster plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.9.10 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9543	The PowerPress Podcasting plugin by Blubrry plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'skipto' shortcode in all versions up to, and including, 11.9.18 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9064	The Elementor Inline SVG plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.2.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-9057	The Curator.io: Show all your social media posts in a beautiful feed. plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the ‘feed_id’ attribute in all versions up to, and including, 1.9 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8987	The Youzify – BuddyPress Community, User Profile, Social Network & Membership Plugin for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's youzify_media shortcode in all versions up to, and including, 1.3.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9072	The GDPR-Extensions-com – Consent Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-9457	The WP Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 3.0.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-9074	The Advanced Blocks Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 1.0.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.	6.4	More Details
CVE-2024-9051	The WP Ultimate Post Grid plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpupg-grid-with-filters shortcode in all versions up to, and including, 3.9.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9449	The Auto iFrame plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'tag' parameter in all versions up to, and including, 1.7 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Author-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9793	A vulnerability classified as critical was found in Tenda AC1206 up to 15.03.06.23. This vulnerability affects the function ate_iwpriv_set/ate_ifconfig_set of the file /goform/ate. The manipulation leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-9974	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file classes/Master.php?f=add_to_card of the component POST Request Handler. The manipulation of the argument product_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9808	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/?page=products/view_product. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9905	A vulnerability, which was classified as critical, has been found in SourceCodester Online Eyewear Shop 1.0. This issue affects some unknown processing of the file /admin/?page=inventory/view_inventory&id=2. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9975	A vulnerability was found in SourceCodester Drag and Drop Image Upload 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /upload.php. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9976	A vulnerability classified as critical has been found in code-projects Pharmacy Management System 1.0. This affects an unknown part of the file /php/manage_customer.php?action=search. The manipulation of the argument text leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9917	A vulnerability, which was classified as critical, was found in HuangDou UTCMS V9. This affects an unknown part of the file app/modules/ut-template/admin/template_creat.php. The manipulation of the argument content leads to deserialization. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-9894	A vulnerability, which was classified as critical, was found in code-projects Blood Bank System 1.0. Affected is an unknown function of the file reset.php. The manipulation of the argument useremail leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9794	A vulnerability, which was classified as critical, has been found in Codezips Online Shopping Portal 1.0. This issue affects some unknown processing of the file /update-image1.php. The manipulation of the argument productimage1 leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9809	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been declared as critical. Affected by this vulnerability is the function delete_product of the file /classes/Master.php?f=delete_product. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9817	A vulnerability was found in code-projects Blood Bank System 1.0. It has been classified as critical. This affects an unknown part of the file /update.php. The manipulation of the argument name leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9973	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/?page=reports of the component Report Viewing Page. The manipulation of the argument date leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9594	A security issue was discovered in the Kubernetes Image Builder versions <= v0.1.37 where default credentials are enabled during the image build process when using the Nutanix, OVA, QEMU or raw providers. The credentials can be used to gain root access. The credentials are disabled at the conclusion of the image build process. Kubernetes clusters are only affected if their nodes use VM images created via the Image Builder project. Because these images were vulnerable during the image build process, they are affected only if an attacker was able to reach the VM where the image build was happening and used the vulnerability to modify the image at the time the image build was occurring.	6.3	More Details
CVE-2024-9520	The UserPlus plugin for WordPress is vulnerable to unauthorized access, modification, and loss of data due to a missing capability check on multiple functions in all versions up to, and including, 2.0. This makes it possible for authenticated attackers with subscriber-level permissions or above, to add, modify, or delete user meta and plugin options.	6.3	More Details
CVE-2024-0129	NVIDIA NeMo contains a vulnerability in SaveRestoreConnector where a user may cause a path traversal issue via an unsafe .tar file extraction. A successful exploit of this vulnerability may lead to code execution and data tampering.	6.3	More Details
CVE-2024-39440	In DRM service, there is a possible system crash due to null pointer dereference. This could lead to local denial of service with System execution privileges needed.	6.2	More Details
CVE-2024-39439	In DRM service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45184	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modems with chipset Exynos 9820, 9825, 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 9110, W920, W930, Modem 5123, and Modem 5300. A USAT out-of-bounds write due to a heap buffer overflow can lead to a Denial of Service.	6.2	More Details
CVE-2024-9592	The Easy PayPal Gift Certificate plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.2.3. This is due to missing or incorrect nonce validation on the 'wpppgc_plugin_options' function. This makes it possible for unauthenticated attackers to update the plugin's settings and inject malicious JavaScript via a forged request, granted they can trick a site administrator into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-48821	Cross Site Scripting vulnerability in Automatic Systems Maintenance SlimLane 29565_d74ecce0c1081d50546db573a499941b10799fb7 allows a remote attacker to escalate privileges via the FtpConfig.php component.	6.1	More Details
CVE-2024-9205	The Maximum Products per User for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 4.2.8. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9670	The 2D Tag Cloud plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 6.0.2. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-48937	Znuny before LTS 6.5.1 through 6.5.10 and 7.0.1 through 7.0.16 allows XSS. JavaScript code in the short description of the SLA field in Activity Dialogues is executed.	6.1	More Details
CVE-2024-45123	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 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.	6.1	More Details
CVE-2024-9377	The Products, Order & Customers Export for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.0.15. 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-2024-21535	Versions of the package markdown-to-jsx before 7.4.0 are vulnerable to Cross-site Scripting (XSS) via the src property due to improper input sanitization. An attacker can execute arbitrary code by injecting a malicious iframe element in the markdown.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9211	The FULL – Cliente plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg & remove_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.1.22. 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-2024-48933	A cross-site scripting (XSS) vulnerability in LemonLDAP::NG before 2.19.3 allows remote attackers to inject arbitrary web script or HTML into the login page via a username if userControl has been set to a non-default value that allows special HTML characters.	6.1	More Details
CVE-2023-45361	An issue was discovered in VectorComponentUserLinks.php in the Vector Skin component in MediaWiki before 1.39.5 and 1.40.x before 1.40.1. vector-intro-page MalformedTitleException is uncaught if it is not a valid title, leading to incorrect web pages.	6.1	More Details
CVE-2024-21263	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22 and prior to 7.1.2. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox and unauthorized read access to a subset of Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:H).	6.1	More Details
CVE-2024-9467	A reflected XSS vulnerability in Palo Alto Networks Expedition enables execution of malicious JavaScript in the context of an authenticated Expedition user's browser if that user clicks on a malicious link, allowing phishing attacks that could lead to Expedition browser session theft.	6.1	More Details
CVE-2024-9221	The Tainacan plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 0.21.10. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-21202	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: PIA Core Technology). Supported versions that are affected are 8.59, 8.60 and 8.61. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise PeopleTools, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9346	The Embed videos and respect privacy plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'v' parameter in all versions up to, and including, 1.2 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-2024-9436	The PublishPress Revisions: Duplicate Posts, Submit, Approve and Schedule Content Changes plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.5.14. 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-2024-8729	The Easy Social Share Buttons plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.4.5. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9616	The BlockMeister – Block Pattern Builder plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.1.10. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9611	The Increase upload file size & Maximum Execution Time limit plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 2.0. 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-2024-9232	The Download Plugins and Themes in ZIP from Dashboard plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.9.1. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-9610	The Language Switcher plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.7.13. 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-2024-47815	IncidentReporting is a MediaWiki extension for moving incident reports from wikitext to database tables. There are a variety of Cross-site Scripting issues, though all of them require elevated permissions. Some are available to anyone who has the `editincidents` right, some are available to those who can edit interface messages (typically administrators and interface admins), and one is available to those who can edit LocalSettings.php. These issues have been addressed in commit `43896a4` and all users are advised to upgrade. Users unable to upgrade should prevent access to the Special:IncidentReports page.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47812	ImportDump is an extension for mediawiki designed to automate user import requests. Anyone who can edit the interface strings of a wiki (typically administrators and interface admins) can embed XSS payloads in the messages for dates, and thus XSS anyone who views Special:RequestImportQueue. This issue has been patched in commit `d054b95` and all users are advised to apply this commit to their branch. Users unable to upgrade may either Prevent access to Special:RequestImportQueue on all wikis, except for the global wiki; and If an interface administrator (or equivalent) level protection is available (which is not provided by default) on the global wiki, protect the affected messages up to that level. This causes the XSS to be virtually useless as users with those rights can already edit Javascript pages. Or Prevent access to Special:RequestImportQueue altogether.	6.0	More Details
CVE-2024-22068	Improper Privilege Management vulnerability in ZTE ZXR10 1800-2S series ,ZXR10 2800-4,ZXR10 3800-8,ZXR10 160 series on 64 bit allows Functionality Bypass.This issue affects ZXR10 1800-2S series ,ZXR10 2800-4,ZXR10 3800-8,ZXR10 160 series: V4.00.10 and earlier.	6.0	More Details
CVE-2024-21273	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22 and prior to 7.1.2. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:N/A:N).	6.0	More Details
CVE-2024-8184	There exists a security vulnerability in Jetty's ThreadLimitHandler.getRemote() which can be exploited by unauthorized users to cause remote denial-of-service (DoS) attack. By repeatedly sending crafted requests, attackers can trigger OutofMemory errors and exhaust the server's memory.	5.9	More Details
CVE-2024-45085	IBM WebSphere Application Server 8.5 is vulnerable to a denial of service, under certain configurations, caused by an unexpected specially crafted request. A remote attacker could exploit this vulnerability to cause an error resulting in a denial of service.	5.9	More Details
CVE-2024-47494	A Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability in the AgentD process of Juniper Networks Junos OS allows an attacker who is already causing impact to established sessions which generates counter changes picked up by the AgentD process during telemetry polling, to move the AgentD process into a state where AgentD attempts to reap an already destroyed sensor. This reaping attempt then leads to memory corruption causing the FPC to crash which is a Denial of Service (DoS). The FPC will recover automatically without user intervention after the crash. This issue affects Junos OS: * All versions before 21.4R3-S9 * From 22.2 before 22.2R3-S5, * From 22.3 before 22.3R3-S4, * From 22.4 before 22.4R3-S3, * From 23.2 before 23.2R2-S2, * From 23.4 before 23.4R2. This issue does not affect Junos OS Evolved.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47491	An Improper Handling of Exceptional Conditions vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network-based, unauthenticated attacker to cause Denial of Service (DoS). When a BGP UPDATE with malformed path attribute is received over an established BGP session, rpd crashes and restarts. Continuous receipt of a BGP UPDATE with a specifically malformed path attribute will create a sustained Denial of Service (DoS) condition for impacted devices. While this issue affects systems running 32-bit and 64-bit systems, the probability of impact on 64-bit system is extremely low. According to KB25803 https://supportportal.juniper.net/s/article/Junos-How-to-check-if-Junos-OS-is-64-or-32-bit-on-a-router , customers can confirm 32-bit or 64-bit system via the ' show version detail ' command: lab@router> show version detaill match 32 JUNOS 32-bit kernel Software Suite lab@router> show version detaill match 64 JUNOS 64-bit kernel Software Suite This issue affects: Juniper Networks Junos OS: * All versions before 21.4R3-S8, * from 22.2 before 22.2R3-S4, * from 22.4 before 22.4R3-S3, * from 23.2 before 23.2R2-S1, * from 23.4 before 23.4R1-S2, 23.4R2. Juniper Networks Junos OS Evolved: * All versions before 21.4R3-S8-EVO, * from 22.2 before 22.2R3-S4-EVO, * from 22.4 before 22.4R3-S3-EVO, * from 23.2 before 23.2R2-S1-EVO, * from 23.4 before 23.4R1-S2-EVO, 23.4R2-EVO.	5.9	More Details
CVE-2024-48913	Hono, a web framework, prior to version 4.6.5 is vulnerable to bypass of cross-site request forgery (CSRF) middleware by a request without Content-Type header. Although the CSRF middleware verifies the Content-Type Header, Hono always considers a request without a Content-Type header to be safe. This can allow an attacker to bypass CSRF protection implemented with Hono CSRF middleware. Version 4.6.5 fixes this issue.	5.9	More Details
CVE-2024-47831	Next.js is a React Framework for the Web. Cersions on the 10.x, 11.x, 12.x, 13.x, and 14.x branches before version 14.2.7 contain a vulnerability in the image optimization feature which allows for a potential Denial of Service (DoS) condition which could lead to excessive CPU consumption. Neither the `next.config.js` file that is configured with `images.unoptimized` set to `true` or `images.loader` set to a non-default value nor the Next.js application that is hosted on Vercel are affected. This issue was fully patched in Next.js `14.2.7`. As a workaround, ensure that the `next.config.js` file has either `images.unoptimized`, `images.loader` or `images.loaderFile` assigned.	5.9	More Details
CVE-2024-48793	An issue in INATRONIC com.inatronic.bmw 2.7.1 allows a remote attacker to obtain sensitive information via the firmware update process.	5.9	More Details
CVE-2024-47885	The Astro web framework has a DOM Clobbering gadget in the client-side router starting in version 3.0.0 and prior to version 4.16.1. It can lead to cross-site scripting (XSS) in websites enables Astro's client-side routing and has *stored* attacker-controlled scriptless HTML elements (i.e., `iframe` tags with unsanitized `name` attributes) on the destination pages. This vulnerability can result in cross-site scripting (XSS) attacks on websites that built with Astro that enable the client-side routing with `ViewTransitions` and store the user-inserted scriptless HTML tags without properly sanitizing the `name` attributes on the page. Version 4.16.1 contains a patch for this issue.	5.9	More Details
CVE-2024-48942	The Syracom Secure Login (2FA) plugin for Jira, Confluence, and Bitbucket through 3.1.4.5 allows remote attackers to easily brute-force the 2FA PIN via the plugins/servlet/twofactor/public/pinvalidation endpoint. The last 30 and the next 30 tokens are valid.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47506	A Deadlock vulnerability in the packet forwarding engine (PFE) of Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause a Denial of Service (DoS). When a large amount of traffic is processed by ATP Cloud inspection, a deadlock can occur which will result in a PFE crash and restart. Whether the crash occurs, depends on system internal timing that is outside the attackers control. This issue affects Junos OS on SRX Series: * All versions before 21.3R3-S1, * 21.4 versions before 21.4R3, * 22.1 versions before 22.1R2, * 22.2 versions before 22.2R1-S2, 22.2R2.	5.9	More Details
CVE-2024-8530	CWE-306: Missing Authentication for Critical Function vulnerability exists that could cause exposure of private data when an already generated “logcaptures” archive is accessed directly by HTTPS.	5.9	More Details
CVE-2024-45397	h2o is an HTTP server with support for HTTP/1.x, HTTP/2 and HTTP/3. When an HTTP request using TLS/1.3 early data on top of TCP Fast Open or QUIC 0-RTT packets is received and the IP-address-based access control is used, the access control does not detect and prohibit HTTP requests conveyed by packets with a spoofed source address. This behavior allows attackers on the network to execute HTTP requests from addresses that are otherwise rejected by the address-based access control. The vulnerability has been addressed in commit 15ed15a. Users may disable the use of TCP FastOpen and QUIC to mitigate the issue.	5.9	More Details
CVE-2024-47507	An Improper Check for Unusual or Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, network-based attacker to cause an integrity impact to the downstream devices. When a peer sends a BGP update message which contains the aggregator attribute with an ASN value of zero (0), rpd accepts and propagates this attribute, which can cause issues for downstream BGP peers receiving this. This issue affects: Junos OS: * All versions before 21.4R3-S6, * 22.2 versions before 22.2R3-S3, * 22.4 versions before 22.4R3; Junos OS Evolved: * All versions before 21.4R3-S7-EVO, * 22.2 versions before 22.2R3-S4-EVO, * 22.4 versions before 22.4R3-EVO.	5.8	More Details
CVE-2024-47489	An Improper Handling of Exceptional Conditions vulnerability in the Packet Forwarding Engine (pfe) of the Juniper Networks Junos OS Evolved on ACX Series devices allows an unauthenticated, network based attacker sending specific transit protocol traffic to cause a partial Denial of Service (DoS) to downstream devices. Receipt of specific transit protocol packets is incorrectly processed by the Routing Engine (RE), filling up the DDoS protection queue which is shared between routing protocols. This influx of transit protocol packets causes DDoS protection violations, resulting in protocol flaps which can affect connectivity to networking devices. This issue affects both IPv4 and IPv6. This issue does not require any specific routing protocol to be configured or enabled. The following commands can be used to monitor the DDoS protection queue: labuser@re0> show evo-pfemand host pkt-stats labuser@re0> show host-path ddos all-policers This issue affects Junos OS Evolved: * All versions before 21.4R3-S8-EVO, * from 22.2 before 22.2R3-S4-EVO, * from 22.3 before 22.3R3-S4-EVO, * from 22.4 before 22.4R3-S3-EVO, * from 23.2 before 23.2R2-EVO, * from 23.4 before 23.4R1-S1-EVO, 23.4R2-EVO, * from 24.2 before 24.2R2-EVO.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47672	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: don't wait for tx queues if firmware is dead There is a WARNING in iwl_trans_wait_tx_queues_empty() (that was recently converted from just a message), that can be hit if we wait for TX queues to become empty after firmware died. Clearly, we can't expect anything from the firmware after it's declared dead. Don't call iwl_trans_wait_tx_queues_empty() in this case. While it could be a good idea to stop the flow earlier, the flush functions do some maintenance work that is not related to the firmware, so keep that part of the code running even when the firmware is not running. [edit commit message]	5.5	More Details
CVE-2024-47420	Animate versions 23.0.7, 24.0.4 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-2024-45145	Lightroom Desktop versions 7.4.1, 13.5, 12.5.1 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-2024-45315	The Improper link resolution before file access ('Link Following') vulnerability in SonicWall Connect Tunnel (version 12.4.3.271 and earlier of Windows client) allows users with standard privileges to create arbitrary folders and files, potentially leading to local Denial of Service (DoS) attack.	5.5	More Details
CVE-2024-5474	A potential information disclosure vulnerability was reported in Lenovo's packaging of Dolby Vision Provisioning software prior to version 2.0.0.2 that could allow a local attacker to read files on the system with elevated privileges during installation of the package. Previously installed versions are not affected by this issue.	5.5	More Details
CVE-2024-47662	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Remove register from DCN35 DMCUB diagnostic collection [Why] These registers should not be read from driver and triggering the security violation when DMCUB work times out and diagnostics are collected blocks Z8 entry. [How] Remove the register read from DCN35.	5.5	More Details
CVE-2024-47663	In the Linux kernel, the following vulnerability has been resolved: staging: iio: frequency: ad9834: Validate frequency parameter value In ad9834_write_frequency() clk_get_rate() can return 0. In such case ad9834_calc_freqreg() call will lead to division by zero. Checking 'if (fout > (clk_freq / 2))' doesn't protect in case of 'fout' is 0. ad9834_write_frequency() is called from ad9834_write(), where fout is taken from text buffer, which can contain any value. Modify parameters checking. Found by Linux Verification Center (linuxtesting.org) with SVACE.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47674	In the Linux kernel, the following vulnerability has been resolved: mm: avoid leaving partial pfn mappings around in error case As Jann points out, PFN mappings are special, because unlike normal memory mappings, there is no lifetime information associated with the mapping - it is just a raw mapping of PFNs with no reference counting of a 'struct page'. That's all very much intentional, but it does mean that it's easy to mess up the cleanup in case of errors. Yes, a failed mmap() will always eventually clean up any partial mappings, but without any explicit lifetime in the page table mapping itself, it's very easy to do the error handling in the wrong order. In particular, it's easy to mistakenly free the physical backing store before the page tables are actually cleaned up and (temporarily) have stale dangling PTE entries. To make this situation less error-prone, just make sure that any partial pfn mapping is torn down early, before any other error handling.	5.5	More Details
CVE-2024-47763	Wasmtime is an open source runtime for WebAssembly. Wasmtime's implementation of WebAssembly tail calls combined with stack traces can result in a runtime crash in certain WebAssembly modules. The runtime crash may be undefined behavior if Wasmtime was compiled with Rust 1.80 or prior. The runtime crash is a deterministic process abort when Wasmtime is compiled with Rust 1.81 and later. WebAssembly tail calls are a proposal which relatively recently reached stage 4 in the standardization process. Wasmtime first enabled support for tail calls by default in Wasmtime 21.0.0, although that release contained a bug where it was only on-by-default for some configurations. In Wasmtime 22.0.0 tail calls were enabled by default for all configurations. The specific crash happens when an exported function in a WebAssembly module (or component) performs a `return_call` (or `return_call_indirect` or `return_call_ref`) to an imported host function which captures a stack trace (for example, the host function raises a trap). In this situation, the stack-walking code previously assumed there was always at least one WebAssembly frame on the stack but with tail calls that is no longer true. With the tail-call proposal it's possible to have an entry trampoline appear as if it directly called the exit trampoline. This situation triggers an internal assert in the stack-walking code which raises a Rust `panic!()`. When Wasmtime is compiled with Rust versions 1.80 and prior this means that an `extern "C"` function in Rust is raising a `panic!()`. This is technically undefined behavior and typically manifests as a process abort when the unwinder fails to unwind Cranelift-generated frames. When Wasmtime is compiled with Rust versions 1.81 and later this panic becomes a deterministic process abort. Overall the impact of this issue is that this is a denial-of-service vector where a malicious WebAssembly module or component can cause the host to crash. There is no other impact at this time other than availability of a service as the result of the crash is always a crash and no more. This issue was discovered by routine fuzzing performed by the Wasmtime project via Google's OSS-Fuzz infrastructure. We have no evidence that it has ever been exploited by an attacker in the wild. All versions of Wasmtime which have tail calls enabled by default have been patched: * 21.0.x - patched in 21.0.2 * 22.0.x - patched in 22.0.1 * 23.0.x - patched in 23.0.3 * 24.0.x - patched in 24.0.1 * 25.0.x - patched in 25.0.2. Wasmtime versions from 12.0.x (the first release with experimental tail call support) to 20.0.x (the last release with tail-calls off-by-default) have support for tail calls but the support is disabled by default. These versions are not affected in their default configurations, but users who explicitly enabled tail call support will need to either disable tail call support or upgrade to a patched version of Wasmtime. The main workaround for this issue is to disable tail support for tail calls in Wasmtime, for example with `Config::wasm_tail_call(false)`. Users are otherwise encouraged to upgrade to patched versions.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47496	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS allows a local, low-privileged attacker to cause a Denial-of-Service (DoS). When a specific command is executed, the pfe crashes. This will cause traffic forwarding to be interrupted until the system self-recovers. Repeated execution will create a sustained DoS condition. This issue only affects MX Series devices with Line cards MPC1-MPC9. This issue affects: Junos OS on MX Series: * All versions before 21.4R3-S9, * from 22.2 before 22.2R3-S5, * from 22.3 before 22.3R3-S4, * from 22.4 before 22.4R3-S2, * from 23.2 before 23.2R2-S1, * from 23.4 before 23.4R2.	5.5	More Details
CVE-2024-48278	Phpgurukul User Registration & Login and User Management System 3.2 is vulnerable to Cross Site Request Forgery (CSRF) via /edit-profile.php.	5.5	More Details
CVE-2024-47658	In the Linux kernel, the following vulnerability has been resolved: crypto: stm32/cryp - call finalize with bh disabled The finalize operation in interrupt mode produce a produces a spinlock recursion warning. The reason is the fact that BH must be disabled during this process.	5.5	More Details
CVE-2024-47664	In the Linux kernel, the following vulnerability has been resolved: spi: hisi-kunpeng: Add verification for the max_frequency provided by the firmware If the value of max_speed_hz is 0, it may cause a division by zero error in hisi_calc_effective_speed(). The value of max_speed_hz is provided by firmware. Firmware is generally considered as a trusted domain. However, as division by zero errors can cause system failure, for defense measure, the value of max_speed is validated here. So 0 is regarded as invalid and an error code is returned.	5.5	More Details
CVE-2024-47661	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid overflow from uint32_t to uint8_t [WHAT & HOW] dmub_rb_cmd's ramping_boundary has size of uint8_t and it is assigned 0xFFFF. Fix it by changing it to uint8_t with value of 0xFF. This fixes 2 INTEGER_OVERFLOW issues reported by Coverity.	5.5	More Details
CVE-2024-47665	In the Linux kernel, the following vulnerability has been resolved: i3c: mipi-i3c-hci: Error out instead on BUG_ON() in IBI DMA setup Definitely condition dma_get_cache_alignment * defined value > 256 during driver initialization is not reason to BUG_ON(). Turn that to graceful error out with -EINVAL.	5.5	More Details
CVE-2024-47419	Animate versions 23.0.7, 24.0.4 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-2024-20787	Substance3D - Painter versions 10.0.1 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 Number	Description	Base Score	Reference
CVE-2024-47501	A NULL Pointer Dereference vulnerability in the packet forwarding engine (pfe) of Juniper Networks Junos OS on MX304, MX with MPC10/11/LC9600, and EX9200 with EX9200-15C allows a locally authenticated attacker with low privileges to cause a Denial of Service (DoS). In a VPLS or Junos Fusion scenario, the execution of specific show commands will cause all FPCs hosting VPLS sessions or connecting to satellites to crash and restart. This issue affects Junos on MX304, MX with MPC10/11/LC9600 and EX9200 with EX9200-15C: * All version before 21.2R3-S1, * 21.3 versions before 21.3R3, * 21.4 versions before 21.4R2.	5.5	More Details
CVE-2024-47673	In the Linux kernel, the following vulnerability has been resolved: wifi: iwlwifi: mvm: pause TCM when the firmware is stopped Not doing so will make us send a host command to the transport while the firmware is not alive, which will trigger a WARNING. bad state = 0 WARNING: CPU: 2 PID: 17434 at drivers/net/wireless/intel/iwlwifi/iwl-trans.c:115 iwl_trans_send_cmd+0x1cb/0x1e0 [iwlwifi] RIP: 0010:iwl_trans_send_cmd+0x1cb/0x1e0 [iwlwifi] Call Trace: <TASK> iwl_mvm_send_cmd+0x40/0xc0 [iwlmvm] iwl_mvm_config_scan+0x198/0x260 [iwlmvm] iwl_mvm_recalc_tcm+0x730/0x11d0 [iwlmvm] iwl_mvm_tcm_work+0x1d/0x30 [iwlmvm] process_one_work+0x29e/0x640 worker_thread+0x2df/0x690 ? rescuer_thread+0x540/0x540 kthread+0x192/0x1e0 ? set_kthread_struct+0x90/0x90 ret_from_fork+0x22/0x30	5.5	More Details
CVE-2024-39527	An Exposure of Sensitive Information to an Unauthorized Actor vulnerability in the command-line interface (CLI) of Juniper Networks Junos OS on SRX Series devices allows a local, low-privileged user with access to the Junos CLI to view the contents of protected files on the file system. Through the execution of crafted CLI commands, a user with limited permissions (e.g., a low privilege login class user) can access protected files that should not be accessible to the user. These files may contain sensitive information that can be used to cause further impact to the system. This issue affects Junos OS on SRX Series: * All versions before 21.4R3-S8, * 22.2 before 22.2R3-S5, * 22.3 before 22.3R3-S4, * 22.4 before 22.4R3-S4, * 23.2 before 23.2R2-S2, * 23.4 before 23.4R2.	5.5	More Details
CVE-2024-47667	In the Linux kernel, the following vulnerability has been resolved: PCI: keystone: Add workaround for Errata #i2037 (AM65x SR 1.0) Errata #i2037 in AM65x/DRA80xM Processors Silicon Revision 1.0 (SPRZ452D_July 2018_Revised December 2019 [1]) mentions when an inbound PCIe TLP spans more than two internal AXI 128-byte bursts, the bus may corrupt the packet payload and the corrupt data may cause associated applications or the processor to hang. The workaround for Errata #i2037 is to limit the maximum read request size and maximum payload size to 128 bytes. Add workaround for Errata #i2037 here. The errata and workaround is applicable only to AM65x SR 1.0 and later versions of the silicon will have this fixed. [1] -> https://www.ti.com/lit/er/sprz452i/sprz452i.pdf	5.5	More Details
CVE-2024-9908	A vulnerability, which was classified as critical, was found in D-Link DIR-619L B1 2.06. Affected is the function formSetMACFilter of the file /goform/formSetMACFilter. The manipulation of the argument curTime leads to buffer overflow. The exploit has been disclosed to the public and may be used.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47669	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix state management in error path of log writing function After commit a694291a6211 ("nilfs2: separate wait function from nilfs_segctor_write") was applied, the log writing function nilfs_segctor_do_construct() was able to issue I/O requests continuously even if user data blocks were split into multiple logs across segments, but two potential flaws were introduced in its error handling. First, if nilfs_segctor_begin_construction() fails while creating the second or subsequent logs, the log writing function returns without calling nilfs_segctor_abort_construction(), so the writeback flag set on pages/folios will remain uncleared. This causes page cache operations to hang waiting for the writeback flag. For example, truncate_inode_pages_final(), which is called via nilfs_evict_inode() when an inode is evicted from memory, will hang. Second, the NILFS_I_COLLECTED flag set on normal inodes remain uncleared. As a result, if the next log write involves checkpoint creation, that's fine, but if a partial log write is performed that does not, inodes with NILFS_I_COLLECTED set are erroneously removed from the "sc_dirty_files" list, and their data and b-tree blocks may not be written to the device, corrupting the block mapping. Fix these issues by uniformly calling nilfs_segctor_abort_construction() on failure of each step in the loop in nilfs_segctor_do_construct(), having it clean up logs and segment usages according to progress, and correcting the conditions for calling nilfs_redirty_inodes() to ensure that the NILFS_I_COLLECTED flag is cleared.	5.5	More Details
CVE-2024-47671	In the Linux kernel, the following vulnerability has been resolved: USB: usbtmc: prevent kernel-usb-infoleak The syzbot reported a kernel-usb-infoleak in usbtmc_write, we need to clear the structure before filling fields.	5.5	More Details
CVE-2024-47666	In the Linux kernel, the following vulnerability has been resolved: scsi: pm80xx: Set phy->enable_completion only when we wait for it pm8001_phy_control() populates the enable_completion pointer with a stack address, sends a PHY_LINK_RESET / PHY_HARD_RESET, waits 300 ms, and returns. The problem arises when a phy control response comes late. After 300 ms the pm8001_phy_control() function returns and the passed enable_completion stack address is no longer valid. Late phy control response invokes complete() on a dangling enable_completion pointer which leads to a kernel crash.	5.5	More Details
CVE-2024-9469	A problem with a detection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices enables a user with Windows non-administrative privileges to disable the agent. This issue may be leveraged by malware to disable the Cortex XDR agent and then to perform malicious activity.	5.5	More Details
CVE-2024-44157	A stack buffer overflow was addressed through improved input validation. This issue is fixed in Apple TV 1.5.0.152 for Windows, iTunes 12.13.3 for Windows. Parsing a maliciously crafted video file may lead to unexpected system termination.	5.5	More Details
CVE-2024-8264	Fortra's Robot Schedule Enterprise Agent prior to version 3.05 writes FTP username and password information to the agent log file when detailed logging is enabled.	5.5	More Details
CVE-2024-48902	In JetBrains YouTrack before 2024.3.46677 improper access control allowed users with project update permission to delete applications via API	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45131	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality and integrity. Exploitation of this issue does not require user interaction.	5.4	More Details
CVE-2024-45128	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity and availability. Exploitation of this issue does not require user interaction.	5.4	More Details
CVE-2024-7049	In version v0.3.8 of open-webui/open-webui, a vulnerability exists where a token is returned when a user with a pending role logs in. This allows the user to perform actions without admin confirmation, bypassing the intended approval process.	5.4	More Details
CVE-2024-9969	NewType WebEIP v3.0 does not properly validate user input, allowing a remote attacker with regular privileges to insert JavaScript into specific parameters, resulting in a Reflected Cross-site Scripting (XSS) attack. The affected product is no longer maintained. It is recommended to upgrade to the new product.	5.4	More Details
CVE-2024-45740	In Splunk Enterprise versions below 9.2.3 and 9.1.6 and Splunk Cloud Platform versions below 9.2.2403, a low-privileged user that does not hold the "admin" or "power" Splunk roles could craft a malicious payload through Scheduled Views that could result in execution of unauthorized JavaScript code in the browser of a user.	5.4	More Details
CVE-2024-45741	In Splunk Enterprise versions below 9.2.3 and 9.1.6 and Splunk Cloud Platform versions below 9.2.2403.108 and 9.1.2312.205, a low-privileged user that does not hold the "admin" or "power" Splunk roles could create a malicious payload through a custom configuration file that the "api.uri" parameter from the "/manager/search/apps/local" endpoint in Splunk Web calls. This could result in execution of unauthorized JavaScript code in the browser of a user.	5.4	More Details
CVE-2024-48941	The Syracom Secure Login (2FA) plugin for Jira, Confluence, and Bitbucket through 3.1.4.5 allows remote attackers to bypass 2FA by interacting with the /rest endpoint of Jira, Confluence, or Bitbucket. In the default configuration, /rest is allowlisted.	5.4	More Details
CVE-2024-21264	Vulnerability in the PeopleSoft Enterprise CC Common Application Objects product of Oracle PeopleSoft (component: Activity Guide Composer). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise CC Common Application Objects. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise CC Common Application Objects accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise CC Common Application Objects accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21286	Vulnerability in the PeopleSoft Enterprise ELM Enterprise Learning Management product of Oracle PeopleSoft (component: Enterprise Learning Management). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise ELM Enterprise Learning Management. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in PeopleSoft Enterprise ELM Enterprise Learning Management, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of PeopleSoft Enterprise ELM Enterprise Learning Management accessible data as well as unauthorized read access to a subset of PeopleSoft Enterprise ELM Enterprise Learning Management accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).	5.4	More Details
CVE-2024-39534	An Incorrect Comparison vulnerability in the local address verification API of Juniper Networks Junos OS Evolved allows an unauthenticated network-adjacent attacker to create sessions or send traffic to the device using the network and broadcast address of the subnet assigned to an interface. This is unintended and unexpected behavior and can allow an attacker to bypass certain compensating controls, such as stateless firewall filters. This issue affects Junos OS Evolved: * All versions before 21.4R3-S8-EVO, * 22.2-EVO before 22.2R3-S4-EVO, * 22.3-EVO before 22.3R3-S4-EVO, * 22.4-EVO before 22.4R3-S3-EVO, * 23.2-EVO before 23.2R2-S1-EVO, * 23.4-EVO before 23.4R1-S2-EVO, 23.4R2-EVO.	5.4	More Details
CVE-2024-47872	Gradio is an open-source Python package designed for quick prototyping. This vulnerability involves **Cross-Site Scripting (XSS)** on any Gradio server that allows file uploads. Authenticated users can upload files such as HTML, JavaScript, or SVG files containing malicious scripts. When other users download or view these files, the scripts will execute in their browser, allowing attackers to perform unauthorized actions or steal sensitive information from their sessions. This impacts any Gradio server that allows file uploads, particularly those using components that process or display user-uploaded files. Users are advised to upgrade to `gradio>=5` to address this issue. As a workaround, users can restrict the types of files that can be uploaded to the Gradio server by limiting uploads to non-executable file types such as images or text. Additionally, developers can implement server-side validation to sanitize uploaded files, ensuring that HTML, JavaScript, and SVG files are properly handled or rejected before being stored or displayed to users.	5.4	More Details
CVE-2024-46237	PHPGurukul Hospital Management System 4.0 is vulnerable to Cross Site Scripting (XSS) via the patname, pataddress, and medhis parameters in doctor/add-patient.php and doctor/edit-patient.php.	5.4	More Details
CVE-2024-48120	X2CRM v8.5 is vulnerable to a stored Cross-Site Scripting (XSS) in the "Opportunities" module. An attacker can inject malicious JavaScript code into the "Name" field when creating a list.	5.4	More Details
CVE-2024-48119	Vtiger CRM v8.2.0 has a HTML Injection vulnerability in the module parameter. Authenticated users can inject arbitrary HTML.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47165	Gradio is an open-source Python package designed for quick prototyping. This vulnerability relates to **CORS origin validation accepting a null origin**. When a Gradio server is deployed locally, the `localhost_aliases` variable includes "null" as a valid origin. This allows attackers to make unauthorized requests from sandboxed iframes or other sources with a null origin, potentially leading to data theft, such as user authentication tokens or uploaded files. This impacts users running Gradio locally, especially those using basic authentication. Users are advised to upgrade to `gradio>=5.0` to address this issue. As a workaround, users can manually modify the `localhost_aliases` list in their local Gradio deployment to exclude "null" as a valid origin. By removing this value, the Gradio server will no longer accept requests from sandboxed iframes or sources with a null origin, mitigating the potential for exploitation.	5.4	More Details
CVE-2024-9587	The Linkz.ai plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'ajax_linkz' function in versions up to, and including, 1.1.8. This makes it possible for authenticated attackers with contributor-level privileges or above, to update plugin settings.	5.4	More Details
CVE-2024-45124	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction.	5.3	More Details
CVE-2024-48790	An issue in ILIFE com.ilife.home.global 1.8.7 allows a remote attacker to obtain sensitive information via the firmware update process.	5.3	More Details
CVE-2024-44807	A directory listing issue in the baserCMS plugin in D-ZERO CO., LTD. BurgerEditor and BurgerEditor Limited Edition before 2.25.1 allows remote attackers to obtain sensitive information by exposing a list of the uploaded files.	5.3	More Details
CVE-2024-48624	In segments\edit.php of DomainMOD below v4.12.0, the segid parameter in the GET request can be exploited to cause a reflected Cross Site Scripting (XSS) vulnerability.	5.3	More Details
CVE-2024-48795	An issue in Creative Labs Pte Ltd com.creative.apps.xficonnect 2.00.02 allows a remote attacker to obtain sensitive information via the firmware update process.	5.3	More Details
CVE-2024-48623	In queue\index.php of DomainMOD below v4.12.0, the list_id and domain_id parameters in the GET request can be exploited to cause a reflected Cross Site Scripting (XSS).	5.3	More Details
CVE-2024-8513	The QA Analytics – Web Analytics Tool with Heatmaps & Session Replay Across All Pages plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the ajax_save_plugin_config() function in all versions up to, and including, 4.1.0.0. This makes it possible for unauthenticated attackers to update the plugin's settings.	5.3	More Details
CVE-2024-6747	Information leakage in mknotifyd in Checkmk before 2.3.0p18, 2.2.0p36, 2.1.0p49 and in 2.0.0p39 (EOL) allows attacker to get potentially sensitive data	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9979	A flaw was found in PyO3. This vulnerability causes a use-after-free issue, potentially leading to memory corruption or crashes via unsound borrowing from weak Python references.	5.3	More Details
CVE-2024-9944	The WooCommerce plugin for WordPress is vulnerable to HTML Injection in all versions up to, and including, 9.0.2. This is due to the plugin not properly neutralizing HTML elements from submitted order forms. This makes it possible for unauthenticated attackers to inject arbitrary HTML that will render when the administrator views order form submissions.	5.3	More Details
CVE-2024-9546	The WPIDE – File Manager & Code Editor plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 3.4.9. This is due to the plugin utilizing the PHP-Parser library, which outputs parser rebuild command execution results. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, which can be used to aid other attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.	5.3	More Details
CVE-2024-21281	Vulnerability in the Oracle Banking Liquidity Management product of Oracle Financial Services Applications (component: Infrastructure). The supported version that is affected is 14.7.0.6.0. Difficult to exploit vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Banking Liquidity Management. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Banking Liquidity Management accessible data as well as unauthorized read access to a subset of Oracle Banking Liquidity Management accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Banking Liquidity Management. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:H/A:L).	5.3	More Details
CVE-2024-9802	The conformance validation endpoint is public so everybody can verify the conformance of onboarded services. The response could contain specific information about the service, including available endpoints, and swagger. It could advise about the running version of a service to an attacker. The attacker could also check if a service is running.	5.3	More Details
CVE-2024-9065	The WP Helper Premium plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'whp_smtp_send_mail_test' function in all versions up to, and including, 4.6.1. This makes it possible for unauthenticated attackers to send emails containing any content and originating from the vulnerable WordPress instance to any recipient.	5.3	More Details
CVE-2024-9671	A vulnerability was found in 3Scale. There is no auth mechanism to see a PDF invoice of a Developer user if the URL is known. Anyone can see the invoice if the URL is known or guessed.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8760	The Stackable – Page Builder Gutenberg Blocks plugin for WordPress is vulnerable to CSS Injection in all versions up to, and including, 3.13.6. This makes it possible for unauthenticated attackers to embed untrusted style information into comments resulting in a possibility of data exfiltration such as admin nonces with limited impact. These nonces could be used to perform CSRF attacks within a limited time window. The presence of other plugins may make additional nonces available, which may pose a risk in plugins that don't perform capability checks to protect AJAX actions or other actions reachable by lower-privileged users.	5.3	More Details
CVE-2024-47828	ampache is a web based audio/video streaming application and file manager. A CSRF attack can be performed in order to delete objects (Playlist, smartlist etc.). Cross-Site Request Forgery (CSRF) is an attack that forces authenticated users to submit a request to a Web application against which they are currently authenticated. This vulnerability can be exploited by creating a malicious script with an arbitrary playlist ID belonging to another user. When the user submits the request, their playlist will be deleted. Any User with active sessions who are tricked into submitting a malicious request are impacted, as their playlists or other objects could be deleted without their consent.	5.3	More Details
CVE-2024-49214	QUIC in HAProxy 3.1.x before 3.1-dev7, 3.0.x before 3.0.5, and 2.9.x before 2.9.11 allows opening a 0-RTT session with a spoofed IP address. This can bypass the IP allow/block list functionality.	5.3	More Details
CVE-2024-9966	Inappropriate implementation in Navigations in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	5.3	More Details
CVE-2024-47166	Gradio is an open-source Python package designed for quick prototyping. This vulnerability involves a **one-level read path traversal** in the `/custom_component` endpoint. Attackers can exploit this flaw to access and leak source code from custom Gradio components by manipulating the file path in the request. Although the traversal is limited to a single directory level, it could expose proprietary or sensitive code that developers intended to keep private. This impacts users who have developed custom Gradio components and are hosting them on publicly accessible servers. Users are advised to upgrade to `gradio>=4.44` to address this issue. As a workaround, developers can sanitize the file paths and ensure that components are not stored in publicly accessible directories.	5.3	More Details
CVE-2024-21258	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: User Interface). Supported versions that are affected are 12.2.3-12.2.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Installed Base. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Installed Base accessible data. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21238	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.39 and prior, 8.4.1 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.3	More Details
CVE-2024-9823	There exists a security vulnerability in Jetty's DosFilter which can be exploited by unauthorized users to cause remote denial-of-service (DoS) attack on the server using DosFilter. By repeatedly sending crafted requests, attackers can trigger OutofMemory errors and exhaust the server's memory finally.	5.3	More Details
CVE-2024-21248	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22 and prior to 7.1.2. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle VM VirtualBox accessible data as well as unauthorized read access to a subset of Oracle VM VirtualBox accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:L).	5.3	More Details
CVE-2024-9787	A vulnerability, which was classified as problematic, was found in Contemporary Control System BASrouter BACnet BASRT-B 2.7.2. This affects an unknown part of the component UDP Packet Handler. The manipulation leads to denial of service. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2024-6157	An attacker who successfully exploited these vulnerabilities could cause the robot to stop. A vulnerability exists in the PROFINET stack included in the RobotWare versions listed below. This vulnerability arises under specific condition when specially crafted message is processed by the system. Below are reported vulnerabilities in the Robot Ware versions. * IRC5- RobotWare 6 < 6.15.06 except 6.10.10, and 6.13.07	5.1	More Details
CVE-2024-44337	The package `github.com/gomarkdown/markdown` is a Go library for parsing Markdown text and rendering as HTML. Prior to pseudoversion `v0.0.0-20240729232818-a2a9c4f`, which corresponds with commit `a2a9c4f76ef5a5c32108e36f7c47f8d310322252`, there was a logical problem in the paragraph function of the parser/block.go file, which allowed a remote attacker to cause a denial of service (DoS) condition by providing a tailor-made input that caused an infinite loop, causing the program to hang and consume resources indefinitely. Submit `a2a9c4f76ef5a5c32108e36f7c47f8d310322252` contains fixes to this problem.	5.1	More Details
CVE-2024-42934	OpenIPMI before 2.0.36 has an out-of-bounds array access (for authentication type) in the ipmi_sim simulator, resulting in denial of service or (with very low probability) authentication bypass or code execution.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39544	An Incorrect Default Permissions vulnerability in the command line interface (CLI) of Juniper Networks Junos OS Evolved allows a low privileged local attacker to view NETCONF traceoptions files, representing an exposure of sensitive information. On all Junos OS Evolved platforms, when NETCONF traceoptions are configured, NETCONF traceoptions files get created with an incorrect group permission, which allows a low-privileged user can access sensitive information compromising the confidentiality of the system. Junos OS Evolved: * All versions before 20.4R3-S9-EVO, * 21.2-EVO before 21.2R3-S7-EVO, * 21.4-EVO before 21.4R3-S5-EVO, * 22.1-EVO before 22.1R3-S5-EVO, * 22.2-EVO before 22.2R3-S3-EVO, * 22.3-EVO before 22.3R3-EVO, 22.3R3-S2-EVO, * 22.4-EVO before 22.4R3-EVO, * 23.2-EVO before 23.2R1-S2-EVO, 23.2R2-EVO.	5.0	More Details
CVE-2024-9923	The Team+ from TEAMPLUS TECHNOLOGY does not properly validate a specific page parameter, allowing remote attackers with administrator privileges to move arbitrary system files to the website root directory and access them.	4.9	More Details
CVE-2024-9507	The Contact Form by Bit Form: Multi Step Form, Calculation Contact Form, Payment Contact Form & Custom Contact Form builder plugin for WordPress is vulnerable to arbitrary file read in all versions up to, and including, 2.15.2 due to improper input validation within the iconUpload function. This makes it possible for authenticated attackers, with Administrator-level access and above, to leverage a PHP filter chain attack and read the contents of arbitrary files on the server, which can contain sensitive information.	4.9	More Details
CVE-2024-9623	An issue was discovered in GitLab CE/EE affecting all versions starting from 8.16 prior to 17.2.9, starting from 17.3 prior to 17.3.5, and starting from 17.4 prior to 17.4.2, which allows deploy keys to push to an archived repository.	4.9	More Details
CVE-2024-21194	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21236	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21239	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21218	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21198	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21199	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21200	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21201	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21241	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21193	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21197	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21207	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.38 and prior, 8.4.1 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-31955	An issue was discovered in Samsung eMMC with KLMAG2GE4A and KLM8G1WEMB firmware. Code bypass through Electromagnetic Fault Injection allows an attacker to successfully authenticate and write to the RPMB (Replay Protected Memory Block) area without possessing secret information.	4.9	More Details
CVE-2024-21219	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21261	Vulnerability in Oracle Application Express (component: General). Supported versions that are affected are 23.2 and 24.1. Difficult to exploit vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Application Express. While the vulnerability is in Oracle Application Express, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Application Express accessible data as well as unauthorized read access to a subset of Oracle Application Express accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:L/I:L/A:N).	4.9	More Details
CVE-2024-45738	In Splunk Enterprise versions below 9.3.1, 9.2.3, and 9.1.6, the software potentially exposes sensitive HTTP parameters to the `_internal` index. This exposure could happen if you configure the Splunk Enterprise `REST_Calls` log channel at the DEBUG logging level.	4.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45119	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 (and earlier) are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. An admin-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require user interaction.	4.9	More Details
CVE-2024-21203	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-21204	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.4.0 and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.9	More Details
CVE-2024-47766	Tuleap is a tool for end to end traceability of application and system developments. Prior to Tuleap Community Edition 15.13.99.110, Tuleap Enterprise Edition 15.13-5, and Tuleap Enterprise Edition 15.12-5, administrators of a project can access the content of trackers with permissions restrictions of project they are members of but not admin via the cross tracker search widget. Tuleap Community Edition 15.13.99.110, Tuleap Enterprise Edition 15.13-5, and Tuleap Enterprise Edition 15.12-8 fix this issue.	4.9	More Details
CVE-2024-45739	In Splunk Enterprise versions below 9.3.1, 9.2.3, and 9.1.6, the software potentially exposes plaintext passwords for local native authentication Splunk users. This exposure could happen when you configure the Splunk Enterprise AdminManager log channel at the DEBUG logging level.	4.9	More Details
CVE-2024-9953	A potential denial-of-service (DoS) vulnerability exists in CERT VINCE software versions prior to 3.0.8. An authenticated administrative user can inject an arbitrary pickle object into a user’s profile, which may lead to a DoS condition when the profile is accessed. While the Django server restricts unpickling to prevent server crashes, this vulnerability could still disrupt operations.	4.9	More Details
CVE-2024-48948	The Elliptic package 6.5.7 for Node.js, in its for ECDSA implementation, does not correctly verify valid signatures if the hash contains at least four leading 0 bytes and when the order of the elliptic curve's base point is smaller than the hash, because of an _truncateToN anomaly. This leads to valid signatures being rejected. Legitimate transactions or communications may be incorrectly flagged as invalid.	4.8	More Details
CVE-2024-45127	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 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 Number	Description	Base Score	Reference
CVE-2024-21235	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).	4.8	More Details
CVE-2024-46988	Tuleap is a tool for end to end traceability of application and system developments. Prior to Tuleap Community Edition 15.13.99.40, Tuleap Enterprise Edition 15.13-3, and Tuleap Enterprise Edition 15.12-6, users might receive email notification with information they should not have access to. Tuleap Community Edition 15.13.99.40, Tuleap Enterprise Edition 15.13-3, and Tuleap Enterprise Edition 15.12-6 fix this issue.	4.8	More Details
CVE-2024-5968	The Photo Gallery by 10Web WordPress plugin before 1.8.28 does not properly sanitise and escape some of its Gallery settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2024-46980	Tuleap is a tool for end to end traceability of application and system developments. Prior to Tuleap Community Edition 15.13.99.37, Tuleap Enterprise Edition 15.13-3, and Tuleap Enterprise Edition 15.12-6, a site administrator could create an artifact link type with a forward label allowing them to execute uncontrolled code (or at least achieve content injection) in a mail client. Tuleap Community Edition 15.13.99.37, Tuleap Enterprise Edition 15.13-3, and Tuleap Enterprise Edition 15.12-6 fix this issue.	4.8	More Details
CVE-2024-47660	In the Linux kernel, the following vulnerability has been resolved: fsnotify: clear PARENT_WATCHED flags lazily In some setups directories can have many (usually negative) dentries. Hence __fsnotify_update_child_dentry_flags() function can take a significant amount of time. Since the bulk of this function happens under inode->i_lock this causes a significant contention on the lock when we remove the watch from the directory as the __fsnotify_update_child_dentry_flags() call from fsnotify_recalc_mask() races with __fsnotify_update_child_dentry_flags() calls from __fsnotify_parent() happening on children. This can lead upto softlockup reports reported by users. Fix the problem by calling fsnotify_update_children_dentry_flags() to set PARENT_WATCHED flags only when parent starts watching children. When parent stops watching children, clear false positive PARENT_WATCHED flags lazily in __fsnotify_parent() for each accessed child.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9904	A vulnerability classified as critical was found in 07FLYCMS, 07FLY-CMS and 07FlyCRM up to 1.2.0. This vulnerability affects the function pictureUpload of the file /admin/File/pictureUpload. 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. The affected product is known with different names like 07FLYCMS, 07FLY-CMS, and 07FlyCRM. It was not possible to reach out to the vendor before assigning a CVE due to a not working mail address.	4.7	More Details
CVE-2024-9918	A vulnerability has been found in HuangDou UTCMS V9 and classified as critical. This vulnerability affects the function RunSql of the file app/modules/ut-data/admin/sql.php. The manipulation of the argument sql leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-47668	In the Linux kernel, the following vulnerability has been resolved: lib/generic-radix-tree.c: Fix rare race in __genradix_ptr_alloc() If we need to increase the tree depth, allocate a new node, and then race with another thread that increased the tree depth before us, we'll still have a preallocated node that might be used later. If we then use that node for a new non-root node, it'll still have a pointer to the old root instead of being zeroed - fix this by zeroing it in the cmpxchg failure path.	4.7	More Details
CVE-2024-9471	A privilege escalation (PE) vulnerability in the XML API of Palo Alto Networks PAN-OS software enables an authenticated PAN-OS administrator with restricted privileges to use a compromised XML API key to perform actions as a higher privileged PAN-OS administrator. For example, an administrator with "Virtual system administrator (read-only)" access could use an XML API key of a "Virtual system administrator" to perform write operations on the virtual system configuration even though they should be limited to read-only operations.	4.7	More Details
CVE-2024-9855	A vulnerability was found in 07FLYCMS, 07FLY-CMS and 07FlyCRM 1.3.8. It has been declared as critical. Affected by this vulnerability is the function uploadFile of the file /admin/SysModule/upload/ajaxmodel/upload/uploadfilepath/sysmodule_1 of the component Module Plug-In Handler. The manipulation of the argument file leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The affected product is known with different names like 07FLYCMS, 07FLY-CMS, and 07FlyCRM. It was not possible to reach out to the vendor before assigning a CVE due to a not working mail address.	4.7	More Details
CVE-2024-47353	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in QuomodoSoft ElementsReady Addons for Elementor.This issue affects ElementsReady Addons for Elementor: from n/a through 6.4.2.	4.7	More Details
CVE-2024-9977	A vulnerability, which was classified as critical, was found in MitraStar GPT-2541GNAC BR_g5.6_1.11(WVK.0)b26. Affected is an unknown function of the file /cgi-bin/settings-firewall.cgi of the component Firewall Settings Page. The manipulation of the argument SrcInterface leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. We tried to contact the vendor early about the disclosure but the official mail address was not working properly.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46870	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Disable DMCUB timeout for DCN35 [Why] DMCUB can intermittently take longer than expected to process commands. Old ASIC policy was to continue while logging a diagnostic error - which works fine for ASIC without IPS, but with IPS this could lead to a race condition where we attempt to access DCN state while it's inaccessible, leading to a system hang when the NIU port is not disabled or register accesses that timeout and the display configuration in an undefined state. [How] We need to investigate why these accesses take longer than expected, but for now we should disable the timeout on DCN35 to avoid this race condition. Since the waits happen only at lower interrupt levels the risk of taking too long at higher IRQ and causing a system watchdog timeout are minimal.	4.7	More Details
CVE-2024-9789	A vulnerability was found in LyLme_spage 1.9.5 and classified as critical. This issue affects some unknown processing of the file /admin/apply.php. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-47354	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in smp7, wp.Insider Simple Membership After Login Redirection.This issue affects Simple Membership After Login Redirection: from n/a through 1.6.	4.7	More Details
CVE-2024-9903	A vulnerability classified as critical has been found in 07FLYCMS, 07FLY-CMS and 07FlyCRM up to 1.2.0. This affects the function fileUpload of the file /admin/File/fileUpload. The manipulation of the argument file leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The affected product is known with different names like 07FLYCMS, 07FLY-CMS, and 07FlyCRM. It was not possible to reach out to the vendor before assigning a CVE due to a not working mail address.	4.7	More Details
CVE-2024-46911	Cross-site Resource Forgery (CSRF), Privilege escalation vulnerability in Apache Roller. On multi-blog/user Roller websites, by default weblog owners are trusted to publish arbitrary weblog content and this combined with a deficiency in Roller's CSRF protections allowed an escalation of privileges attack. This issue affects Apache Roller before 6.1.4. Roller users who run multi-blog/user Roller websites are recommended to upgrade to version 6.1.4, which fixes the issue. Roller 6.1.4 release announcement: https://lists.apache.org/thread/3c3f6rwqptyw6wdc95654fq5vlosqdpw	4.7	More Details
CVE-2024-44731	Mirotalk before commit 9de226 was discovered to contain a DOM-based cross-site scripting (XSS) vulnerability which allows attackers to execute arbitrary code via sending crafted payloads in messages to other users over RTC connections.	4.7	More Details
CVE-2024-9790	A vulnerability was found in LyLme_spage 1.9.5. It has been classified as critical. Affected is an unknown function of the file /admin/sou.php. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-47648	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in EventPrime Events EventPrime.This issue affects EventPrime: from n/a through 4.0.4.5.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9788	A vulnerability has been found in LyLme_spage 1.9.5 and classified as critical. This vulnerability affects unknown code of the file /admin/tag.php. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2024-9816	A vulnerability was found in Codezips Tourist Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file /admin/change-image.php. The manipulation of the argument packageimage leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-9815	A vulnerability has been found in Codezips Tourist Management System 1.0 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /admin/create-package.php. The manipulation of the argument packageimage leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.7	More Details
CVE-2024-9804	A vulnerability was found in code-projects Blood Bank System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /admin/campsdetails.php. The manipulation of the argument hospital leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	4.7	More Details
CVE-2024-6985	A path traversal vulnerability exists in the api open_personality_folder endpoint of parisneo/lollms-webui. This vulnerability allows an attacker to read any folder in the personality_folder on the victim's computer, even though sanitize_path is set. The issue arises due to improper sanitization of the personality_folder parameter, which can be exploited to traverse directories and access arbitrary files.	4.4	More Details
CVE-2024-21212	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Health Monitor). Supported versions that are affected are 8.0.39 and prior and 8.4.0. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).	4.4	More Details
CVE-2024-38862	Insertion of Sensitive Information into Log File in Checkmk GmbH's Checkmk versions <2.3.0p18, <2.2.0p35, <2.1.0p48 and <=2.0.0p39 (EOL) causes SNMP and IMPI secrets of host and folder properties to be written to audit log files accessible to administrators.	4.4	More Details
CVE-2024-21192	Vulnerability in the Oracle Enterprise Manager for Fusion Middleware product of Oracle Fusion Middleware (component: WebLogic Mgmt). The supported version that is affected is 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle Enterprise Manager for Fusion Middleware executes to compromise Oracle Enterprise Manager for Fusion Middleware. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Enterprise Manager for Fusion Middleware accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7489	The Forms for Mailchimp by Optin Cat – Grow Your MailChimp List plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the form color parameters in all versions up to, and including, 2.5.6 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.	4.4	More Details
CVE-2024-9776	The ImagePress – Image Gallery plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings 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 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-2024-38815	VMware NSX contains a content spoofing vulnerability. An unauthenticated malicious actor may be able to craft a URL and redirect a victim to an attacker controlled domain leading to sensitive information disclosure.	4.3	More Details
CVE-2024-21206	Vulnerability in the Oracle Enterprise Command Center Framework product of Oracle E-Business Suite (component: Diagnostics). Supported versions that are affected are ECC:11-13. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Enterprise Command Center Framework. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Enterprise Command Center Framework accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2024-21249	Vulnerability in the PeopleSoft Enterprise FIN Expenses product of Oracle PeopleSoft (component: Expenses). The supported version that is affected is 9.2. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise PeopleSoft Enterprise FIN Expenses. Successful attacks of this vulnerability can result in unauthorized read access to a subset of PeopleSoft Enterprise FIN Expenses accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).	4.3	More Details
CVE-2024-21233	Vulnerability in the Oracle Database Core component of Oracle Database Server. Supported versions that are affected are 19.3-19.24, 21.3-21.15 and 23.4-23.5. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Oracle Database Core. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database Core accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).	4.3	More Details
CVE-2024-9778	The ImagePress – Image Gallery plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.2.2. This is due to missing or incorrect nonce validation on the 'imagepress_admin_page' function. This makes it possible for unauthenticated attackers to update plugin settings, including redirection URLs, 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 Number	Description	Base Score	Reference
CVE-2024-45129	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in Privilege escalation. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction.	4.3	More Details
CVE-2024-45737	In Splunk Enterprise versions below 9.3.1, 9.2.3, and 9.1.6 and Splunk Cloud Platform versions below 9.2.2403.108, and 9.1.2312.204, a low-privileged user that does not hold the "admin" or "power" Splunk roles could change the maintenance mode state of App Key Value Store (KVStore) through a Cross-Site Request Forgery (CSRF).	4.3	More Details
CVE-2024-47767	Tuleap is a tool for end to end traceability of application and system developments. Prior to Tuleap Community Edition 15.13.99.113, Tuleap Enterprise Edition 15.13-5, and Tuleap Enterprise Edition 15.12-5, users might see tracker names they should not have access to. Tuleap Community Edition 15.13.99.113, Tuleap Enterprise Edition 15.13-5, and Tuleap Enterprise Edition 15.12-8 fix this issue.	4.3	More Details
CVE-2024-45735	In Splunk Enterprise versions below 9.2.3 and 9.1.6, and Splunk Secure Gateway versions on Splunk Cloud Platform versions below 3.4.259, 3.6.17, and 3.7.0, a low-privileged user that does not hold the "admin" or "power" Splunk roles can see App Key Value Store (KV Store) deployment configuration and public/private keys in the Splunk Secure Gateway App.	4.3	More Details
CVE-2024-47168	Gradio is an open-source Python package designed for quick prototyping. This vulnerability involves data exposure due to the enable_monitoring flag not properly disabling monitoring when set to False. Even when monitoring is supposedly disabled, an attacker or unauthorized user can still access the monitoring dashboard by directly requesting the /monitoring endpoint. This means that sensitive application analytics may still be exposed, particularly in environments where monitoring is expected to be disabled. Users who set enable_monitoring=False to prevent unauthorized access to monitoring data are impacted. Users are advised to upgrade to gradio>=4.44 to address this issue. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2024-45130	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction.	4.3	More Details
CVE-2024-9756	The Order Attachments for WooCommerce plugin for WordPress is vulnerable to unauthorized limited arbitrary file uploads due to a missing capability check on the wcoa_add_attachment AJAX action in versions 2.0 to 2.4.1. This makes it possible for authenticated attackers, with subscriber-level access and above, to upload limited file types.	4.3	More Details
CVE-2024-45734	In Splunk Enterprise versions 9.3.0, 9.2.3, and 9.1.6, a low-privileged user that does not hold the "admin" or "power" Splunk roles could view images on the machine that runs Splunk Enterprise by using the PDF export feature in Splunk classic dashboards. The images on the machine could be exposed by exporting the dashboard as a PDF, using the local image path in the img tag in the source extensible markup language (XML) code for the Splunk classic dashboard.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9958	Inappropriate implementation in PictureInPicture in Google Chrome prior to 130.0.6723.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-9539	An information disclosure vulnerability was identified in GitHub Enterprise Server via attacker uploaded asset URL allowing the attacker to retrieve metadata information of a user who clicks on the URL and further exploit it to create a convincing phishing page. This required the attacker to upload malicious SVG files and phish a victim user to click on that uploaded asset URL. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.14 and was fixed in versions 3.14.2, 3.13.5, 3.12.10, 3.11.16. This vulnerability was reported via the GitHub Bug Bounty program.	4.3	More Details
CVE-2024-8902	The Elementor Addon Elements plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 1.13.8 via the render_column function in modules/data-table/widgets/data-table.php. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft template data.	4.3	More Details
CVE-2024-45125	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could exploit this vulnerability to have a low impact on integrity. Exploitation of this issue does not require user interaction.	4.3	More Details
CVE-2024-45122	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction.	4.3	More Details
CVE-2024-9962	Inappropriate implementation in Permissions in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-45121	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction.	4.3	More Details
CVE-2024-6757	The Elementor Website Builder – More than Just a Page Builder plugin for WordPress is vulnerable to Basic Information Exposure in all versions up to, and including, 3.23.5 via the get_image_alt function. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract either excerpt data or titles of private or password-protected posts.	4.3	More Details
CVE-2024-9824	The ImagePress – Image Gallery plugin for WordPress is vulnerable to unauthorized modification and loss of data due to a missing capability check on the 'ip_delete_post' and 'ip_update_post_title' functions in all versions up to, and including, 1.2.2. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary posts and update post titles.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9963	Insufficient data validation in Downloads in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-9187	The Read more By Adam plugin for WordPress is vulnerable to unauthorized loss of data due to a missing capability check on the deleteRm() function in all versions up to, and including, 1.1.8. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete read more buttons.	4.3	More Details
CVE-2024-9067	The Youzify – BuddyPress Community, User Profile, Social Network & Membership Plugin for WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the 'delete_attachment' function in all versions up to, and including, 1.3.0. This makes it possible for authenticated attackers, with Subscriber-level access and above, to delete arbitrary attachments.	4.3	More Details
CVE-2024-8477	The Newsletter, SMTP, Email marketing and Subscribe forms by Brevo (formely Sendinblue) plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 3.1.87. This is due to missing or incorrect nonce validation on the Init() function. This makes it possible for unauthenticated attackers to log out of a Brevo connection via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details
CVE-2024-9685	The Notification for Telegram plugin for WordPress is vulnerable to unauthorized test message sending due to a missing capability check on the 'nftb_test_action' function in versions up to, and including, 3.3.1. This makes it possible for authenticated attackers, with subscriber-level access and above, to send a test message via the Telegram Bot API to all users configured in the settings.	4.3	More Details
CVE-2024-5005	An issue has been discovered discovered in GitLab EE/CE affecting all versions starting from 11.4 before 17.2.9, all versions starting from 17.3 before 17.3.5, all versions starting from 17.4 before 17.4.2 It was possible for guest users to disclose project templates using the API.	4.3	More Details
CVE-2024-8913	The The Plus Addons for Elementor – Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 5.6.11 via the render function in modules/widgets/tp_accordion.php. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft template data.	4.3	More Details
CVE-2024-49382	Excessive attack surface in archive-server service due to binding to an unrestricted IP address. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 38690.	4.3	More Details
CVE-2024-49383	Excessive attack surface in acep-importer service due to binding to an unrestricted IP address. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 38690.	4.3	More Details
CVE-2024-49384	Excessive attack surface in acep-collector service due to binding to an unrestricted IP address. The following products are affected: Acronis Cyber Protect 16 (Linux, Windows) before build 38690.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9538	The ShopLentor plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 2.9.8 via the 'render' function in includes/addons/wl_faq.php. This makes it possible for authenticated attackers, with Contributor-level access and above, to extract sensitive private, pending, and draft Elementor template data.	4.3	More Details
CVE-2024-9964	Inappropriate implementation in Payments in Google Chrome prior to 130.0.6723.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Low)	4.3	More Details
CVE-2024-46528	An Insecure Direct Object Reference (IDOR) vulnerability in KubeSphere 4.x before 4.1.3 and 3.x through 3.4.1 and KubeSphere Enterprise 4.x before 4.1.3 and 3.x through 3.5.0 allows low-privileged authenticated attackers to access sensitive resources without proper authorization checks.	4.3	More Details
CVE-2024-21213	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:N/I:N/A:H).	4.2	More Details
CVE-2024-21247	Vulnerability in the MySQL Client product of Oracle MySQL (component: Client: mysqldump). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Client accessible data as well as unauthorized read access to a subset of MySQL Client accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N).	3.8	More Details
CVE-2024-9596	An issue has been discovered in GitLab EE affecting all versions starting from 16.6 prior to 17.2.9, from 17.3 prior to 17.3.5, and from 17.4 prior to 17.4.2. It was possible for an unauthenticated attacker to determine the GitLab version number for a GitLab instance.	3.7	More Details
CVE-2024-21217	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21211	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Compiler). Supported versions that are affected are Oracle Java SE: 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details
CVE-2024-6763	Eclipse Jetty is a lightweight, highly scalable, Java-based web server and Servlet engine . It includes a utility class, HttpURI, for URI/URL parsing. The HttpURI class does insufficient validation on the authority segment of a URI. However the behaviour of HttpURI differs from the common browsers in how it handles a URI that would be considered invalid if fully validated against the RRC. Specifically HttpURI and the browser may differ on the value of the host extracted from an invalid URI and thus a combination of Jetty and a vulnerable browser may be vulnerable to a open redirect attack or to a SSRF attack if the URI is used after passing validation checks.	3.7	More Details
CVE-2024-21210	Vulnerability in Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4 and 23. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE accessible data. Note: This vulnerability can be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. This vulnerability also applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21208	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Oracle Java SE: 8u421, 8u421-perf, 11.0.24, 17.0.12, 21.0.4, 23; Oracle GraalVM for JDK: 17.0.12, 21.0.4, 23; Oracle GraalVM Enterprise Edition: 20.3.15 and 21.3.11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).	3.7	More Details
CVE-2023-36325	i2p before 2.3.0 (Java) allows de-anonymizing the public IPv4 and IPv6 addresses of i2p hidden services (aka eepsites) via a correlation attack across the IPv4 and IPv6 addresses that occurs when a tunneled, replayed message has a behavior discrepancy (it may be dropped, or may result in a Wrong Destination response). An attack would take days to complete.	3.7	More Details
CVE-2024-45403	h2o is an HTTP server with support for HTTP/1.x, HTTP/2 and HTTP/3. When h2o is configured as a reverse proxy and HTTP/3 requests are cancelled by the client, h2o might crash due to an assertion failure. The crash can be exploited by an attacker to mount a Denial-of-Service attack. By default, the h2o standalone server automatically restarts, minimizing the impact. However, HTTP requests that were served concurrently will still be disrupted. The vulnerability has been addressed in commit 1ed32b2. Users may disable the use of HTTP/3 to mitigate the issue.	3.7	More Details
CVE-2024-47869	Gradio is an open-source Python package designed for quick prototyping. This vulnerability involves a **timing attack** in the way Gradio compares hashes for the `analytics_dashboard` function. Since the comparison is not done in constant time, an attacker could exploit this by measuring the response time of different requests to infer the correct hash byte-by-byte. This can lead to unauthorized access to the analytics dashboard, especially if the attacker can repeatedly query the system with different keys. Users are advised to upgrade to `gradio>4.44` to mitigate this issue. To mitigate the risk before applying the patch, developers can manually patch the `analytics_dashboard` dashboard to use a **constant-time comparison** function for comparing sensitive values, such as hashes. Alternatively, access to the analytics dashboard can be disabled.	3.7	More Details
CVE-2024-9907	A vulnerability classified as problematic was found in QileCMS up to 1.1.3. This vulnerability affects the function sendEmail of the file /qilecms/user/controller/Forget.php of the component Verification Code Handler. The manipulation leads to weak password recovery. The attack can be initiated 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 vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2024-9506	Improper regular expression in Vue's parseHTML function leads to a potential regular expression denial of service vulnerability.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9906	A vulnerability, which was classified as problematic, was found in SourceCodester Online Eyewear Shop 1.0. Affected is an unknown function of the file /admin/?page=inventory/view_inventory&id=2. The manipulation of the argument Code leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-9799	A vulnerability has been found in SourceCodester Profile Registration without Reload Refresh 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file add.php. The manipulation of the argument email_address/address/company_name/job_title/jobDescriptionparameter leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-47826	eLabFTW is an open source electronic lab notebook for research labs. A vulnerability in versions prior to 5.1.5 allows an attacker to inject arbitrary HTML tags in the pages: "experiments.php" (show mode), "database.php" (show mode) or "search.php". It works by providing HTML code in the extended search string, which will then be displayed back to the user in the error message. This means that injected HTML will appear in a red "alert/danger" box, and be part of an error message. Due to some other security measures, it is not possible to execute arbitrary javascript from this attack. As such, this attack is deemed low impact. Users should upgrade to at least version 5.1.5 to receive a patch. No known workarounds are available.	3.5	More Details
CVE-2024-9806	A vulnerability has been found in Craig Rodway Classroombookings up to 2.8.6 and classified as problematic. This vulnerability affects unknown code of the file /rooms/fields of the component Room Page. The manipulation of the argument Name leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2.8.7 is able to address this issue. It is recommended to upgrade the affected component. The project maintainer was contacted early about the disclosure. He responded very quickly, friendly, and professional.	3.5	More Details
CVE-2024-9803	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been classified as problematic. This affects an unknown part of the file blooddetails.php. The manipulation of the argument Availibility 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. Other parameters might be affected as well.	3.5	More Details
CVE-2024-9810	A vulnerability was found in SourceCodester Record Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file sort2_user.php. The manipulation of the argument qualification leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-9805	A vulnerability was found in code-projects Blood Bank System 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /admin/campsdetails.php. The manipulation of the argument hospital/address/city/contact leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "hospital".	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-30118	HCL Connections is vulnerable to an information disclosure vulnerability which could allow a user to obtain sensitive information they are not entitled to because of improperly handling the request data.	3.5	More Details
CVE-2024-21242	Vulnerability in the XML Database component of Oracle Database Server. Supported versions that are affected are 19.3-19.24, 21.3-21.15 and 23.4-23.5. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via HTTP to compromise XML Database. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of XML Database. CVSS 3.1 Base Score 3.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:L).	3.5	More Details
CVE-2024-21251	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.24, 21.3-21.15 and 23.4-23.5. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java VM accessible data. CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).	3.1	More Details
CVE-2024-45120	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could lead to a security feature bypass. An attacker could exploit this vulnerability to alter a condition between the check and the use of a resource, having a low impact on integrity. Exploitation of this issue requires user interaction.	3.1	More Details
CVE-2024-25622	h2o is an HTTP server with support for HTTP/1.x, HTTP/2 and HTTP/3. The configuration directives provided by the headers handler allows users to modify the response headers being sent by h2o. The configuration file of h2o has scopes, and the inner scopes (e.g., path level) are expected to inherit the configuration defined in outer scopes (e.g., global level). However, if a header directive is used in the inner scope, all the definition in outer scopes are ignored. This can lead to headers not being modified as expected. Depending on the headers being added or removed unexpectedly, this behavior could lead to unexpected client behavior. This vulnerability is fixed in commit 123f5e2b65dcdba8f7ef659a00d24bd1249141be.	3.1	More Details
CVE-2024-6762	Jetty PushSessionCacheFilter can be exploited by unauthenticated users to launch remote DoS attacks by exhausting the server’s memory.	3.1	More Details
CVE-2024-21231	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client programs). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L).	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21257	Vulnerability in the Oracle Hyperion BI+ product of Oracle Hyperion (component: UI and Visualization). The supported version that is affected is 11.2.18.0.000. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the Oracle Hyperion BI+ executes to compromise Oracle Hyperion BI+. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Hyperion BI+ accessible data. CVSS 3.1 Base Score 3.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N).	3.0	More Details
CVE-2024-47813	Wasmtime is an open source runtime for WebAssembly. Under certain concurrent event orderings, a `wasmtime::Engine`'s internal type registry was susceptible to double-unregistration bugs due to a race condition, leading to panics and potentially type registry corruption. That registry corruption could, following an additional and particular sequence of concurrent events, lead to violations of WebAssembly's control-flow integrity (CFI) and type safety. Users that do not use `wasmtime::Engine` across multiple threads are not affected. Users that only create new modules across threads over time are additionally not affected. Reproducing this bug requires creating and dropping multiple type instances (such as `wasmtime::FuncType` or `wasmtime::ArrayType`) concurrently on multiple threads, where all types are associated with the same `wasmtime::Engine`. **Wasm guests cannot trigger this bug.** See the "References" section below for a list of Wasmtime types-related APIs that are affected. Wasmtime maintains an internal registry of types within a `wasmtime::Engine` and an engine is shareable across threads. Types can be created and referenced through creation of a `wasmtime::Module`, creation of `wasmtime::FuncType`, or a number of other APIs where the host creates a function (see "References" below). Each of these cases interacts with an engine to deduplicate type information and manage type indices that are used to implement type checks in WebAssembly's `call_indirect` function, for example. This bug is a race condition in this management where the internal type registry could be corrupted to trigger an assert or contain invalid state. Wasmtime's internal representation of a type has individual types (e.g. one-per-host-function) maintain a registration count of how many time it's been used. Types additionally have state within an engine behind a read-write lock such as lookup/deduplication information. The race here is a time-of-check versus time-of-use (TOCTOU) bug where one thread atomically decrements a type entry's registration count, observes zero registrations, and then acquires a lock in order to unregister that entry. However, between when this first thread observed the zero-registration count and when it acquires that lock, another thread could perform the following sequence of events: re-register another copy of the type, which deduplicates to that same entry, resurrecting it and incrementing its registration count; then drop the type and decrement its registration count; observe that the registration count is now zero; acquire the type registry lock; and finally unregister the type. Now, when the original thread finally acquires the lock and unregisters the entry, it is the second time this entry has been unregistered. This bug was originally introduced in Wasmtime 19's development of the WebAssembly GC proposal. This bug affects users who are not using the GC proposal, however, and affects Wasmtime in its default configuration even when the GC proposal is disabled. Wasmtime users using 19.0.0 and after are all affected by this issue. We have released the following Wasmtime versions, all of which have a fix for this bug: * 21.0.2 * 22.0.1 * 23.0.3 * 24.0.1 * 25.0.2. If your application creates and drops Wasmtime types on multiple threads concurrently, there are no known workarounds. Users are encouraged to upgrade to a patched release.	2.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-39586	Dell AppSync Server, version 4.3 through 4.6, contains an XML External Entity Injection vulnerability. An adjacent high privileged attacker could potentially exploit this vulnerability, leading to information disclosure.	2.9	More Details
CVE-2024-45134	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction.	2.7	More Details
CVE-2024-45133	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Information Exposure vulnerability that could result in a security feature bypass. An admin attacker could leverage this vulnerability to have a low impact on confidentiality which may aid in further attacks. Exploitation of this issue does not require user interaction.	2.7	More Details
CVE-2024-45135	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An admin attacker could leverage this vulnerability to bypass security measures and have a low impact on integrity. Exploitation of this issue does not require user interaction.	2.7	More Details
CVE-2024-45149	Adobe Commerce versions 2.4.7-p2, 2.4.6-p7, 2.4.5-p9, 2.4.4-p10 and earlier are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. A high-privileged attacker could leverage this vulnerability to bypass security measures and have a low impact on confidentiality. Exploitation of this issue does not require user interaction.	2.7	More Details
CVE-2024-7038	An information disclosure vulnerability exists in open-webui version 0.3.8. The vulnerability is related to the embedding model update feature under admin settings. When a user updates the model path, the system checks if the file exists and provides different error messages based on the existence and configuration of the file. This behavior allows an attacker to enumerate file names and traverse directories by observing the error messages, leading to potential exposure of sensitive information.	2.7	More Details
CVE-2024-30117	A dynamic search for a prerequisite library could allow the possibility for an attacker to replace the correct file under some circumstances.	2.5	More Details
CVE-2024-9952	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/?page=system_info/contact_info of the component Contact Information Page. The manipulation of the argument Address leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	2.4	More Details
CVE-2024-9807	A vulnerability was found in Craig Rodway Classroombookings 2.8.7 and classified as problematic. This issue affects some unknown processing of the file /sessions of the component Session Page. The manipulation of the argument Name leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 2.8.8 is able to address this issue. It is recommended to upgrade the affected component. The project maintainer was contacted early about the disclosure. He responded very quickly, friendly, and professional.	2.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9792	A vulnerability classified as problematic has been found in D-Link DSL-2750U R5B017. This affects an unknown part of the component Port Forwarding Page. The manipulation of the argument PortMappingDescription leads to cross site scripting. It is possible to initiate the attack remotely.	2.4	More Details
CVE-2024-9856	A vulnerability was found in 07FLYCMS, 07FLY-CMS and 07FlyCRM 1.3.8. It has been rated as problematic. Affected by this issue is some unknown functionality of the component System Settings Page. The manipulation of the argument Login Interface Copyright leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The affected product is known with different names like 07FLYCMS, 07FLY-CMS, and 07FlyCRM. It was not possible to reach out to the vendor before assigning a CVE due to a not working mail address.	2.4	More Details
CVE-2024-21253	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.22. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 2.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.3	More Details
CVE-2024-21244	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Telemetry). Supported versions that are affected are 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N).	2.2	More Details
CVE-2024-21237	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication GCS). Supported versions that are affected are 8.0.39 and prior, 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.2	More Details
CVE-2024-21232	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).	2.2	More Details
CVE-2024-21243	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Telemetry). Supported versions that are affected are 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N).	2.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-21209	Vulnerability in the MySQL Client product of Oracle MySQL (component: Client: mysqldump). Supported versions that are affected are 8.4.2 and prior and 9.0.1 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Client accessible data. CVSS 3.1 Base Score 2.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N).	2.0	More Details
CVE-2024-48909	SpiceDB is an open source database for scalably storing and querying fine-grained authorization data. Starting in version 1.35.0 and prior to version 1.37.1, clients that have enabled `LookupResources2` and have caveats in the evaluation path for their requests can return a permissionship of `CONDITIONAL` with context marked as missing, even then the context was supplied. LookupResources2 is the new default in SpiceDB 1.37.0 and has been opt-in since SpiceDB 1.35.0. The bug is patched as part of SpiceDB 1.37.1. As a workaround, disable LookupResources2 via the `--enable-experimental-lookup-resources` flag by setting it to `false`.	2.0	More Details
CVE-2024-44711	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-2024-25283	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-25285	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-4658	SQL Injection: Hibernate vulnerability in TE Informatics Nova CMS allows SQL Injection.This issue affects Nova CMS: before 5.0.	N/A	More Details
CVE-2024-25282	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-48261	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-48251. Reason: This candidate is a reservation duplicate of CVE-2024-48251. Notes: All CVE users should reference CVE-2024-48251 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-40616	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 Number	Description	Base Score	Reference
CVE-2024-8602	When the XML is read from the codes in the PDF and parsed using a DocumentBuilder, the default settings of the DocumentBuilder allow for an XXE (XML External Entity) attack. Further information on this can be found on the website of the Open Worldwide Application Security Project (OWASP). An attacker could theoretically leverage this by delivering a manipulated PDF file to the target, and depending on the environment, various actions can be executed. These actions include: * Reading files from the operating system * Crashing the thread handling the parsing or causing it to enter an infinite loop * Executing HTTP requests * Loading additional DTDs or XML files * Under certain conditions, executing OS commands	N/A	More Details
CVE-2023-25581	pac4j is a security framework for Java. `pac4j-core` prior to version 4.0.0 is affected by a Java deserialization vulnerability. The vulnerability affects systems that store externally controlled values in attributes of the `UserProfile` class from pac4j-core. It can be exploited by providing an attribute that contains a serialized Java object with a special prefix `{#sb64}` and Base64 encoding. This issue may lead to Remote Code Execution (RCE) in the worst case. Although a `RestrictedObjectInputStream` is in place, that puts some restriction on what classes can be deserialized, it still allows a broad range of java packages and potentially exploitable with different gadget chains. pac4j versions 4.0.0 and greater are not affected by this issue. Users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2024-7099	netease-youdao/qanything version 1.4.1 contains a vulnerability where unsafe data obtained from user input is concatenated in SQL queries, leading to SQL injection. The affected functions include `get_knowledge_base_name`, `from_status_to_status`, `delete_files`, and `get_file_by_status`. An attacker can exploit this vulnerability to execute arbitrary SQL queries, potentially stealing information from the database. The issue is fixed in version 1.4.2.	N/A	More Details
CVE-2024-25286	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-25284	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-9286	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'), Improper Input Validation vulnerability in TRtek Software Distant Education Platform allows SQL Injection, Parameter Injection.This issue affects Distant Education Platform: before 3.2024.11.	N/A	More Details
CVE-2024-36051	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2024-38365. Reason: This record is a duplicate of CVE-2024-38365. Notes: All CVE users should reference CVE-2024-38365 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-45817	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-9823. Reason: This candidate is a reservation duplicate of CVE-2024-9823. Notes: All CVE users should reference CVE-2024-9823 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9470	A vulnerability in Cortex XSOAR allows the disclosure of incident data to users who do not have the privilege to view the data.	N/A	More Details
CVE-2024-47832	ssoready is a single sign on provider implemented via docker. Affected versions are vulnerable to XML signature bypass attacks. An attacker can carry out signature bypass if you have access to certain IDP-signed messages. The underlying mechanism exploits differential behavior between XML parsers. Users of https://ssoready.com, the public hosted instance of SSOReady, are unaffected. We advise folks who self-host SSOReady to upgrade to 7f92a06 or later. Do so by updating your SSOReady Docker images from sha-... to sha-7f92a06. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2024-9468	A memory corruption vulnerability in Palo Alto Networks PAN-OS software allows an unauthenticated attacker to crash PAN-OS due to a crafted packet through the data plane, resulting in a denial of service (DoS) condition. Repeated attempts to trigger this condition will result in PAN-OS entering maintenance mode.	N/A	More Details
CVE-2024-9869	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2024-42988	Lack of access control in ChallengeSolves (/api/v1/challenges/<challenge id>/solves) of CTFd v2.0.0 - v3.7.2 allows authenticated users to retrieve a list of users who have solved the challenge, regardless of the Account Visibility settings. The issue is fixed in v3.7.3+.	N/A	More Details
CVE-2024-7037	In version v0.3.8 of open-webui/open-webui, the endpoint /api/pipelines/upload is vulnerable to arbitrary file write and delete due to unsanitized file.filename concatenation with CACHE_DIR. This vulnerability allows attackers to overwrite and delete system files, potentially leading to remote code execution.	N/A	More Details
CVE-2024-7041	An Insecure Direct Object Reference (IDOR) vulnerability exists in open-webui/open-webui version v0.3.8. The vulnerability occurs in the API endpoint `http://0.0.0.0:3000/api/v1/memories/{id}/update`, where the decentralization design is flawed, allowing attackers to edit other users' memories without proper authorization.	N/A	More Details
CVE-2024-48915	Agent Dart is an agent library built for Internet Computer for Dart and Flutter apps. Prior to version 1.0.0-dev.29, certificate verification in `lib/agent/certificate.dart` does not occur properly. During the delegation verification in the `_checkDelegation` function, the canister_ranges aren't verified. The impact of not checking the canister_ranges is that a subnet can sign canister responses in behalf of another subnet. The certificate's timestamp, i.e /time path, is also not verified, meaning that the certificate effectively has no expiration time. Version 1.0.0-dev.29 implements appropriate certificate verification.	N/A	More Details
CVE-2024-7048	In version v0.3.8 of open-webui, an improper privilege management vulnerability exists in the API endpoints GET /api/v1/documents/ and POST /rag/api/v1/doc. This vulnerability allows a lower-privileged user to access and overwrite files managed by a higher-privileged admin. By exploiting this vulnerability, an attacker can view metadata of files uploaded by an admin and overwrite these files, compromising the integrity and availability of the RAG models.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47876	Sakai is a Collaboration and Learning Environment. Starting in version 23.0 and prior to version 23.2, kernel users created with type roleview can log in as a normal user. This can result in illegal access being granted to the system. Version 23.3 fixes this vulnerability.	N/A	More Details
CVE-2024-47874	Starlette is an Asynchronous Server Gateway Interface (ASGI) framework/toolkit. Prior to version 0.40.0, Starlette treats `multipart/form-data` parts without a `filename` as text form fields and buffers those in byte strings with no size limit. This allows an attacker to upload arbitrary large form fields and cause Starlette to both slow down significantly due to excessive memory allocations and copy operations, and also consume more and more memory until the server starts swapping and grinds to a halt, or the OS terminates the server process with an OOM error. Uploading multiple such requests in parallel may be enough to render a service practically unusable, even if reasonable request size limits are enforced by a reverse proxy in front of Starlette. This Denial of service (DoS) vulnerability affects all applications built with Starlette (or FastAPI) accepting form requests. Verison 0.40.0 fixes this issue.	N/A	More Details
CVE-2024-47824	matrix-react-sdk is react-based software development kit for inserting a Matrix chat/VOIP client into a web page. Starting in version 3.18.0 and before 3.102.0, matrix-react-sdk allows a malicious homeserver to potentially steal message keys for a room when a user invites another user to that room, via injection of a malicious device controlled by the homeserver. This is possible because matrix-react-sdk before 3.102.0 shared historical message keys on invite. Version 3.102.0 fixes this issue by disabling sharing message keys on invite by removing calls to the vulnerable functionality. No known workarounds are available.	N/A	More Details
CVE-2024-47779	Element is a Matrix web client built using the Matrix React SDK. Element Web versions 1.11.70 through 1.11.80 contain a vulnerability which can, under specially crafted conditions, lead to the access token becoming exposed to third parties. At least one vector has been identified internally, involving malicious widgets, but other vectors may exist. Note that despite superficial similarity to CVE-2024-47771, this is an entirely separate vulnerability, caused by a separate piece of code included only in Element Web. Element Web and Element Desktop share most but not all, of their code and this vulnerability exists in the part of the code base which is not shared between the projects. Users are strongly advised to upgrade to version 1.11.81 to remediate the issue. As a workaround, avoid granting permissions to untrusted widgets.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47080	matrix-js-sdk is the Matrix Client-Server SDK for JavaScript and TypeScript. In matrix-js-sdk versions versions 9.11.0 through 34.7.0, the method `MatrixClient.sendSharedHistoryKeys` is vulnerable to interception by malicious homeservers. The method was introduced by MSC3061) and is commonly used to share historical message keys with newly invited users, granting them access to past messages in the room. However, it unconditionally sends these "shared" keys to all of the invited user's devices, regardless of whether the user's cryptographic identity is verified or whether the user's devices are signed by that identity. This allows the attacker to potentially inject its own devices to receive sensitive historical keys without proper security checks. Note that this only affects clients running the SDK with the legacy crypto stack. Clients using the new Rust cryptography stack (i.e. those that call `MatrixClient.initRustCrypto()` instead of `MatrixClient.initCrypto()`) are unaffected by this vulnerability, because `MatrixClient.sendSharedHistoryKeys()` raises an exception in such environments. The vulnerability was fixed in matrix-js-sdk 34.8.0 by removing the vulnerable functionality. As a workaround, remove use of affected functionality from clients.	N/A	More Details
CVE-2024-8912	An HTTP Request Smuggling vulnerability in Looker allowed an unauthorized attacker to capture HTTP responses destined for legitimate users. There are two Looker versions that are hosted by Looker: * Looker (Google Cloud core) was found to be vulnerable. This issue has already been mitigated and our investigation has found no signs of exploitation. * Looker (original) was not vulnerable to this issue. Customer-hosted Looker instances were found to be vulnerable and must be upgraded. This vulnerability has been patched in all supported versions of customer-hosted Looker, which are available on the Looker download page https://download.looker.com/ . For Looker customer-hosted instances, please update to the latest supported version of Looker as soon as possible. The versions below have all been updated to protect from this vulnerability. You can download these versions at the Looker download page: * 23.12 -> 23.12.123+ * 23.18 -> 23.18.117+ * 24.0 -> 24.0.92+ * 24.6 -> 24.6.77+ * 24.8 -> 24.8.66+ * 24.10 -> 24.10.78+ * 24.12 -> 24.12.56+ * 24.14 -> 24.14.37+	N/A	More Details
CVE-2024-47884	foxmarks is a CLI read-only interface for Firefox's bookmarks and history. A temporary file was created under the /tmp directory with read permissions for all users containing a copy of Firefox's database of bookmarks, history, input history, visits counter, use counter, view counter and more confidential information about the history of using Firefox. Permissions default to 0o600 for NamedTempFile. However, after copying the database, its permissions were copied with it resulting in an insecure file with 0x644 permissions. A malicious user is able to read the database when the targeted user executes foxmarks bookmarks or foxmarks history. This vulnerability is patched in v2.1.0.	N/A	More Details
CVE-2024-6971	A path traversal vulnerability exists in the parisneo/lollms-webui repository, specifically in the `lollms_file_system.py` file. The functions `add_rag_database`, `toggle_mount_rag_database`, and `vectorize_folder` do not implement security measures such as `sanitize_path_from_endpoint` or `sanitize_path`. This allows an attacker to perform vectorize operations on `.sqlite` files in any directory on the victim's computer, potentially installing multiple packages and causing a crash.	N/A	More Details
CVE-2024-45317	A Server-Side Request Forgery (SSRF) vulnerability in SMA1000 appliance firmware versions 12.4.3-02676 and earlier allows a remote, unauthenticated attacker to cause the SMA1000 server-side application to make requests to an unintended IP address.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47943	The firmware upgrade function in the admin web interface of the Rittal IoT Interface & CMC III Processing Unit devices checks if the patch files are signed before executing the containing run.sh script. The signing process is kind of an HMAC with a long string as key which is hard-coded in the firmware and is freely available for download. This allows crafting malicious "signed" .patch files in order to compromise the device and execute arbitrary code.	N/A	More Details
CVE-2024-47771	Element Desktop is a Matrix client for desktop platforms. Element Desktop versions 1.11.70 through 1.11.80 contain a vulnerability which can, under specially crafted conditions, lead to the access token becoming exposed to third parties. At least one vector has been identified internally, involving malicious widgets, but other vectors may exist. Users are strongly advised to upgrade to version 1.11.81 to remediate the issue. As a workaround, avoid granting permissions to untrusted widgets.	N/A	More Details