SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 17 April 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-2023-51409	Unrestricted Upload of File with Dangerous Type vulnerability in Jordy Meow AI Engine: ChatGPT Chatbot.This issue affects AI Engine: ChatGPT Chatbot: from n/a through 1.9.98.	10.0	More Details
CVE-2024-3400	A command injection as a result of arbitrary file creation vulnerability in the GlobalProtect feature of Palo Alto Networks PAN-OS software for specific PAN-OS versions and distinct feature configurations may enable an unauthenticated attacker to execute arbitrary code with root privileges on the firewall. Cloud NGFW, Panorama appliances, and Prisma Access are not impacted by this vulnerability.	10.0	More Details
CVE-2024-31996	XWiki Platform is a generic wiki platform. Starting in version 3.0.1 and prior to versions 4.10.19, 15.5.4, and 15.10-rc-1, the HTML escaping of escaping tool that is used in XWiki doesn't escape `{`, which, when used in certain places, allows XWiki syntax injection and thereby remote code execution. The vulnerability has been fixed in XWiki 14.10.19, 15.5.5, and 15.9 RC1. Apart from upgrading, there is no generic workaround. However, replacing `$escapetool.html` by `$escapetool.xml` in XWiki documents fixes the vulnerability. In a standard XWiki installation, the maintainers are only aware of the document `Panels.PanelLayoutUpdate` that exposes this vulnerability, patching this document is thus a workaround. Any extension could expose this vulnerability and might thus require patching, too.	10.0	More Details
CVE-2024-2912	An insecure deserialization vulnerability exists in the BentoML framework, allowing remote code execution (RCE) by sending a specially crafted POST request. By exploiting this vulnerability, attackers can execute arbitrary commands on the server hosting the BentoML application. The vulnerability is triggered when a serialized object, crafted to execute OS commands upon deserialization, is sent to any valid BentoML endpoint. This issue poses a significant security risk, enabling attackers to compromise the server and potentially gain unauthorized access or control.	10.0	More Details
CVE-2024-31982	XWiki Platform is a generic wiki platform. Starting in version 2.4-milestone-1 and prior to versions 4.10.20, 15.5.4, and 15.10-rc-1, XWiki's database search allows remote code execution through the search text. This allows remote code execution for any visitor of a public wiki or user of a closed wiki as the database search is by default accessible for all users. This impacts the confidentiality, integrity and availability of the whole XWiki installation. This vulnerability has been patched in XWiki 14.10.20, 15.5.4 and 15.10RC1. As a workaround, one may manually apply the patch to the page `Main.DatabaseSearch`. Alternatively, unless database search is explicitly used by users, this page can be deleted as this is not the default search interface of XWiki.	10.0	More Details
CVE-2024-31981	XWiki Platform is a generic wiki platform. Starting in version 3.0.1 and prior to versions 4.10.20, 15.5.4, and 15.10-rc-1, remote code execution is possible via PDF export templates. This vulnerability has been patched in XWiki 14.10.20, 15.5.4 and 15.10-rc-1. If PDF templates are not typically used on the instance, an administrator can create the document `XWiki.PDFClass` and block its edition, after making sure that it does not contain a `style` attribute. Otherwise, there are no known workarounds aside from upgrading.	9.9	More Details
CVE-2024-31997	XWiki Platform is a generic wiki platform. Prior to versions 4.10.19, 15.5.4, and 15.10-rc-1, parameters of UI extensions are always interpreted as Velocity code and executed with programming rights. Any user with edit right on any document like the user's own profile can create UI extensions. This allows remote code execution and thereby impacts the confidentiality, integrity and availability of the whole XWiki installation. This vulnerability has been patched in XWiki 14.10.19, 15.5.4 and 15.9-RC1. No known workarounds are available.	9.9	More Details
CVE-2024-31987	XWiki Platform is a generic wiki platform. Starting in version 6.4-milestone-1 and prior to versions 4.10.19, 15.5.4, and 15.10-rc-1, any user who can edit any page like their profile can create a custom skin with a template override that is executed with programming right, thus allowing remote code execution. This has been patched in XWiki 14.10.19, 15.5.4 and 15.10RC1. No known workarounds are available except for upgrading.	9.9	More Details
CVE-2024-31984	XWiki Platform is a generic wiki platform. Starting in version 7.2-rc-1 and prior to versions 4.10.20, 15.5.4, and 15.10-rc-1, by creating a document with a specially crafted title, it is possible to trigger remote code execution in the (Solr-based) search in XWiki. This allows any user who can edit the title of a space (all users by default) to execute any Groovy code in the XWiki installation which compromises the confidentiality, integrity and availability of the whole XWiki installation. This has been patched in XWiki 14.10.20, 15.5.4 and 15.10 RC1. As a workaround, manually apply the patch to the `Main.SolrSpaceFacet` page.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31983	XWiki Platform is a generic wiki platform. In multilingual wikis, translations can be edited by any user who has edit right, circumventing the rights that are normally required for authoring translations (script right for user-scope translations, wiki admin for translations on the wiki). Starting in version 4.3-milestone-2 and prior to versions 4.10.20, 15.5.4, and 15.10-rc-1, this can be exploited for remote code execution if the translation value is not properly escaped where it is used. This has been patched in XWiki 14.10.20, 15.5.4 and 15.10RC1. As a workaround, one may restrict edit rights on documents that contain translations.	9.9	More Details
CVE-2024-20997	Vulnerability in the Oracle Hospitality Simphony product of Oracle Food and Beverage Applications (component: Simphony Enterprise Server). Supported versions that are affected are 19.1.0-19.5.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Simphony. While the vulnerability is in Oracle Hospitality Simphony, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Hospitality Simphony. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2024-21010	Vulnerability in the Oracle Hospitality Simphony product of Oracle Food and Beverage Applications (component: Simphony Enterprise Server). Supported versions that are affected are 19.1.0-19.5.4. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle Hospitality Simphony. While the vulnerability is in Oracle Hospitality Simphony, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Hospitality Simphony. CVSS 3.1 Base Score 9.9 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).	9.9	More Details
CVE-2024-31465	XWiki Platform is a generic wiki platform. Starting in version 5.0-rc-1 and prior to versions 14.10.20, 15.5.4, and 15.9-rc-1, any user with edit right on any page can execute any code on the server by adding an object of type `XWiki.SearchSuggestSourceClass` to their user profile or any other page. This compromises the confidentiality, integrity and availability of the whole XWiki installation. This vulnerability has been patched in XWiki 14.10.20, 15.5.4 and 15.10 RC1. As a workaround, manually apply the patch to the document `XWiki.SearchSuggestSourceSheet`.	9.9	More Details
CVE-2024-21014	Vulnerability in the Oracle Hospitality Simphony product of Oracle Food and Beverage Applications (component: Simphony Enterprise Server). Supported versions that are affected are 19.1.0-19.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in takeover of Oracle Hospitality Simphony. 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-2024-29836	The Web interface of Evolution Controller Versions 2.04.560.31.03.2024 and below contains poorly configured access control, allowing for an unauthenticated attacker to update and add user profiles within the application, and gain full access of the site.	9.8	More Details
CVE-2024-29844	Default credentials on the Web Interface of Evolution Controller 2.x allows anyone to log in to the server directly to perform administrative functions. Upon installation or upon first login, the application does not ask the user to change the password. There is no warning or prompt to ask the user to change the default password.	9.8	More Details
CVE-2024-3777	The password reset feature of Ai3 QbiBot lacks proper access control, allowing unauthenticated remote attackers to reset any user's password.	9.8	More Details
CVE-2024-3701	The system application (com.transsion.kolun.aiservice) component does not perform an authentication check, which allows attackers to perform malicious exploitations and affect system services.	9.8	More Details
CVE-2024-23486	Plaintext storage of a password issue exists in BUFFALO wireless LAN routers, which may allow a network-adjacent unauthenticated attacker with access to the product's login page may obtain configured credentials.	9.8	More Details
CVE-2024-28556	SQL Injection vulnerability in Sourcecodester php task management system v1.0, allows remote attackers to execute arbitrary code, escalate privileges, and obtain sensitive information via crafted payload to admin-manage-user.php.	9.8	More Details
CVE-2023-48710	iTop is an IT service management platform. Files from the `env-production` folder can be retrieved even though they should have restricted access. Hopefully, there is no sensitive files stored in that folder natively, but there could be from a third-party module. The `pages/exec.php` script as been fixed to limit execution of PHP files only. Other file types won't be retrieved and exposed. The vulnerability is fixed in 2.7.10, 3.0.4, 3.1.1, and 3.2.0.	9.8	More Details
CVE-2024-3660	A arbitrary code injection vulnerability in TensorFlow's Keras framework (<2.13) allows attackers to execute arbitrary code with the same permissions as the application using a model that allow arbitrary code irrespective of the application.	9.8	More Details
CVE-2024-28056	Amazon AWS Amplify CLI before 12.10.1 incorrectly configures the role trust policy of IAM roles associated with Amplify projects. When the Authentication component is removed from an Amplify project, a Condition property is removed but "Effect":"Allow" remains present, and consequently sts:AssumeRoleWithWebIdentity would be available to threat actors with no conditions. Thus, if Amplify CLI had been used to remove the Authentication component from a project built between August 2019 and January 2024, an "assume role" may have occurred, and may have been leveraged to obtain unauthorized access to an organization's AWS resources. NOTE: the problem could only occur if an authorized AWS user removed an Authentication component. (The vulnerability did not give a threat actor the ability to remove an Authentication component.) However, in realistic situations, an authorized AWS user may have removed an Authentication component, e.g., if the objective were to stop using built-in Cognito resources, or move to a completely different identity provider.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-3871	The Delta Electronics DVW-W02W2-E2 devices expose a web administration interface to users. This interface implements multiple features that are affected by command injections and stack overflows vulnerabilities. Successful exploitation of these flaws would allow remote unauthenticated attackers to gain remote code execution with elevated privileges on the affected devices. This issue affects DVW-W02W2-E2 through version 2.5.2.	9.8	More Details
CVE-2024-3704	SQL Injection Vulnerability has been found on OpenGnsys product affecting version 1.1.1d (Espeto). This vulnerability allows an attacker to inject malicious SQL code into login page to bypass it or even retrieve all the information stored in the database.	9.8	More Details
CVE-2024-28557	SQL Injection vulnerability in Sourcecodester php task management system v1.0, allows remote attackers to execute arbitrary code, escalate privileges, and obtain sensitive information via crafted payload to update-admin.php.	9.8	More Details
CVE-2024-3765	A vulnerability classified as critical was found in Xiongmai AHB7804R-MH-V2, AHB8004T-GL, AHB8008T-GL, AHB7004T-GS-V3, AHB7004T-MHV2, AHB8032F-LME and XM530_R80X30-PQ_8M. Affected by this vulnerability is an unknown functionality of the component Sofia Service. The manipulation with the input ff00000000000000000000000000f103250000007b202252657422203a203130302c202253657373696f6e494422203a202230783022207d0a leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-260605 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	9.8	More Details
CVE-2024-21082	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: XML Services). Supported versions that are affected are 7.0.0.0.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated 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 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-2024-31819	An issue in WWBN AVideo v.12.4 through v.14.2 allows a remote attacker to execute arbitrary code via the systemRootPath parameter of the submitIndex.php component.	9.8	More Details
CVE-2024-29937	NFS in a BSD derived codebase, as used in OpenBSD through 7.4 and FreeBSD through 14.0-RELEASE, allows remote attackers to execute arbitrary code via a bug that is unrelated to memory corruption.	9.8	More Details
CVE-2024-29500	An issue in the kiosk mode of Secure Lockdown Multi Application Edition v2.00.219 allows attackers to execute arbitrary code via running a ClickOnce application instance.	9.8	More Details
CVE-2024-31818	Directory Traversal vulnerability in DerbyNet v.9.0 allows a remote attacker to execute arbitrary code via the page parameter of the kiosk.php component.	9.8	More Details
CVE-2024-3566	A command inject vulnerability allows an attacker to perform command injection on Windows applications that indirectly depend on the CreateProcess function when the specific conditions are satisfied.	9.8	More Details
CVE-2024-27683	D-Link Go-RT-AC750 GORTAC750_A1_FW_v101b03 contains a stack-based buffer overflow via the function hnap_main. An attacker can send a POST request to trigger the vulnerablilify.	9.8	More Details
CVE-2024-25912	Missing Authorization vulnerability in Skymoonlabs MoveTo.This issue affects MoveTo: from n/a through 6.2.	9.8	More Details
CVE-2024-21508	Versions of the package mysql2 before 3.9.4 are vulnerable to Remote Code Execution (RCE) via the readCodeFor function due to improper validation of the supportBigNumbers and bigNumberStrings values.	9.8	More Details
CVE-2024-31678	Sourcecodester Loan Management System v1.0 is vulnerable to SQL Injection via the "password" parameter in the "login.php" file.	9.8	More Details
CVE-2024-28718	An issue in OpenStack magnum yoga-eom version allows a remote attacker to execute arbitrary code via the cert_manager.py. component.	9.8	More Details
CVE-2024-31988	XWiki Platform is a generic wiki platform. Starting in version 13.9-rc-1 and prior to versions 4.10.19, 15.5.4, and 15.10-rc-1, when the realtime editor is installed in XWiki, it allows arbitrary remote code execution with the interaction of an admin user with programming right. More precisely, by getting an admin user to either visit a crafted URL or to view an image with this URL that could be in a comment, the attacker can get the admin to execute arbitrary XWiki syntax including scripting macros with Groovy or Python code. This compromises the confidentiality, integrity and availability of the whole XWiki installation. This vulnerability has been patched in XWiki 14.10.19, 15.5.4 and 15.9. As a workaround, one may update `RTFrontend.ConvertHTML` manually with the patch. This will, however, break some synchronization processes in the realtime editor, so upgrading should be the preferred way on installations where this editor is used.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31214	Traccar is an open source GPS tracking system. Traccar versions 5.1 through 5.12 allow arbitrary files to be uploaded through the device image upload API. Attackers have full control over the file contents, full control over the directory where the file is stored, full control over the file extension, and partial control over the file name. While it's not for an attacker to overwrite an existing file, an attacker can create new files with certain names and attacker-controlled extensions anywhere on the file system. This can potentially lead to remote code execution, XSS, DOS, etc. The default install of Traccar makes this vulnerability more severe. Self-registration is enabled by default, allowing anyone to create an account to exploit this vulnerability. Traccar also runs by default with root/system privileges, allowing files to be placed anywhere on the file system. Version 6.0 contains a fix for the issue. One may also turn off self-registration by default, as that would make most vulnerabilities in the application much harder to exploit by default and reduce the severity considerably.	9.6	More Details
CVE-2024-28878	IO-1020 Micro ELD downloads source code or an executable from an adjacent location and executes the code without sufficiently verifying the origin or integrity of the code.	9.6	More Details
CVE-2024-31650	A cross-site scripting (XSS) in Cosmetics and Beauty Product Online Store v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Last Name parameter.	9.6	More Details
CVE-2024-3157	Out of bounds memory access in Compositing in Google Chrome prior to 123.0.6312.122 allowed a remote attacker who had compromised the GPU process to potentially perform a sandbox escape via specific UI gestures. (Chromium security severity: High)	9.6	More Details
CVE-2024-32128	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Realtyna Realtyna Organic IDX plugin.This issue affects Realtyna Organic IDX plugin: from n/a through 4.14.4.	9.3	More Details
CVE-2024-32025	Kohya_ss is a GUI for Kohya's Stable Diffusion trainers. Kohya_ss is vulnerable to a command injection in `group_images_gui.py`. This vulnerability is fixed in 23.1.5.	9.1	More Details
CVE-2024-32027	Kohya_ss is a GUI for Kohya's Stable Diffusion trainers. Kohya_ss v22.6.1 is vulnerable to command injection in `finetune_gui.py` This vulnerability is fixed in 23.1.5.	9.1	More Details
CVE-2024-32026	Kohya_ss is a GUI for Kohya's Stable Diffusion trainers. Kohya_ss is vulnerable to a command injection in `git_caption_gui.py`. This vulnerability is fixed in 23.1.5.	9.1	More Details
CVE-2024-24486	An issue discovered in silex technology DS-600 Firmware v.1.4.1 allows a remote attacker to edit device settings via the SAVE EEP_DATA command.	9.1	More Details
CVE-2024-32022	Kohya_ss is a GUI for Kohya's Stable Diffusion trainers. Kohya_ss is vulnerable to command injection in basic_caption_gui.py. This vulnerability is fixed in 23.1.5.	9.1	More Details
CVE-2024-31461	Plane, an open-source project management tool, has a Server-Side Request Forgery (SSRF) vulnerability in versions prior to 0.17-dev. This issue may allow an attacker to send arbitrary requests from the server hosting the application, potentially leading to unauthorized access to internal systems. The impact of this vulnerability includes, but is not limited to, unauthorized access to internal services accessible from the server, potential leakage of sensitive information from internal services, manipulation of internal systems by interacting with internal APIs. Version 0.17-dev contains a patch for this issue. Those who are unable to update immediately may mitigate the issue by restricting outgoing network connections from servers hosting the application to essential services only and/or implementing strict input validation on URLs or parameters that are used to generate server-side requests.	9.1	More Details
CVE-2024-21071	Vulnerability in the Oracle Workflow product of Oracle E-Business Suite (component: Admin Screens and Grants UI). Supported versions that are affected are 12.2.3-12.2.13. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle Workflow. While the vulnerability is in Oracle Workflow, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Workflow. CVSS 3.1 Base Score 9.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).	9.1	More Details
CVE-2024-3781	Command injection vulnerability in the operating system. Improper neutralisation of special elements in Active Directory integration allows the intended command to be modified when sent to a downstream component in WBSAirback 21.02.04.	9.1	More Details
CVE-2024-23080	Joda Time v2.12.5 was discovered to contain a NullPointerException via the component org.joda.time.format.PeriodFormat::wordBased(Locale). NOTE: this is disputed by multiple third parties who believe there was not reasonable evidence to determine the existence of a vulnerability. The submission may have been based on a tool that is not sufficiently robust for vulnerability identification.	9.1	More Details
CVE-2024-20758	Adobe Commerce versions 2.4.6-p4, 2.4.5-p6, 2.4.4-p7, 2.4.7-beta3 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction, but the attack complexity is high.	9.0	More Details
CVE-2024-3120	A stack-buffer overflow vulnerability exists in all versions of sngrep since v1.4.1. The flaw is due to inadequate bounds checking when copying 'Content-Length' and 'Warning' headers into fixed-size buffers in the sip_validate_packet and sip_parse_extra_headers functions within src/sip.c. This vulnerability allows remote attackers to execute arbitrary code or cause a denial of service (DoS) via crafted SIP messages.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31986	XWiki Platform is a generic wiki platform. Starting in version 3.1 and prior to versions 4.10.19, 15.5.4, and 15.10-rc-1, by creating a document with a special crafted documented reference and an `XWiki.SchedulerJobClass` XObject, it is possible to execute arbitrary code on the server whenever an admin visits the scheduler page or the scheduler page is referenced, e.g., via an image in a comment on a page in the wiki. The vulnerability has been fixed in XWiki 14.10.19, 15.5.5, and 15.9. As a workaround, apply the patch manually by modifying the `Scheduler.WebHome` page.	9.0	More Details
CVE-2024-3119	A buffer overflow vulnerability exists in all versions of sngrep since v0.4.2, due to improper handling of 'Call-ID' and 'X-Call-ID' SIP headers. The functions sip_get_callid and sip_get_xcallid in sip.c use the strncpy function to copy header contents into fixed-size buffers without checking the data length. This flaw allows remote attackers to execute arbitrary code or cause a denial of service (DoS) through specially crafted SIP messages.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2024-25572	Cross-site request forgery (CSRF) vulnerability exists in Ninja Forms prior to 3.4.31. If a website administrator views a malicious page while logging in, unintended oper
CVE-2024-32254	Phpgurukul Tourism Management System v2.0 is vulnerable to Unrestricted Upload of File with Dangerous Type via tms/admin/create-package.php. When creating a r the image.
CVE-2024-21067	Vulnerability in the Oracle Enterprise Manager Base Platform product of Oracle Enterprise Manager (component: Host Management). The supported version that is affe attacker with logon to the infrastructure where Oracle Enterprise Manager Base Platform executes to compromise Oracle Enterprise Manager Base Platform. While the may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in takeover of Oracle Enterprise Manager Base Platform. impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).
CVE-2024-32003	wn-dusk-plugin (Dusk plugin) is a plugin which integrates Laravel Dusk browser testing into Winter CMS. The Dusk plugin provides some special routes as part of its te Chrome) to act as a user in the Backend or User plugin without having to go through authentication. This route is `[[URL]]/_dusk/login/[[USER ID]]/[[MANAGER]]` - whe account and `[[MANAGER]]` is the authentication manager (either `backend` for Backend, or `user` for the User plugin). If a configuration of a site using the Dusk plugir test cases in Dusk are run with live data, this route may potentially be used to gain access to any user account in either the Backend or User plugin without authenticati development and should *NOT* be used in a production instance. It is specifically recommended that the plugin be installed as a development dependency only in Corr will now no longer be registered unless the `APP_ENV` environment variable is specifically set to `dusk`. Since Winter by default does not use this environment variabl configuration is used (which won't exhibit this vulnerability) or if a developer manually specifies it in their configuration. The automatic configuration performed by the Du not allow external environment variables to leak into this configuration. This will only affect users in which the Winter CMS installation meets ALL the following criteria: 1 application is in production mode (ie. the `debug` config value is set to `true` in `config/app.php`). 3. The Dusk plugin's automatic configuration has been overridden, eit configuration in the `config/dusk` folder, or by providing configuration environment variables externally. 4. The environment has been configured to use production data Dusk uses by default. 5. The application is connectable via the web. This issue has been fixed in version 2.1.0. Users are advised to upgrade.
CVE-2024-32019	Netdata is an open source observability tool. In affected versions the `ndsudo` tool shipped with affected versions of the Netdata Agent allows an attacker to run arbitra `root`-owned executable with the SUID bit set. It only runs a restricted set of external commands, but its search paths are supplied by the `PATH` environment variable. commands, which may be a path the attacker has write access to. This may lead to local privilege escalation. This vulnerability has been addressed in versions 1.45.3 a workarounds for this vulnerability.
CVE-2024-3882	A vulnerability was found in Tenda W30E 1.0.1.25(633). It has been classified as critical. Affected is the function fromRouteStatic of the file /goform/fromRouteStatic. Th overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-260916. N respond in any way.
CVE-2024-3881	A vulnerability was found in Tenda W30E 1.0.1.25(633) and classified as critical. This issue affects the function frmL7PlotForm of the file /goform/frmL7ProtForm. The r The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-260915. NOTE respond in any way.
CVE-2024-29837	The Web interface of Evolution Controller Versions 2.04.560.31.03.2024 and below uses poor session management, allowing for an unauthenticated attacker to access
CVE-2024-1755	The NPS computy WordPress plugin through 2.7.5 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwante
CVE-2024-3879	A vulnerability, which was classified as critical, was found in Tenda W30E 1.0.1.25(633). This affects the function formSetCfm of the file /goform/setcfm. The manipulati possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-260913 was assigned to this vulnerability. NO respond in any way.
CVE-2024-3878	A vulnerability, which was classified as critical, has been found in Tenda F1202 1.2.0.20(408). Affected by this issue is the function fromwebExcptypemanFilter of the fil page leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this v about this disclosure but did not respond in any way.
CVE-2024-3877	A vulnerability classified as critical was found in Tenda F1202 1.2.0.20(408). Affected by this vulnerability is the function fromqossetting of the file /goform/fromqossettin overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-260 did not respond in any way.

CVE Number	Description
CVE-2024-3876	A vulnerability classified as critical has been found in Tenda F1202 1.2.0.20(408). Affected is the function fromVirtualSer of the file /goform/VirtualSer. The manipulatior possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-260910 is the identifier assigned to this vulnerability. NOTE respond in any way.
CVE-2024-3875	A vulnerability was found in Tenda F1202 1.2.0.20(408). It has been rated as critical. This issue affects the function fromNatlimit of the file /goform/Natlimit. The manipu attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-260909 was assigned to this vulnerability. NOTE: Tl in any way.
CVE-2024-31424	Cross-Site Request Forgery (CSRF) vulnerability in Hamid Alinia - idehweb Login with phone number.This issue affects Login with phone number: from n/a through 1.6
CVE-2024-29269	An issue discovered in Telesquare TLR-2005Ksh 1.0.0 and 1.1.4 allows attackers to run arbitrary system commands via the Cmd parameter.
CVE-2024-3874	A vulnerability was found in Tenda W20E 15.11.0.6. It has been declared as critical. This vulnerability affects the function formSetRemoteWebManage of the file /goforr leads to stack-based buffer overflow. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerabi disclosure but did not respond in any way.
CVE-2024-29218	Out-of-bounds write vulnerability exists in KV STUDIO Ver.11.64 and earlier, KV REPLAY VIEWER Ver.2.64 and earlier, and VT5-WX15/WX12 Ver.6.02 and earlier, wl having a user of the affected product open a specially crafted file.
CVE-2024-3856	A use-after-free could occur during WASM execution if garbage collection ran during the creation of an array. This vulnerability affects Firefox < 125.
CVE-2024-30220	Command injection vulnerability in MZK-MF300N all firmware versions allows a network-adjacent unauthenticated attacker to execute an arbitrary command by sending
CVE-2024-3854	In some code patterns the JIT incorrectly optimized switch statements and generated code with out-of-bounds-reads. This vulnerability affects Firefox < 125, Firefox ES
CVE-2024-3782	Cross-Site Request Forgery vulnerability in WBSAirback 21.02.04, which could allow an attacker to create a manipulated HTML form to perform privileged actions once
CVE-2023-47622	iTop is an IT service management platform. When dashlet are refreshed, XSS attacks are possible. This vulnerability is fixed in 3.0.4 and 3.1.1.
CVE-2023-47626	iTop is an IT service management platform. When displaying/editing the user's personal tokens, XSS attacks are possible. This vulnerability is fixed in 3.1.1.
CVE-2023-4856	A format string vulnerability was identified in SMM/SMM2 and FPC that could allow an authenticated user to execute arbitrary commands on a specific API endpoint.
CVE-2024-22014	An issue discovered in 360 Total Security Antivirus through 11.0.0.1061 for Windows allows attackers to gain escalated privileges via Symbolic Link Follow to Arbitrary
CVE-2024-28558	SQL Injection vulnerability in sourcecodester Petrol pump management software v1.0, allows remote attackers to execute arbitrary code, escalate privileges, and obtair
CVE-2024-27474	Leantime 3.0.6 is vulnerable to Cross Site Request Forgery (CSRF). This vulnerability allows malicious actors to perform unauthorized actions on behalf of authenticate
CVE-2024-29022	Xibo is an Open Source Digital Signage platform with a web content management system and Windows display player software. In affected versions some request hea tables. These headers can be used to inject a malicious script into the session page to exfiltrate session IDs and User Agents. These session IDs / User Agents can sul injected into the display grid to exfiltrate information related to displays. Users should upgrade to version 3.3.10 or 4.0.9 which fix this issue. Customers who host their C patch to resolve this issue regardless of the CMS version that they are running. Upgrading to a fixed version is necessary to remediate. Patches are available for earlier ebeccd000b51f00b9a25f56a2f252d6812ebf850.diff. 1.8 patch a81044e6ccdd92cc967e34c125bd8162432e51bc.diff. There are no known workarounds for this issue.
CVE-2024-1655	Certain ASUS WiFi routers models has an OS Command Injection vulnerability, allowing an authenticated remote attacker to execute arbitrary system commands by se
CVE-2024-21115	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.16. Easily exploitable infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly i vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:

CVE Number	Description
CVE-2024-21113	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.16. Easily exploitable infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly i vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:
CVE-2024-25852	Linksys RE7000 v2.0.9, v2.0.11, and v2.0.15 have a command execution vulnerability in the "AccessControlList" parameter of the access control function point. An atta
CVE-2024-26362	HTML injection vulnerability in Enpass Password Manager Desktop Client 6.9.2 for Windows and Linux allows attackers to run arbitrary HTML code via creation of craft
CVE-2023-51515	Missing Authorization vulnerability in Undsgn Uncode Core allows Privilege Escalation.This issue affects Uncode Core: from n/a through 2.8.8.
CVE-2024-3705	Unrestricted file upload vulnerability in OpenGnsys affecting version 1.1.1d (Espeto). This vulnerability allows an attacker to send a POST request to the endpoint '/oper file extension verification, resulting in a webshell injection.
CVE-2024-31759	An issue in sanluan PublicCMS v.4.0.202302.e allows an attacker to escalate privileges via the change password function.
CVE-2020-8006	The server in Circontrol Raption through 5.11.2 has a pre-authentication stack-based buffer overflow that can be exploited to gain run-time control of the device as root. a number of common exploitation mitigations. In particular, there are no stack canaries and they do not use the Position Independent Executable (PIE) format.
CVE-2024-21112	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.16. Easily exploitable infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly i vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:
CVE-2024-3211	The Shopping Cart & eCommerce Store plugin for WordPress is vulnerable to SQL Injection via the 'productid' attribute of the ec_addtocart shortcode in all versions up parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with contributor-level access and above, to a used to extract sensitive information from the database.
CVE-2024-30850	An issue in tiagorlampert CHAOS v5.0.1 allows a remote attacker to execute arbitrary code via the BuildClient function within client_service.go
CVE-2024-21114	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.16. Easily exploitable infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly i vulnerability can result in takeover of Oracle VM VirtualBox. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:
CVE-2024-3092	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.9 before 16.9.4, all versions starting from 16.10 before 16.10.2. A payload may lea perform arbitrary actions on behalf of victims.
CVE-2023-47123	iTop is an IT service management platform. By filling malicious code in an object friendlyname / complementary name, an XSS attack can be performed when this obje vulnerability is fixed in 3.1.1 and 3.2.0.
CVE-2024-2279	An issue has been discovered in GitLab CE/EE affecting all versions starting from 16.7 to 16.8.6 all versions starting from 16.9 before 16.9.4, all versions starting from feature a crafted payload may lead to a stored XSS, allowing attackers to perform arbitrary actions on behalf of victims.
CVE-2024-25911	Missing Authorization vulnerability in Skymoon Labs MoveTo.This issue affects MoveTo: from n/a through 6.2.
CVE-2024-32487	less through 653 allows OS command execution via a newline character in the name of a file, because quoting is mishandled in filename.c. Exploitation typically require from an untrusted archive. Exploitation also requires the LESSOPEN environment variable, but this is set by default in many common cases.
CVE-2024-3493	A specific malformed fragmented packet type (fragmented packets may be generated automatically by devices that send large amounts of data) can cause a major non Guard Logix 5580, CompactLogix 5380, and 1756-EN4TR. If exploited, the affected product will become unavailable and require a manual restart to recover it. Addition devices.
CVE-2024-32139	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Podlove Podlove Podcast Publisher.This issue affects Podlove
CVE-2024-32125	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Booking Algorithms BA Book Everything.This issue affects BA B

CVE Number	Description
CVE-2024-32127	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Markus Seyer Find Duplicates.This issue affects Find Duplicate
CVE-2024-32137	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Solwin User Activity Log Pro.This issue affects User Activity Log
CVE-2024-31355	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Tribulant Slideshow Gallery.This issue affects Slideshow Galler
CVE-2024-24809	Traccar is an open source GPS tracking system. Versions prior to 6.0 are vulnerable to path traversal and unrestricted upload of file with dangerous type. Since the sys permissions by registering an account and exploit this vulnerability to upload files with the prefix `device.` under any folder. Attackers can use this vulnerability for phish commands on the server. Version 6.0 contains a patch for the issue.
CVE-2023-52070	JFreeChart v1.5.4 was discovered to be vulnerable to ArrayIndexOutOfBounds via the 'setSeriesNeedle(int index, int type)' method. NOTE: this is disputed by multiple the existence of a vulnerability. The submission may have been based on a tool that is not sufficiently robust for vulnerability identification.
CVE-2024-30381	An Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Juniper Networks Paragon Active Assurance Control Center allows a network-adjacent a sensitive information about downstream devices. The "netrounds-probe-login" daemon (also called probe_serviced) exposes functions where the Test Agent (TA) Appli service accidentally exposes an internal database object that can be used for direct database access on the Paragon Active Assurance Control Center. This issue affec
CVE-2024-22435	A potential security vulnerability has been identified in Web ViewPoint Enterprise software. This vulnerability could be exploited to allow unauthorized users to access s
CVE-2023-40000	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in LiteSpeed Technologies LiteSpeed Cache allows Stored XSS.This
CVE-2024-21095	Vulnerability in the Primavera P6 Enterprise Project Portfolio Management product of Oracle Construction and Engineering (component: Web Access). Supported versi 21.12.18, 22.12.0-22.12.12 and 23.12.0-23.12.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Primave this vulnerability can result in unauthorized access to critical data or complete access to all Primavera P6 Enterprise Project Portfolio Management accessible data as v Primavera P6 Enterprise Project Portfolio Management accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV
CVE-2024-32005	NiceGUI is an easy-to-use, Python-based UI framework. A local file inclusion is present in the NiceUI leaflet component when requesting resource files under the `/_nic on the backend filesystem which the web server has access to can be read by an attacker with access to the NiceUI leaflet website. This vulnerability has been address workarounds for this vulnerability.
CVE-2024-20999	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Zones). The supported version that is affected is 11. Easily exploitable vulnerability allows hi Solaris executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Succes CVSS 3.1 Base Score 8.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H).
CVE-2023-45000	Missing Authorization vulnerability in LiteSpeed Technologies LiteSpeed Cache.This issue affects LiteSpeed Cache: from n/a through 5.7.
CVE-2024-31492	An external control of file name or path vulnerability [CWE-73] in FortiClientMac version 7.2.3 and below, version 7.0.10 and below installer may allow a local attacker t configuration file in /tmp before starting the installation process.
CVE-2024-20759	Adobe Commerce versions 2.4.6-p4, 2.4.5-p6, 2.4.4-p7, 2.4.7-beta3 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused b form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Confidentiality and integrity are c
CVE-2024-31452	OpenFGA is a high-performance and flexible authorization/permission engine. Some end users of OpenFGA v1.5.0 or later are vulnerable to authorization bypass when model involves exclusion (e.g. `a but not b`) or intersection (e.g. `a and b`). This vulnerability is fixed in v1.5.3.
CVE-2024-22262	Applications that use UriComponentsBuilder to parse an externally provided URL (e.g. through a query parameter) AND perform validation checks on the host of the pa https://cwe.mitre.org/data/definitions/601.html attack or to a SSRF attack if the URL is used after passing validation checks. This is the same as CVE-2024-22259 https https://spring.io/security/cve-2024-22243 , but with different input.
CVE-2024-29019	ESPHome is a system to control microcontrollers remotely through Home Automation systems. API endpoints in dashboard component of ESPHome version 2023.12.9 Forgery (CSRF) allowing remote attackers to carry out attacks against a logged user of the dashboard to perform operations on configuration files (create, edit, delete). page that triggers a cross site request against ESPHome, this allows bypassing the authentication for API calls on the platform. This vulnerability allows bypassing auth behalf of a logged user. In order to trigger the vulnerability, the victim must visit a weaponized page. In addition to this, it is possible to chain this vulnerability with GHS user account. Version 2024.3.0 contains a patch for this issue.
CVE-2024-3864	Memory safety bug present in Firefox 124, Firefox ESR 115.9, and Thunderbird 115.9. This bug showed evidence of memory corruption and we presume that with enou vulnerability affects Firefox < 125, Firefox ESR < 115.10, and Thunderbird < 115.10.

CVE Number	Description
CVE-2024-3865	Memory safety bugs present in Firefox 124. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could h Firefox < 125.
CVE-2024-22719	SQL Injection vulnerability in Form Tools 3.1.1 allows attackers to run arbitrary SQL commands via the 'keyword' when searching for a client.
CVE-2024-32256	Phpgurukul Tourism Management System v2.0 is vulnerable to Unrestricted Upload of File with Dangerous Type via /tms/admin/change-image.php. When updating a c from the image.
CVE-2023-44857	An issue in Cobham SAILOR VSAT Ku v.164B019, allows a remote attacker to execute arbitrary code via a crafted script to the sub_21D24 function in the acu_web co
CVE-2024-30407	The Use of a Hard-coded Cryptographic Key vulnerability in Juniper Networks Juniper Cloud Native Router (JCNR) and containerized routing Protocol Deamon (cRPD) attacks which results in complete compromise of the container. Due to hardcoded SSH host keys being present on the container, a PitM attacker can intercept SSH traf All versions before 23.4. This issue affects Juniper Networks cRPD: * All versions before 23.4R1.
CVE-2024-21092	Vulnerability in the Oracle Agile Product Lifecycle Management for Process product of Oracle Supply Chain (component: Product Quality Management). The supported low privileged attacker with network access via HTTP to compromise Oracle Agile Product Lifecycle Management for Process. Successful attacks of this vulnerability ca critical data or all Oracle Agile Product Lifecycle Management for Process accessible data as well as unauthorized access to critical data or complete access to all Orac 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).
CVE-2023-2794	A flaw was found in ofono, an Open Source Telephony on Linux. A stack overflow bug is triggered within the decode_deliver() function during the SMS decoding. It is a modem, a malicious base station, or just SMS. There is a bound check for this memcpy length in decode_submit(), but it was forgotten in decode_deliver().
CVE-2023-48709	iTop is an IT service management platform. When exporting data from backoffice or portal in CSV or Excel files, users' inputs may include malicious formulas that may Code Execution by default, uninformed users may become victims. This vulnerability is fixed in 2.7.9, 3.0.4, 3.1.1, and 3.2.0.
CVE-2023-49528	Buffer Overflow vulnerability in FFmpeg version n6.1-3-g466799d4f5, allows a local attacker to execute arbitrary code and cause a denial of service (DoS) via the af_di
CVE-2024-25545	An issue in Weave Weave Desktop v.7.78.10 allows a local attacker to execute arbitrary code via a crafted script to the nwjs framework component.
CVE-2024-20795	Animate versions 23.0.4, 24.0.1 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context o that a victim must open a malicious file.
CVE-2024-3780	A vulnerability of Information Exposure has been found on Technicolor CGA2121 affecting the version 1.01, this vulnerability allows a local attacker to obtain sensitive i respective passwords.
CVE-2024-20797	Animate versions 23.0.4, 24.0.1 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 a 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.
CVE-2024-30271	Illustrator versions 28.3, 27.9.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current u must open a malicious file.
CVE-2021-47198	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Fix use-after-free in lpfc_unreg_rpi() routine An error is detected with the following report wh lpfc_unreg_rpi+0x1b1b" The NLP_REG_LOGIN_SEND nlp_flag is set in lpfc_reg_fab_ctrl_node(), but the flag is not cleared upon completion of the login. This allows a LPFC_RPI_ALLOW_ERROR. This results in a use after free access when used as an rpi_ids array index. Fix by clearing the NLP_REG_LOGIN_SEND nlp_flag in lpfc
CVE-2021-47194	In the Linux kernel, the following vulnerability has been resolved: cfg80211: call cfg80211_stop_ap when switch from P2P_GO type If the userspace tools switch from N send_msg(NL80211_CMD_SET_INTERFACE), it does not call the cleanup cfg80211_stop_ap(), this leads to the initialization of in-use data. For example, this path re- assigned_vifs list, and makes that linked list corrupt.
CVE-2024-30272	Illustrator versions 28.3, 27.9.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current u must open a malicious file.
CVE-2024-28099	VT STUDIO Ver.8.32 and earlier contains an issue with the DLL search path, which may lead to insecurely loading Dynamic Link Libraries. As a result, arbitrary code m
CVE-2024-30273	Illustrator versions 28.3, 27.9.2 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the c victim must open a malicious file.

CVE Number	Description
CVE-2024-25376	An issue discovered in Thesycon Software Solutions Gmbh & Co. KG TUSBAudio MSI-based installers before 5.68.0 allows a local attacker to execute arbitrary code v
CVE-2024-32488	In Foxit PDF Reader and Editor before 2024.1, Local Privilege Escalation could occur during update checks because weak permissions on the update-service folder all
CVE-2023-33806	Insecure default configurations in Hikvision Interactive Tablet DS-D5B86RB/B V2.3.0 build220119, allows attackers to execute arbitrary commands.
CVE-2024-29219	Out-of-bounds read vulnerability exists in KV STUDIO Ver.11.64 and earlier and KV REPLAY VIEWER Ver.2.64 and earlier, and VT5-WX15/WX12 Ver.6.02 and earlier having a user of the affected product open a specially crafted file.
CVE-2024-21111	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.16. Easily exploitable infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM V 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).
CVE-2024-21059	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). The supported version that is affected is 11. Difficult to exploit vulnerability allows low executes to compromise Oracle Solaris. While the vulnerability is in Oracle Solaris, attacks may significantly impact additional products (scope change). Successful atta 3.1 Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H).
CVE-2024-20772	Media Encoder versions 24.2.1, 23.6.4 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context that a victim must open a malicious file.
CVE-2024-21103	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.16. Easily exploitable infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM V Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).
CVE-2024-3857	The JIT created incorrect code for arguments in certain cases. This led to potential use-after-free crashes during garbage collection. This vulnerability affects Firefox <
CVE-2024-21116	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.16. Easily exploitable infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM V Base Score 7.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).
CVE-2024-31240	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in InfoTheme WP Poll Maker.This issue affects WP Poll Maker: from n/a thro
CVE-2024-3783	The Backup Agents section in WBSAirback 21.02.04 is affected by a Path Traversal vulnerability, allowing a user with low privileges to download files from the system.
CVE-2024-2740	Information exposure vulnerability in Planet IGS-4215-16T2S, affecting firmware version 1.305b210528. This vulnerability could allow a remote attacker to access some Switch web interface.
CVE-2024-31446	OpenComputers is a Minecraft mod that adds programmable computers and robots to the game. A user can use OpenComputers to get a Computer thread stuck in the to be forcibly shut down. This can be accomplished using any device in the mod and can be performed by anyone who can execute Lua code on them. This occurs whi vulnerability is fixed in 1.8.4. The GregTech: New Horizons modpack uses its own modified version of OpenComputers. They have applied the relevant patch in version
CVE-2024-32132	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Codeboxr Team CBX Bookmark & Favorite.This issue affects C
CVE-2024-32098	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Page Visit Counter Advanced Page Visit Counter.This issue aff
CVE-2024-32136	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Xenioushk BWL Advanced FAQ Manager.This issue affects BW
CVE-2024-32134	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Nasirahmed Forms to Zapier, Integromat, IFTTT, Workato, Auto to Zapier, Integromat, IFTTT, Workato, Automate.Io, elastic.Io, Built.Io, APIANT, Webhook: from n/a through 1.1.12.
CVE-2024-31356	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Solwin Infotech User Activity Log.This issue affects User Activit

CVE Number	Description
CVE-2024-29399	An issue was discovered in GNU Savane v.3.13 and before, allows a remote attacker to execute arbitrary code and escalate privileges via a crafted file to the upload.pl
CVE-2024-2243	A vulnerability was found in csmock where a regular user of the OSH service (anyone with a valid Kerberos ticket) can use the vulnerability to disclose the confidential S workers.
CVE-2024-32135	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in WPZest Disable Comments I WPZest.This issue affects Disable
CVE-2024-29504	Cross Site Scripting vulnerability in Summernote v.0.8.18 and before allows a remote attacker to execute arbtirary code via a crafted payload to the codeview paramete
CVE-2024-32087	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in ExportFeed.Com Product Feed on WooCommerce for Google.T through 3.5.7.
CVE-2024-1739	lunary-ai/lunary is vulnerable to an authentication issue due to improper validation of email addresses during the signup process. Specifically, the server fails to treat en accounts with the same email address by varying the case of the email characters. For example, accounts for 'abc@gmail.com' and 'Abc@gmail.com' can both be crea
CVE-2023-51391	A bug in Micrium OS Network HTTP Server permits an invalid pointer dereference during header processing - potentially allowing a device crash and Denial of Service.
CVE-2024-3384	A vulnerability in Palo Alto Networks PAN-OS software enables a remote attacker to reboot PAN-OS firewalls when receiving Windows New Technology LAN Manager cause the firewall to enter maintenance mode, which requires manual intervention to bring the firewall back online.
CVE-2023-5392	C300 information leak due to an analysis feature which allows extracting more memory over the network than required by the function. Honeywell recommends updatin Notification for recommendations on upgrading and versioning.
CVE-2024-29838	The Web interface of Evolution Controller Versions 2.04.560.31.03.2024 and below does not proper sanitize user input, allowing for an unauthenticated attacker to cras
CVE-2024-29842	The Web interface of Evolution Controller Versions 2.04.560.31.03.2024 and below contains poorly configured access control on DESKTOP_EDIT_USER_GET_ABAC abacard field of any user
CVE-2021-47186	In the Linux kernel, the following vulnerability has been resolved: tipc: check for null after calling kmemdup kmemdup can return a null pointer so need to check for it, ot can be seen in the trace [1]. [1] https://syzkaller.appspot.com/bug?id=bca180abb29567b189efdbdb34cbf7ba851c2a58
CVE-2024-3385	A packet processing mechanism in Palo Alto Networks PAN-OS software enables a remote attacker to reboot hardware-based firewalls. Repeated attacks eventually c intervention to bring the firewall back online. This affects the following hardware firewall models: - PA-5400 Series firewalls - PA-7000 Series firewalls
CVE-2024-29841	The Web interface of Evolution Controller Versions 2.04.560.31.03.2024 and below contains poorly configured access control on DESKTOP_EDIT_USER_GET_KEYS value of any user
CVE-2024-29840	The Web interface of Evolution Controller Versions 2.04.560.31.03.2024 and below contains poorly configured access control on DESKTOP_EDIT_USER_GET_PIN_F of any user
CVE-2024-3382	A memory leak exists in Palo Alto Networks PAN-OS software that enables an attacker to send a burst of crafted packets through the firewall that eventually prevents tl Series devices that are running PAN-OS software with the SSL Forward Proxy feature enabled.
CVE-2024-29839	The Web interface of Evolution Controller Versions 2.04.560.31.03.2024 and below contains poorly configured access control on DESKTOP_EDIT_USER_GET_CARD of any user
CVE-2024-29843	The Web interface of Evolution Controller Versions 2.04.560.31.03.2024 and below contains poorly configured access control on MOBILE_GET_USERS_LIST, allowin levels
CVE-2024-28869	Traefik is an HTTP reverse proxy and load balancer. In affected versions sending a GET request to any Traefik endpoint with the "Content-length" request header resul can be exploited by attackers to induce a denial of service. This vulnerability has been addressed in version 2.11.2 and 3.0.0-rc5. Users are advised to upgrade. For aff readTimeout option.

CVE Number	Description
CVE-2024-21006	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. network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or comple 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).
CVE-2024-30395	An Improper Validation of Specified Type of Input vulnerability in Routing Protocol Daemon (RPD) of Junos OS and Junos OS Evolved allows an unauthenticated, netw received over an established BGP session which contains a tunnel encapsulation attribute with a specifically malformed TLV, rpd will crash and restart. This issue affec 21.3R3-S5, * from 21.4 before 21.4R3-S5, * 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, * before 21.2R3-S7-EVO, * from 21.3-EVO before 21.3R3-S5-EVO, * from 21.4-EVO before 21.4R3-S5-EVO, * from 22.2-EVO before 22.2R3-S3-EVO, * from 22.3-E\ from 23.2-EVO before 23.2R1-S2-EVO, 23.2R2-EVO. This is a related but separate issue than the one described in JSA75739
CVE-2024-21088	Vulnerability in the Oracle Production Scheduling product of Oracle E-Business Suite (component: Import Utility). Supported versions that are affected are 12.2.4-12.2.1 network access via HTTP to compromise Oracle Production Scheduling. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modifica 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).
CVE-2024-29400	An issue was discovered in RuoYi v4.5.1, allows attackers to obtain sensitive information via the status parameter.
CVE-2024-21079	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Campaign LOV). Supported versions that are affected are 12.2.3-12.2.13. Easily access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Or (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2024-21598	An Improper Validation of Syntactic Correctness of Input vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allov Service (DoS). If a BGP update is received over an established BGP session which contains a tunnel encapsulation attribute with a specifically malformed TLV, rpd will versions 20.4R1 and later versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 2 than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2; Junos OS Evolved: * 20.4 EVO; * 21.2-EVO versions earlier than 21.2R3-S7-EVO; * 21.3-EVO versions earlier than 21.3R3-S5-EVO; * 21.4-EVO versions earlier than 21.4R3-S5-EVO; * 22.1-E\ than 22.2R3-S3-EVO; * 22.3-EVO versions earlier than 22.3R3-S1-EVO; * 22.4-EVO versions earlier than 22.4R3-EVO; * 23.2-EVO versions earlier than 23.2R1-S2-E\ OS versions earlier than 20.4R1; * Junos OS Evolved versions earlier than 20.4R1-EVO. This is a related but separate issue than the one described in JSA79095.
CVE-2023-51142	An issue in ZKTeco BioTime v.8.5.4 and before allows a remote attacker to obtain sensitive information.
CVE-2023-51672	Missing Authorization vulnerability in FunnelKit FunnelKit Checkout.This issue affects FunnelKit Checkout: from n/a through 3.10.3.
CVE-2024-21078	Vulnerability in the Oracle Marketing product of Oracle E-Business Suite (component: Campaign LOV). Supported versions that are affected are 12.2.3-12.2.13. Easily access via HTTP to compromise Oracle Marketing. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Or (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2024-21077	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: GL Accounts LOV). Supported versions that are affected are 12.2.3-12. network access via HTTP to compromise Oracle Trade Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or comple 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).
CVE-2024-30394	A Stack-based Buffer Overflow vulnerability in the Routing Protocol Daemon (RPD) component of Junos OS and Junos OS Evolved allows an unauthenticated, networl (DoS). On all Junos OS and Junos OS Evolved platforms, when EVPN is configured, and a specific EVPN type-5 route is received via BGP, rpd crashes and restarts. C Service (DoS) condition. This issue affects: Junos OS: * all versions before 21.2R3-S7, * from 21.4 before 21.4R3-S5, * from 22.1 before 22.1R3-S4, * from 22.2 before from 23.2 before 23.2R2. Junos OS Evolved: * all versions before 21.4R3-S5-EVO, * from 22.1-EVO before 22.1R3-S4-EVO, * from 22.2-EVO before 22.2R3-S2-EVO, 22.4R3-EVO, * from 23.2-EVO before 23.2R2-EVO.
CVE-2024-21076	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Offer LOV). Supported versions that are affected are 12.2.3-12.2.13. Ea network access via HTTP to compromise Oracle Trade Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or comple 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).
CVE-2024-21007	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. network access via T3, IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or comple 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).
CVE-2024-30405	An Incorrect Calculation of Buffer Size vulnerability in Juniper Networks Junos OS SRX 5000 Series devices using SPC2 line cards while ALGs are enabled allows an a of Service (DoS). Continued receipt and processing of these specific packets will sustain the Denial of Service condition. This issue affects: Juniper Networks Junos OS than 21.2R3-S7; * 21.4 versions earlier than 21.4R3-S6; * 22.1 versions earlier than 22.1R3-S5; * 22.2 versions earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3 23.2R2.
CVE-2024-21075	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Claim Line LOV). Supported versions that are affected are 12.2.3-12.2. network access via HTTP to compromise Oracle Trade Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or comple 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).
CVE-2024-28458	Null Pointer Dereference vulnerability in swfdump in swftools 0.9.2 allows attackers to crash the appliation via the function compileSWFActionCode in action/actioncom
CVE-2024-30382	An Improper Handling of Exceptional Conditions vulnerability in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a netwo causing an rpd core due to memory corruption, leading to a Denial of Service (DoS). This issue can only be triggered when the system is configured for CoS-based forw (see below). This issue affects: Junos OS: * all versions before 20.4R3-S10, * from 21.2 before 21.2R3-S8, * from 21.3 before 21.3R3, * from 21.4 before 21.4R3, * fror S8-EVO, * from 21.3 before 21.3R3-EVO, * from 21.4 before 21.4R3-EVO, * from 22.1 before 22.1R2-EVO.

CVE Number	Description
CVE-2024-23077	JFreeChart v1.5.4 was discovered to be vulnerable to ArrayIndexOutOfBounds via the component /chart/plot/CompassPlot.java. NOTE: this is disputed by multiple third the existence of a vulnerability. The submission may have been based on a tool that is not sufficiently robust for vulnerability identification.
CVE-2024-21074	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Finance LOV). Supported versions that are affected are 12.2.3-12.2.13. network access via HTTP to compromise Oracle Trade Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or comple 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).
CVE-2024-30392	A Stack-based Buffer Overflow vulnerability in Flow Processing Daemon (flowd) of Juniper Networks Junos OS allows an unauthenticated, network-based attacker to c SPC3 and MS-MPC/-MIC, when URL filtering is enabled and a specific URL request is received and processed, flowd will crash and restart. Continuous reception of th condition. This issue affects: Junos OS: * all versions before 21.2R3-S6, * from 21.3 before 21.3R3-S5, * from 21.4 before 21.4R3-S5, * from 22.1 before 22.1R3-S3, * from 22.4 before 22.4R2-S1, 22.4R3.
CVE-2024-30397	An Improper Check for Unusual or Exceptional Conditions vulnerability in the the Public Key Infrastructure daemon (pkid) of Juniper Networks Junos OS allows an unau pkid is responsible for the certificate verification. Upon a failed verification, the pkid uses all CPU resources and becomes unresponsive to future verification attempts. T certificate verification will fail. This CPU utilization of pkid can be checked using this command: root@srx> show system processes extensive | match pkid xxxxx root Juniper Networks Junos OS * All versions prior to 20.4R3-S10; * 21.2 versions prior to 21.2R3-S7; * 21.4 versions prior to 21.4R3-S5; * 22.1 versions prior to 22.1R3-S * 22.4 versions prior to 22.4R3; * 23.2 versions prior to 23.2R1-S2, 23.2R2.
CVE-2024-30398	An Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS allows Service (DoS). When a high amount of specific traffic is received on a SRX4600 device, due to an error in internal packet handling, a consistent rise in CPU memory uti the PFE crashes. A manual reboot of the PFE will be required to restore the device to original state. This issue affects Junos OS: * 21.2 before 21.2R3-S7, * 21.4 befo before 22.3R3-S2, * 22.4 before 22.4R3, * 23.2 before 23.2R1-S2, 23.2R2.
CVE-2024-21073	Vulnerability in the Oracle Trade Management product of Oracle E-Business Suite (component: Claim LOV). Supported versions that are affected are 12.2.3-12.2.13. E network access via HTTP to compromise Oracle Trade Management. Successful attacks of this vulnerability can result in unauthorized access to critical data or comple 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).
CVE-2024-21090	Vulnerability in the MySQL Connectors product of Oracle MySQL (component: Connector/Python). Supported versions that are affected are 8.3.0 and prior. Easily explo via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeata 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).
CVE-2024-31872	IBM Security Verify Access Appliance 10.0.0 through 10.0.7 could allow a malicious actor to conduct a man in the middle attack when deploying Open Source scripts d
CVE-2024-3852	GetBoundName could return the wrong version of an object when JIT optimizations were applied. This vulnerability affects Firefox < 125, Firefox ESR < 115.10, and Th
CVE-2024-31309	HTTP/2 CONTINUATION DoS attack can cause Apache Traffic Server to consume more resources on the server. Version from 8.0.0 through 8.1.9, from 9.0.0 through (proxy.config.http2.max_continuation_frames_per_minute) to limit the number of CONTINUATION frames per minute. ATS does have a fixed amount of memory a req Users are recommended to upgrade to versions 8.1.10 or 9.2.4 which fixes the issue.
CVE-2024-23911	Out-of-bounds read vulnerability caused by improper checking of the option length values in IPv6 NDP packets exists in Cente middleware TCP/IP Network Series, whi by sending a specially crafted packet.
CVE-2024-3858	It was possible to mutate a JavaScript object so that the JIT could crash while tracing it. This vulnerability affects Firefox < 125.
CVE-2024-24485	An issue discovered in silex technology DS-600 Firmware v.1.4.1 allows a remote attacker to obtain sensitive information via the GET EEP_DATA command.
CVE-2023-4857	An authentication bypass vulnerability was identified in SMM/SMM2 and FPC that could allow an authenticated user to execute certain IPMI calls that could lead to exp
CVE-2024-31887	IBM Security Verify Privilege 11.6.25 could allow an unauthenticated actor to obtain sensitive information from the SOAP API. IBM X-Force ID: 287651.
CVE-2024-0218	A Denial of Service (Dos) vulnerability in Nozomi Networks Guardian, caused by improper input validation in certain fields used in the Radius parsing functionality of ou malformed network packets to cause the IDS module to stop updating nodes, links, and assets. Network traffic may not be analyzed until the IDS module is restarted.
CVE-2024-31259	Insertion of Sensitive Information into Log File vulnerability in Searchiq SearchIQ.This issue affects SearchIQ: from n/a through 4.5.
CVE-2024-3853	A use-after-free could result if a JavaScript realm was in the process of being initialized when a garbage collection started. This vulnerability affects Firefox < 125.

CVE Number	Description
CVE-2024-32086	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in AitThemes Citadela Listing.This issue affects Citadela Listing: from n/a through 5.18.1.
CVE-2024-2424	An input validation vulnerability exists in the Rockwell Automation 5015-AENFTXT that causes the secondary adapter to result in a major nonrecoverable fault (MNRF) will be impacted, and a manual restart is required. Additionally, a malformed PTP packet is needed to exploit this vulnerability.
CVE-2024-23076	JFreeChart v1.5.4 was discovered to contain a NullPointerException via the component /labels/BubbleXYItemLabelGenerator.java. NOTE: this is disputed by multiple tl the existence of a vulnerability. The submission may have been based on a tool that is not sufficiently robust for vulnerability identification.
CVE-2024-31297	Missing Authorization vulnerability in WPExperts Wholesale For WooCommerce.This issue affects Wholesale For WooCommerce: from n/a through 2.3.0.
CVE-2023-50872	The API in Accredible Credential.net December 6th, 2023 allows an Insecure Direct Object Reference attack that discloses partial information about certificates and the this issue mentions "Vendor says that it's not a security issue."
CVE-2024-31873	IBM Security Verify Access Appliance 10.0.0 through 10.0.7 contains hard-coded credentials which it uses for its own inbound authentication that could be obtained by
CVE-2024-31358	Missing Authorization vulnerability in Saleswonder.Biz 5 Stars Rating Funnel.This issue affects 5 Stars Rating Funnel: from n/a through 1.2.67.
CVE-2024-31343	Missing Authorization vulnerability in Sonaar Music MP3 Audio Player for Music, Radio & Podcast by Sonaar.This issue affects MP3 Audio Player for Music, Radio & P
CVE-2024-31871	IBM Security Verify Access Appliance 10.0.0 through 10.0.7 could allow a malicious actor to conduct a man in the middle attack when deploying Python scripts due to i
CVE-2023-5394	Server receiving a malformed message that where the GCL message hostname may be too large which may cause a stack overflow; resulting in possible remote code of the product. See Honeywell Security Notification for recommendations on upgrading and versioning.
CVE-2024-3383	A vulnerability in how Palo Alto Networks PAN-OS software processes data received from Cloud Identity Engine (CIE) agents enables modification of User-ID groups. T inappropriately denied or allowed access to resources based on your existing Security Policy rules.
CVE-2024-30210	IO-1020 Micro ELD uses a default WIFI password that could allow an adjacent attacker to connect to the device.
CVE-2023-5393	Server receiving a malformed message that causes a disconnect to a hostname may causing a stack overflow resulting in possible remote code execution. Honeywell r Honeywell Security Notification for recommendations on upgrading and versioning.
CVE-2024-31069	IO-1020 Micro ELD web server uses a default password for authentication.
CVE-2024-31999	@festify/secure-session creates a secure stateless cookie session for Fastify. At the end of the request handling, it will encrypt all data in the session with a secret key name. After that, the session on the server side is destroyed. When an encrypted cookie with matching session name is provided with subsequent requests, it will decry with the data in the ciphertext. Thus theoretically the web instance is still accessing the data from a server-side session, but technically that session is generated solely because it is encrypted with a secret key not known to the user). The issue exists in the session removal process. In the delete function of the code, when the session i access to the cookie, they could keep using it forever. Version 7.3.0 contains a patch for the issue. As a workaround, one may include a "last update" field in the sessio
CVE-2024-27309	While an Apache Kafka cluster is being migrated from ZooKeeper mode to KRaft mode, in some cases ACLs will not be correctly enforced. Two preconditions are neec The resource associated with the removed ACL continues to have two or more other ACLs associated with it after the removal. When those two preconditions are met, after the removal, rather than the two or more that would be correct. The incorrect condition is cleared by removing all brokers in ZK mode, or by adding a new ACL to t metadata loss (the ACLs all remain). The full impact depends on the ACLs in use. If only ALLOW ACLs were configured during the migration, the impact would be limite include confidentiality and integrity impact depending on the ACLs configured, as the DENY ACLs might be ignored due to this vulnerability during the migration period.
CVE-2024-22450	Dell Alienware Command Center, versions prior to 6.2.7.0, contain an uncontrolled search path element vulnerability. A local malicious user could potentially inject mali
CVE-2024-3691	A vulnerability, which was classified as critical, has been found in PHPGurukul Small CRM 3.0. Affected by this issue is some unknown functionality of the component F may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-260480.

CVE Number	Description
CVE-2024-3534	A vulnerability, which was classified as critical, has been found in Campcodes Church Management System 1.0. Affected by this issue is some unknown functionality of sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259904.
CVE-2024-3738	A vulnerability classified as critical has been found in cym1102 nginxWebUI up to 3.9.9. This affects the function handlePath of the file /adminPage/conf/saveCmd. The validation. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-260577 was assigned to this vu
CVE-2024-21110	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.16. Easily exploitable infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks require human interaction from a person other than the a Oracle VM VirtualBox. CVSS 3.1 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H).
CVE-2024-3535	A vulnerability, which was classified as critical, was found in Campcodes Church Management System 1.0. This affects an unknown part of the file /admin/index.php. Tl possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-259905 was assigned to this vulnerability.
CVE-2023-6236	A flaw was found in Red Hat Enterprise Application Platform 8. When an OIDC app that serves multiple tenants attempts to access the second tenant, it should prompt different OIDC configuration. The underlying issue is in OidcSessionTokenStore when determining if a cached token should be used or not. This logic needs to be upda "realm" option. EAP-7 does not provide the vulnerable provider-url configuration option in its OIDC implementation and is not affected by this flaw.
CVE-2024-22437	A potential security vulnerability has been identified in VSS Provider and CAPI Proxy software for certain HPE MSA storage products. This vulnerability could be exploit
CVE-2024-3769	A vulnerability, which was classified as critical, was found in PHPGurukul Student Record System 3.20. Affected is an unknown function of the file /login.php. The manip to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-260616.
CVE-2023-6811	The Language Translate Widget for WordPress – ConveyThis plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'api_key' parameter in all versio output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected pa
CVE-2020-22539	An arbitrary file upload vulnerability in the Add Category function of Codoforum v4.9 allows attackers to execute arbitrary code via uploading a crafted file.
CVE-2023-6916	Audit records for OpenAPI requests may include sensitive information. This could lead to unauthorized accesses and privilege escalation.
CVE-2023-4855	A command injection vulnerability was identified in SMM/SMM2 and FPC that could allow an authenticated user with elevated privileges to execute unauthorized comm
CVE-2024-3067	The WooCommerce Google Feed Manager plugin for WordPress is vulnerable to SQL Injection via the 'id' parameter in all versions up to, and including, 2.4.2 due to in preparation on the existing SQL query. This makes it possible for authenticated attackers, with administrator-level access and above, to append additional SQL queries information from the database. This can also be used by unauthenticated attackers to inject malicious web scripts.
CVE-2024-21083	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Script Engine). Supported versions that are affected are 7.0.0.0.0 and 12.2.1.4.0. Easily 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 7.2 (C (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2024-3054	WPvivid Backup & Migration Plugin for WordPress is vulnerable to PHAR Deserialization in all versions up to, and including, 0.9.99 via deserialization of untrusted inpu the plugin not providing sufficient path validation on the tree_node[node][id] parameter. This makes it possible for authenticated attackers, with admin-level access and and call arbitrary PHP Objects. No POP chain is present in the vulnerable plugin. If a POP chain is present via an additional plugin or theme installed on the target syst data, or execute code.
CVE-2024-2659	A command injection vulnerability was identified in SMM/SMM2 and FPC that could allow an authenticated user with elevated privileges to execute system commands
CVE-2024-32631	Out-of-Bounds read in ciCCIOTOPT in ASR180X will cause incorrect computations.
CVE-2024-22722	Server Side Template Injection (SSTI) vulnerability in Form Tools 3.1.1 allows attackers to run arbitrary commands via the Group Name field under the add forms sectio
CVE-2024-3020	The plugin is vulnerable to PHP Object Injection in versions up to and including, 2.6.3 via deserialization of untrusted input in the import function via the 'shortcode' para access to inject a PHP Object. If a POP chain is present via an additional plugin or theme installed on the target system, it could allow the attacker to delete arbitrary file
CVE-2024-29023	Xibo is an Open Source Digital Signage platform with a web content management system and Windows display player software. Session tokens are exposed in the retu can be exfiltrated and used to hijack a session. Users must be granted access to the session page, or be a super admin. Users should upgrade to version 3.3.10 or 4.0 Signage service have already received an upgrade or patch to resolve this issue regardless of the CMS version that they are running. Patches are available for earlier v ebeccd000b51f00b9a25f56a2f252d6812ebf850.diff. 1.8 patch a81044e6ccdd92cc967e34c125bd8162432e51bc.diff. There are no known workarounds for this vulnerab

CVE Number	Description
CVE-2024-3778	The file upload functionality of Ai3 QbiBot does not properly restrict types of uploaded files, allowing remote attackers with administrator privilege to upload files with da
CVE-2024-27992	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Link Whisper Link Whisper Free allows Reflected XSS.This issue a
CVE-2024-31285	Cross-Site Request Forgery (CSRF) vulnerability in Tooltip WordPress Tooltips allows Stored XSS.This issue affects WordPress Tooltips: from n/a through 9.5.3.
CVE-2024-31299	Cross-Site Request Forgery (CSRF) vulnerability in Reservation Diary ReDi Restaurant Reservation allows Cross-Site Scripting (XSS).This issue affects ReDi Restaur
CVE-2024-32082	Cross-Site Request Forgery (CSRF) vulnerability in kp4coder Sync Post With Other Site allows Cross-Site Scripting (XSS).This issue affects Sync Post With Other Site
CVE-2024-30884	Reflected Cross-Site Scripting (XSS) vulnerability in Discuz! version X3.4 20220811, allows remote attackers to execute arbitrary code and obtain sensitive information component.
CVE-2024-31093	Cross-Site Request Forgery (CSRF) vulnerability in Kaloyan K. Tsvetkov Broken Images allows Cross-Site Scripting (XSS).This issue affects Broken Images: from n/a
CVE-2024-31086	Cross-Site Request Forgery (CSRF) vulnerability in Venugopal Change default login logo,url and title allows Cross-Site Scripting (XSS).This issue affects Change defa
CVE-2024-32149	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BlueGlass Jobs for WordPress allows Reflected XSS.This issue af
CVE-2024-32145	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in PineWise WP Google Analytics Events allows Reflected XSS.This
CVE-2024-32133	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michael Schuppenies EZ Form Calculator allows Reflected XSS.Th
CVE-2024-32138	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in KaizenCoders Short URL allows Reflected XSS.This issue affects
CVE-2024-30545	Cross-Site Request Forgery (CSRF) vulnerability in Nick Powers Social Author Bio allows Stored XSS.This issue affects Social Author Bio: from n/a through 2.4.
CVE-2024-2741	Cross-Site Request Forgery (CSRF) vulnerability in Planet IGS-4215-16T2S, affecting firmware version 1.305b210528. This vulnerability could allow a remote attacker session, such as adding or updating accounts through the Switch web interface.
CVE-2023-29483	eventlet before 0.35.2, as used in dnspython before 2.6.0, allows remote attackers to interfere with DNS name resolution by quickly sending an invalid packet from the words, dnspython does not have the preferred behavior in which the DNS name resolution algorithm would proceed, within the full time window, in order to wait for a va was addressed in 2.6.1.
CVE-2024-20989	Vulnerability in the Oracle Hospitality Simphony product of Oracle Food and Beverage Applications (component: Simphony POS). Supported versions that are affected attacker with network access via HTTP to compromise Oracle Hospitality Simphony. Successful attacks of this vulnerability can result in unauthorized access to critical data as well as unauthorized update, insert or delete access to some of Oracle Hospitality Simphony accessible data and unauthorized ability to cause a partial denial Score 7.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:L).
CVE-2024-22439	A potential security vulnerability has been identified in HPE FlexFabric and FlexNetwork series products. This vulnerability could be exploited to gain privileged access
CVE-2024-30219	Active debug code vulnerability exists in MZK-MF300N all firmware versions. If a logged-in user who knows how to use the debug function accesses the device's mana
CVE-2024-24487	An issue discovered in silex technology DS-600 Firmware v.1.4.1 allows a remote attacker to cause a denial of service via crafted UDP packets using the EXEC REBO

CVE Number	Description
CVE-2023-44396	iTop is an IT service management platform. Dashlet edits ajax endpoints can be used to produce XSS. Fixed in iTop 2.7.10, 3.0.4, and 3.1.1.
CVE-2024-31464	XWiki Platform is a generic wiki platform. Starting in version 5.0-rc-1 and prior to versions 14.10.19, 15.5.4, and 15.9-rc-1, it is possible to access the hash of a passwo password is deleted. Using that vulnerability it's possible for an attacker to have access to the hash password of a user if they have rights to edit the users' page. With t on user profiles, except by users with Admin rights. Note that this vulnerability also impacts any extensions that might use passwords stored in xobjects: for those usec be 100% sure that this vulnerability has been exploited, as an attacker with enough privilege could have deleted the revision where the xobject was deleted after rolling the target page (Admin right). A page with a user password xobject which have in its history a revision where the object has been deleted should be considered at risk coming from a password field. As another mitigation, admins should ensure that the user pages are properly protected: the edit right shouldn't be allowed for other user is not much workaround possible for a privileged user other than upgrading XWiki.
CVE-2024-0159	Dell Alienware Command Center, versions 5.5.52.0 and prior, contain improper access control vulnerability, leading to Denial of Service on local system.
CVE-2024-23593	A vulnerability was reported in a system recovery bootloader that was part of the Lenovo preloaded Windows 7 and 8 operating systems from 2012 to 2014 that could and escalate privileges.
CVE-2024-21107	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.16. Easily exploitable infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in takeover of Oracle VM V 3.1 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2024-3785	Vulnerability in WBSAirback 21.02.04, which involves improper neutralisation of Server-Side Includes (SSI), through Device NAS shared section (/admin/DeviceNAS). E arbitrary code.
CVE-2024-3786	Vulnerability in WBSAirback 21.02.04, which involves improper neutralisation of Server-Side Includes (SSI), through Device Synchronizations (/admin/DeviceReplicatio arbitrary code.
CVE-2024-32632	A value in ATCMD will be misinterpreted by printf, causing incorrect output and possibly out-of-bounds memory access
CVE-2024-29460	An issue in PX4 Autopilot v.1.14.0 allows an attacker to manipulate the flight path allowing for crashes of the drone via the home point location of the mission_block.cpp
CVE-2024-3784	Vulnerability in WBSAirback 21.02.04, which involves improper neutralisation of Server-Side Includes (SSI), through S3 Accounts (/admin/CloudAccounts). Exploitation
CVE-2023-44855	Cross Site Scripting (XSS) vulnerability in Cobham SAILOR VSAT Ku v.164B019 allows a remote attacker to execute arbitrary code via a crafted script to the rdiag, ser acu_web file.
CVE-2024-21091	Vulnerability in the Oracle Agile Product Lifecycle Management for Process product of Oracle Supply Chain (component: Data Import). The supported version that is af attacker with network access via HTTP to compromise Oracle Agile Product Lifecycle Management for Process. Successful attacks of this vulnerability can result in una Product Lifecycle Management for Process 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
CVE-2024-21104	Vulnerability in the Oracle ZFS Storage Appliance Kit product of Oracle Systems (component: Core). The supported version that is affected is 8.8. Easily exploitable vu where Oracle ZFS Storage Appliance Kit executes to compromise Oracle ZFS Storage Appliance Kit. Successful attacks require human interaction from a person other takeover of Oracle ZFS Storage Appliance Kit. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/
CVE-2024-21106	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.16. Easily exploitable infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly i vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle VM VirtualBox. CVSS 3.1 Base Score 6.5 (Avai (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).
CVE-2024-21121	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.16. Easily exploitable infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. While the vulnerability is in Oracle VM VirtualBox, attacks may significantly i vulnerability can result in unauthorized access to critical data or complete access to all Oracle VM VirtualBox accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N).
CVE-2023-48865	An issue discovered in Reportico Till 8.1.0 allows attackers to obtain sensitive information via execute_mode parameter of the URL.
CVE-2024-32557	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Exclusive Addons Exclusive Addons Elementor allows Stored XSS 2.6.9.2.
CVE-2024-21089	Vulnerability in the Oracle Concurrent Processing product of Oracle E-Business Suite (component: Request Submission and Scheduling). Supported versions that are privileged attacker with network access via HTTP to compromise Oracle Concurrent Processing. Successful attacks of this vulnerability can result in unauthorized acce Processing 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).

CVE Number	Description
CVE-2024-32079	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Michael Dempfle Advanced iFrame allows Stored XSS.This issue a
CVE-2024-3367	Argument injection in websphere_mq agent plugin in Checkmk 2.0.0, 2.1.0, <2.2.0p26 and <2.3.0b5 allows local attacker to inject one argument to runmqsc
CVE-2024-30840	A Stack Overflow vulnerability in Tenda AC15 v15.03.05.18 allows attackers to cause a denial of service via the LISTEN parameter in the fromDhcpListClient function.
CVE-2024-32023	Kohya_ss is a GUI for Kohya's Stable Diffusion trainers. Kohya_ss is vulnerable to a path injection in the `common_gui.py` `find_and_replace` function. This vulnerabili
CVE-2024-32024	Kohya_ss is a GUI for Kohya's Stable Diffusion trainers. Kohya_ss is vulnerable to a path injection in the `common_gui.py` `add_pre_postfix` function. This vulnerability
CVE-2024-3855	In certain cases the JIT incorrectly optimized MSubstr operations, which led to out-of-bounds reads. This vulnerability affects Firefox < 125.
CVE-2024-3652	The Libreswan Project was notified of an issue causing libreswan to restart when using IKEv1 without specifying an esp= line. When the peer requests AES-GMAC, libr crashes and restarts. IKEv2 connections are not affected.
CVE-2024-32091	Cross-Site Request Forgery (CSRF) vulnerability in Tonjoo Sangar Slider.This issue affects Sangar Slider: from n/a through 1.3.2.
CVE-2022-24805	net-snmp provides various tools relating to the Simple Network Management Protocol. Prior to version 5.9.2, a buffer overflow in the handling of the `INDEX` of `NET-S with read-only credentials can exploit the issue. Version 5.9.2 contains a patch. Users should use strong SNMPv3 credentials and avoid sharing the credentials. Those string and enhance the protection by restricting access to a given IP address range.
CVE-2022-24806	net-snmp provides various tools relating to the Simple Network Management Protocol. Prior to version 5.9.2, a user with read-write credentials can exploit an Improper agent and subagent simultaneously. Version 5.9.2 contains a patch. Users should use strong SNMPv3 credentials and avoid sharing the credentials. Those who must u enhance the protection by restricting access to a given IP address range.
CVE-2022-24807	net-snmp provides various tools relating to the Simple Network Management Protocol. Prior to version 5.9.2, a malformed OID in a SET request to `SNMP-VIEW-BASE access. A user with read-write credentials can exploit the issue. Version 5.9.2 contains a patch. Users should use strong SNMPv3 credentials and avoid sharing the cre complex community string and enhance the protection by restricting access to a given IP address range.
CVE-2024-32147	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Form Plugin Team - GhozyLab Easy Contact Form Lite allows Stor 1.1.23.
CVE-2024-32140	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Libsyn Libsyn Publisher Hub allows Stored XSS.This issue affects
CVE-2022-24808	net-snmp provides various tools relating to the Simple Network Management Protocol. Prior to version 5.9.2, a user with read-write credentials can use a malformed OI a NULL pointer dereference. Version 5.9.2 contains a patch. Users should use strong SNMPv3 credentials and avoid sharing the credentials. Those who must use SNM the protection by restricting access to a given IP address range.
CVE-2024-21080	Vulnerability in the Oracle Applications Framework product of Oracle E-Business Suite (component: REST Services). Supported versions that are affected are 12.2.9-1 network access via HTTP to compromise Oracle Applications Framework. Successful attacks of this vulnerability can result in unauthorized access to critical data or co 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).
CVE-2022-24809	net-snmp provides various tools relating to the Simple Network Management Protocol. Prior to version 5.9.2, a user with read-only credentials can use a malformed OID pointer dereference. Version 5.9.2 contains a patch. Users should use strong SNMPv3 credentials and avoid sharing the credentials. Those who must use SNMPv1 or protection by restricting access to a given IP address range.
CVE-2024-1307	The Smart Forms WordPress plugin before 2.6.94 does not have proper authorization in some actions, which could allow users with a role as low as a subscriber to cal
CVE-2023-7201	The Everest Backup WordPress plugin before 2.2.5 does not properly validate backup files to be uploaded, allowing high privilege users such as admin to upload arbitr example in multisite setup)

CVE Number	Description
CVE-2024-30380	An Improper Handling of Exceptional Conditions vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows an adjacent unauthenticated attacker to cau by sending a specific TLV. The l2cpd process is responsible for layer 2 control protocols, such as STP, RSTP, MSTP, VSTP, ERP, and LLDP. The impact of the l2cpd MVRP and ERP, leading to a Denial of Service. Continued receipt and processing of this specific TLV will create a sustained Denial of Service (DoS) condition. This is 21.2R3-S7, from 21.3 before 21.3R3-S5, from 21.4 before 21.4R3-S4, from 22.1 before 22.1R3-S4, from 22.2 before 22.2R3-S2, from 22.3 before 22.3R2-S2, 22.3R3- 23.2R2; Junos OS Evolved: all versions before 21.2R3-S7, from 21.3 before 21.3R3-S5-EVO, from 21.4 before 21.4R3-S5-EVO, from 22.1 before 22.1R3-S4-EVO, fro 22.3R3-S1-EVO, from 22.4 before 22.4R2-S2-EVO, 22.4R3-EVO, from 23.2 before 23.2R1-S1-EVO, 23.2R2-EVO.
CVE-2024-30403	A NULL Pointer Dereference vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS Evolved allows an unauthenticated, adjacent attacker a logical interface, MAC learning happens. If during this process, the interface flaps, an Advanced Forwarding Toolkit manager (evo-aftmand-bt) core is observed. This events happens, which will lead to a sustained DoS condition. This issue affects Juniper Networks Junos OS Evolved 23.2-EVO versions earlier than 23.2R1-S1-EVO,
CVE-2024-30388	An Improper Isolation or Compartmentalization vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS on QFX5000 Series and EX Series al (DoS). If a specific malformed LACP packet is received by a QFX5000 Series, or an EX4400, EX4100 or EX4650 Series device, an LACP flap will occur resulting in traf EX4400, EX4100 or EX4650 Series: * 20.4 versions from 20.4R3-S4 before 20.4R3-S8, * 21.2 versions from 21.2R3-S2 before 21.2R3-S6, * 21.4 versions from 21.4R2 22.2 versions before 22.2R3-S1, * 22.3 versions before 22.3R2-S2, 22.3R3, * 22.4 versions before 22.4R2-S1, 22.4R3.
CVE-2024-30387	A Missing Synchronization vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on ACX5448 and ACX710 allows an unauthenticated, ac while the system gathers statistics on that interface, two processes simultaneously access a shared resource which leads to a PFE crash and restart. This issue affects 21.2R3-S5, * 21.3 versions before 21.3R3-S5, * 21.4 versions before 21.4R3-S4, * 22.1 versions before 22.1R3-S2, * 22.2 versions before 22.2R3-S2, * 22.3 versions
CVE-2024-31391	Insertion of Sensitive Information into Log File vulnerability in the Apache Solr Operator. This issue affects all versions of the Apache Solr Operator from 0.3.0 through (basic authentication and create several accounts for accessing Solr: including the "solr" and "admin" accounts for use by end-users, and a "k8s-oper" account which the these operator requests is healthchecks: liveness, readiness, and startup probes are all used to determine Solr's health and ability to receive traffic. By default, the oper authentication, but users may specifically request that authentication be required on probe endpoints as well. Whenever one of these probes would fail, if authentication containing the username and password of the "k8s-oper" account. Within the affected version range, this vulnerability affects any solrcloud resource which (1) bootstrap `.solrOptions.security.authenticationType=basic` option, and (2) required authentication be used on probes by setting `.solrOptions.security.probesRequireAuth=true`. U fixes this issue by ensuring that probes no longer print the credentials used for Solr requests. Users may also mitigate the vulnerability by disabling authentication on th `.solrOptions.security.probesRequireAuth=false`.
CVE-2024-21618	An Access of Memory Location After End of Buffer vulnerability in the Layer-2 Control Protocols Daemon (l2cpd) of Juniper Networks Junos OS and Junos OS Evolved (DoS). On all Junos OS and Junos OS Evolved platforms, when LLDP is enabled on a specific interface, and a malformed LLDP packet is received, l2cpd crashes and (RSTP, MSTP or VSTP), and MVRP and ERP. Also, if any services depend on LLDP state (like PoE or VoIP device recognition), then these will also be affected. This i before 22.1R3-S4, * from 22.2 before 22.2R3-S2, * from 22.3 before 22.3R2-S2, 22.3R3-S1, * from 22.4 before 22.4R3, * from 23.2 before 23.2R2. Junos OS Evolve 22.1R3-S4-EVO, * from 22.2-EVO before 22.2R3-S2-EVO, * from 22.3-EVO before 22.3R2-S2-EVO, 22.3R3-S1-EVO, * from 22.4-EVO before 22.4R3-EVO, * from 2 versions prior to 21.4R1; * Junos OS Evolved versions prior to 21.4R1-EVO.
CVE-2024-21609	A Missing Release of Memory after Effective Lifetime vulnerability in the IKE daemon (iked) of Juniper Networks Junos OS on MX Series with SPC3, and SRX Series a establish IPsec tunnels to cause a Denial of Service (DoS). If specific values for the IPsec parameters local-ip, remote-ip, remote ike-id, and traffic selectors are sent fro carried out with a specific message sequence. This will eventually result in an iked process crash and restart. The iked process memory consumption can be checked u extensive | grep iked PID USERNAME PRI NICE SIZE RES STATE C TIME WCPU COMMAND 56903 root 31 0 4016M 2543M CPU0 0 2: versions earlier than 20.4R3-S9; * 21.2 versions earlier than 21.2R3-S7; * 21.3 versions earlier than 21.3R3-S5; * 21.4 versions earlier than 21.4R3-S4; * 22.1 versions versions earlier than 22.3R3; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2.
CVE-2024-21605	An Exposure of Resource to Wrong Sphere vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on SRX 300 Series allows an unauthen valid link-local traffic is not blocked on ports in STP blocked state but is instead sent to the control plane of the device. This leads to excessive resource consumption ar device. This issue affects Juniper Networks Junos OS: * 21.2 version 21.2R3-S3 and later versions earlier than 21.2R3-S6; * 22.1 version 22.1R3 and later versions ea than 22.2R3-S2; * 22.3 version 22.3R2 and later versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R2-S2, 22.4R3; * 23.2 versions earlier than 23.2R1-S 21.4R1 and later versions of 21.4.
CVE-2024-21593	An Improper Check or Handling of Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS and Junos OS Evolved a (DoS). If an attacker sends a specific MPLS packet, which upon processing, causes an internal loop, that leads to a PFE crash and restart. Continued receipt of these p cross-connect (CCC) needs to be configured on the device for it to be affected by this issue. This issue only affects MX Series with MPC10, MPC11, LC9600, and MX3 21.4R3 earlier than 21.4R3-S5; 22.2 versions from 22.2R2 earlier than 22.2R3-S2; 22.3 versions from 22.3R1 earlier than 22.3R2-S2; 22.3 versions from 22.3R3 earlie 22.4R3; 23.2 versions earlier than 23.2R1-S1, 23.2R2.
CVE-2022-24810	net-snmp provides various tools relating to the Simple Network Management Protocol. Prior to version 5.9.2, a user with read-write credentials can use a malformed OI dereference. Version 5.9.2 contains a patch. Users should use strong SNMPv3 credentials and avoid sharing the credentials. Those who must use SNMPv1 or SNMPv by restricting access to a given IP address range.
CVE-2023-40148	Server-side request forgery (SSRF) in PingFederate allows unauthenticated http requests to attack network resources and consume server-side resources via forged H
CVE-2024-27988	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WEN Themes WEN Responsive Columns allows Stored XSS.This
CVE-2024-21507	Versions of the package mysql2 before 3.9.3 are vulnerable to Improper Input Validation through the keyFromFields function, resulting in cache poisoning. An attacker
CVE-2024-21509	Versions of the package mysql2 before 3.9.4 are vulnerable to Prototype Poisoning due to insecure results object creation and improper user input sanitization passed

CVE Number	Description
CVE-2024-27989	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in I Thirteen Web Solution WP Responsive Tabs horizontal vertical ar Tabs horizontal vertical and accordion Tabs: from n/a through 1.1.17.
CVE-2024-2665	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's button in all versions up to, and including, 4.10.27 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 v
CVE-2024-3515	Use after free in Dawn in Google Chrome prior to 123.0.6312.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium
CVE-2024-27969	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Enhanced Free Downloads WooCommerce allows Stored XSS 3.5.8.2.
CVE-2024-3516	Heap buffer overflow in ANGLE in Google Chrome prior to 123.0.6312.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (C
CVE-2024-27990	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in The Moneytizer allows Stored XSS.This issue affects The Moneytiz
CVE-2024-31287	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Max Foundry Media Library Folders.This issue affects Media Library Folde
CVE-2023-51141	An issue in ZKTeko BioTime v.8.5.4 and before allows a remote attacker to obtain sensitive information via the Authentication & Authorization component
CVE-2024-27991	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in SupportCandy allows Stored XSS.This issue affects SupportCandy
CVE-2022-44633	Missing Authorization vulnerability in YITH YITH WooCommerce Gift Cards Premium.This issue affects YITH WooCommerce Gift Cards Premium: from n/a through 3.2
CVE-2024-31342	Missing Authorization vulnerability in WPcloudgallery WordPress Gallery Exporter.This issue affects WordPress Gallery Exporter: from n/a through 1.3.
CVE-2024-2539	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via widget '_id' attributes in all versions up to, and including, 8.3.(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 v
CVE-2024-3344	The Otter Blocks – Gutenberg Blocks, Page Builder for Gutenberg Editor & FSE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG file upload ir 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
CVE-2024-3343	The Otter Blocks – Gutenberg Blocks, Page Builder for Gutenberg Editor & FSE plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's block input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject a an injected page.
CVE-2024-3210	The Paid Membership Plugin, Ecommerce, User Registration Form, Login Form, User Profile & Restrict Content – ProfilePress plugin for WordPress is vulnerable to St in all versions up to, and including, 4.15.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated scripts in pages that will execute whenever a user accesses an injected page.
CVE-2024-2655	The Elementor Addons by Livemesh plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Post widgets in all versions up to, and including, (display names. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whe
CVE-2024-2734	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's AI features all versions up to, and including, 4.8.8 due to insuffi 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 ac
CVE-2024-2736	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via HTML Tags in all versions up to, and including, 4.8.8 due to insufficient inp 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 accesse
CVE-2024-2735	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'Price List' element in all versions up to, and including, 4.8.8 due to insu 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

CVE Number	Description
CVE-2024-3027	The Smart Slider 3 plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the upload function in all versions up to attackers, with contributor-level access and above, to upload files, including SVG files, which can be used to conduct stored cross-site scripting attacks.
CVE-2024-1042	The WP Radio – Worldwide Online Radio Stations Directory for WordPress plugin for WordPress is vulnerable to unauthorized modification of data due to a missing ca including, 3.1.9. This makes it possible for authenticated attackers, with subscriber access and above, to import radio stations, remove countries, and modify the plugin CVE-2024-1041.
CVE-2024-1041	The WP Radio – Worldwide Online Radio Stations Directory for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's settings in sanitization and output escaping as well as insufficient access control on the settings. This makes it possible for authenticated attackers, with subscriber access and ab user accesses an injected page.
CVE-2024-2137	The All-in-One Addons for Elementor – WidgetKit plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple pricing widgets (e.g. Pricing Single, Pric insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scr page.
CVE-2024-2801	The Shopkeeper Extender plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'image_slide' shortcode in all versions up to, and including, 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
CVE-2024-1957	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'give_form' shortcode in all v and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web s page.
CVE-2024-27261	IBM Storage Defender - Resiliency Service 2.0.0 through 2.0.2 could allow a privileged user to install a potentially dangerous tar file, which could give them access to s 283986.
CVE-2024-2742	Operating system command injection vulnerability in Planet IGS-4215-16T2S, affecting firmware version 1.305b210528. An authenticated attacker could execute arbitra
CVE-2024-23594	A buffer overflow vulnerability was reported in a system recovery bootloader that was part of the Lenovo preloaded Windows 7 and 8 operating systems from 2012 to 2 arbitrary code.
CVE-2024-30256	Open WebUI is a user-friendly WebUI for LLMs. Open-webui is vulnerable to authenticated blind server-side request forgery. This vulnerability is fixed in 0.1.117.
CVE-2024-3285	The Slider, Gallery, and Carousel by MetaSlider – Responsive WordPress Slideshows plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and abov user accesses an injected page.
CVE-2024-3672	The BA Book Everything plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'all-items' shortcode in all versions up to, and including, 1.6.8 supplied attributes such as 'classes'. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages
CVE-2024-1357	The Shortcodes and extra features for Phlox theme plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's aux_timeline shortcode in all versi output escaping on user supplied attributes such as thumb_mode and date_type. This makes it possible for authenticated attackers with contributor-level and above pe whenever a user accesses an injected page.
CVE-2024-2664	The Premium Addons for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Countdown Widget in all versions up to, and inclu 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 e
CVE-2024-22721	Cross Site Request Forgery (CSRF) vulnerability in Form Tools 3.1.1 allows attackers to manipulate sensitive user data via crafted link.
CVE-2024-3537	A vulnerability was found in Campcodes Church Management System 1.0 and classified as critical. This issue affects some unknown processing of the file /admin/admi injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-259
CVE-2024-3770	A vulnerability has been found in PHPGurukul Student Record System 3.20 and classified as critical. Affected by this vulnerability is an unknown functionality of the file leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-260617 was assigned to
CVE-2024-3690	A vulnerability classified as critical was found in PHPGurukul Small CRM 3.0. Affected by this vulnerability is an unknown functionality of the component Change Passw launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-260479.
CVE-2024-3767	A vulnerability classified as critical was found in PHPGurukul News Portal 4.1. This vulnerability affects unknown code of the file /admin/edit-post.php. The manipulatior initiated remotely. The exploit has been disclosed to the public and may be used. VDB-260614 is the identifier assigned to this vulnerability.

CVE Number	Description
CVE-2024-3768	A vulnerability, which was classified as critical, has been found in PHPGurukul/itsourcecode News Portal 4.1. This issue affects some unknown processing of the file se injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-2606
CVE-2024-3719	A vulnerability, which was classified as critical, was found in Campcodes House Rental Management System 1.0. This affects an unknown part of the file ajax.php. The initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-260571.
CVE-2024-3803	A vulnerability classified as critical was found in Vesystem Cloud Desktop up to 20240408. This vulnerability affects unknown code of the file /Public/webuploader/0.1.5 unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-26077 not respond in any way.
CVE-2024-3739	A vulnerability classified as critical was found in cym1102 nginxWebUI up to 3.9.9. This vulnerability affects unknown code of the file /adminPage/main/upload. The mar can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-260578 is the identifier assigned to this vulnerability.
CVE-2024-3688	A vulnerability was found in Xiamen Four-Faith RMP Router Management Platform 5.2.2. It has been declared as critical. This vulnerability affects unknown code of the deviceCode=&searchField=&deviceState=. The manipulation of the argument groupId leads to sql injection. The attack can be initiated remotely. The exploit has been vulnerability is VDB-260476. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2024-23558	HCL DevOps Deploy / HCL Launch does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system.
CVE-2024-3797	A vulnerability was found in SourceCodester QR Code Bookmark System 1.0. It has been declared as critical. This vulnerability affects unknown code of the file /endpo argument bookmark leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vuln
CVE-2024-29461	An issue in Floodlight SDN OpenFlow Controller v.1.2 allows a remote attacker to cause a denial of service via the datapath id component.
CVE-2024-3685	A vulnerability, which was classified as critical, was found in DedeCMS 5.7.112-UTF8. Affected is an unknown function of the file stepselect_main.php. The manipulatio attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-260472. NOTE: The vendor was contacted ear
CVE-2021-47189	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix memory ordering between normal and ordered work functions Ordered work functions aren't work functions. The only way execution between normal/ordered functions is synchronized is via the WORK_DONE_BIT, unfortunately the used bitops don't guarantee crashes on ARM64, where async_chunk::inode is seen as non-null in async_cow_submit which causes submit_compressed_extents to be called and crash occurs bec similar to: pc : submit_compressed_extents+0x38/0x3d0 lr : async_cow_submit+0x50/0xd0 sp : ffff800015d4bc20 <registers omitted for brevity> Call trace: submit_com run_ordered_work+0xc8/0x280 btrfs_work_helper+0x98/0x250 process_one_work+0x1f0/0x4ac worker_thread+0x188/0x504 kthread+0x110/0x114 ret_from_fork+0x1 accesses preceding setting of WORK_DONE_BIT are strictly ordered before setting the flag. At the same time add a read barrier after reading of WORK_DONE_BIT in ordered after reading the bit. This in turn ensures are all accesses before WORK_DONE_BIT are going to be strictly ordered before any access that can occur in ordere
CVE-2024-31272	Cross-Site Request Forgery (CSRF) vulnerability in Repute InfoSystems ARForms Form Builder.This issue affects ARForms Form Builder: from n/a through 1.6.1.
CVE-2024-3740	A vulnerability, which was classified as critical, has been found in cym1102 nginxWebUI up to 3.9.9. This issue affects the function exec of the file /adminPage/conf/relo The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-260579.
CVE-2024-30567	An issue in JNT Telecom JNT Liftcom UMS V1.J Core Version JM-V15 allows a remote attacker to execute arbitrary code via the Network Troubleshooting functionality
CVE-2024-3771	A vulnerability was found in PHPGurukul Student Record System 3.20 and classified as critical. Affected by this issue is some unknown functionality of the file /edit-sub leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-260618 is the identifier assigned to thi
CVE-2024-3697	A vulnerability was found in Campcodes House Rental Management System 1.0. It has been classified as critical. Affected is an unknown function of the file manage_te possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-260484.
CVE-2024-3721	A vulnerability was found in TBK DVR-4104 and DVR-4216 up to 20240412 and classified as critical. This issue affects some unknown processing of the file /device.rsp the argument mdb/mdc leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identif
CVE-2024-3804	A vulnerability, which was classified as critical, has been found in Vesystem Cloud Desktop up to 20240408. This issue affects some unknown processing of the file /Pu argument file leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-2607 early about this disclosure but did not respond in any way.
CVE-2023-32295	Missing Authorization vulnerability in Alex Tselegidis Easy!Appointments.This issue affects Easy!Appointments: from n/a through 1.3.3.

CVE Number	Description
CVE-2024-3536	A vulnerability has been found in Campcodes Church Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/delet injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-259906 is the identifier assigned to this vulnerability
CVE-2024-31462	stable-diffusion-webui is a web interface for Stable Diffusion, implemented using Gradio library. Stable-diffusion-webui 1.7.0 is vulnerable to a limited file write affecting modules/ui_extensions.py takes user input into the config_save_name variable on line 653. This user input is later used in the save_config_state method and used to c 67, which leads to a limited file write exploitable on Windows systems. This issue may lead to limited file write. It allows for writing json files anywhere on the server whe
CVE-2024-3737	A vulnerability was found in cym1102 nginxWebUI up to 3.9.9. It has been rated as critical. Affected by this issue is the function findCountByQuery of the file /adminPag traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-260576.
CVE-2024-3720	A vulnerability has been found in Tianwell Fire Intelligent Command Platform 1.1.1.1 and classified as critical. This vulnerability affects unknown code of the file /mfsNot argument gsdwid leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnera
CVE-2024-3698	A vulnerability was found in Campcodes House Rental Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functional leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-260485 was assigned to
CVE-2024-3540	A vulnerability was found in Campcodes Church Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /a leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-259910 is the identifier assigned to thi
CVE-2024-3538	A vulnerability was found in Campcodes Church Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/addTithes possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259908.
CVE-2024-22358	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.20, 7.1 through 7.1.2.16, 7.2 through 7.2.3.9, 7.3 through 7.3.2.4 and IBM DevOps Deploy 8.0 through 8.0.0.1 does no to impersonate another user on the system. IBM X-Force ID: 280896.
CVE-2024-3539	A vulnerability was found in Campcodes Church Management System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of th leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-259909 was assigned to
CVE-2024-3880	A vulnerability has been found in Tenda W30E 1.0.1.25(633) and classified as critical. This vulnerability affects the function formWriteFacMac of the file /goform/WriteFa injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-260914 is the identifier assigned to this vulnerability not respond in any way.
CVE-2024-3696	A vulnerability was found in Campcodes House Rental Management System 1.0 and classified as critical. This issue affects some unknown processing of the file view_ The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-260483.
CVE-2024-3860	An out-of-memory condition during object initialization could result in an empty shape list. If the JIT subsequently traced the object it would crash. This vulnerability affe
CVE-2024-31874	IBM Security Verify Access Appliance 10.0.0 through 10.0.7 uses uninitialized variables when deploying that could allow a local user to cause a denial of service. IBM X
CVE-2024-2397	Due to a bug in packet data buffers management, the PPP printer in tcpdump can enter an infinite loop when reading a crafted DLT_PPP_SERIAL .pcap savefile. This master branch from 2023-06-05 to 2024-03-21.
CVE-2024-22734	An issue was discovered in AMCS Group Trux Waste Management Software before version 7.19.0018.26912, allows local attackers to obtain sensitive information via TruxUser.cfg components.
CVE-2024-31634	Cross Site Scripting (XSS) vulnerability in Xunruicms versions 4.6.3 and before, allows remote attacker to execute arbitrary code via the Security.php file in the catalog
CVE-2024-21036	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a perso Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21024	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a perso Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).

CVE Number	Description
CVE-2024-21025	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21032	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21026	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21031	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21027	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21035	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21034	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21028	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21022	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21029	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21030	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21033	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).

CVE Number	Description
CVE-2024-21023	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-27794	Claris FileMaker Server before version 20.3.2 was susceptible to a reflected Cross-Site Scripting vulnerability due to an improperly handled parameter in the FileMaker Server 20.3.2 by escaping the HTML contents of the login error message on the login page.
CVE-2024-21021	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-1780	The BizCalendar Web plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'tab' parameter in all versions up to, and including, 1.1.0.19 due to ins 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
CVE-2024-23559	HCL DevOps Deploy / Launch is generating an obsolete HTTP header.
CVE-2024-23735	Cross Site Scripting (XSS) vulnerability in in the S/MIME certificate upload functionality of the User Profile pages in savignano S/Notify before 4.0.0 for Confluence allov
CVE-2024-31651	A cross-site scripting (XSS) in Cosmetics and Beauty Product Online Store v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected
CVE-2024-27477	In Leantime 3.0.6, a Cross-Site Scripting vulnerability exists within the ticket creation and modification functionality, allowing attackers to inject malicious JavaScript coc vulnerability can be exploited to perform Server-Side Request Forgery (SSRF) attacks.
CVE-2024-3867	The archive-tainacan-collection theme for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on t 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.
CVE-2024-22359	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.20, 7.1 through 7.1.2.16, 7.2 through 7.2.3.9, 7.3 through 7.3.2.4 and IBM DevOps Deploy 8.0 through 8.0.0.1 are vuln arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 28(
CVE-2024-2857	The Simple Buttons Creator WordPress plugin through 1.04 does not have any authorisation as well as CSRF in its add button function, allowing unauthenticated users lack of sanitisation and escaping, it could also allow them to perform Stored Cross-Site Scripting attacks against logged in admins.
CVE-2024-32489	TCPDF before 6.7.4 mishandles calls that use HTML syntax.
CVE-2024-32634	In huge memory get unmapped area check, code can never be reached because of a logical contradiction.
CVE-2024-21016	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-31652	A cross-site scripting (XSS) in Cosmetics and Beauty Product Online Store v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected
CVE-2024-21018	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).

CVE Number	Description
CVE-2024-21019	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21020	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21037	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-30845	Cross Site Scripting vulnerability in Rainbow external link network disk v.5.5 allows a remote attacker to execute arbitrary code via the validation component of the inpu
CVE-2024-31784	An issue in Typora v.1.8.10 and before, allows a local attacker to obtain sensitive information and execute arbitrary code via a crafted payload to the src component.
CVE-2024-3776	The parameter used in the login page of Netvision airPASS is not properly filtered for user input. An unauthenticated remote attacker can insert JavaScript code to the p
CVE-2024-21017	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2023-44854	Cross Site Scripting (XSS) vulnerability in Cobham SAILOR VSAT Ku v.164B019, allows a remote attacker to execute arbitrary code via a crafted script to the c_set_rs
CVE-2024-21045	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-22717	Cross Site Scripting (XSS) vulnerability in Form Tools 3.1.1 allows attackers to run arbitrary code via the First Name field in the application.
CVE-2024-21072	Vulnerability in the Oracle Installed Base product of Oracle E-Business Suite (component: Data Provider UI). Supported versions that are affected are 12.2.3-12.2.13. E network access via HTTP to compromise Oracle Installed Base. Successful attacks require human interaction from a person other than the attacker and while the vulne additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Installed Base a Oracle Installed Base 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:L
CVE-2024-31648	Cross Site Scripting (XSS) in Insurance Management System v1.0, allows remote attackers to execute arbitrary web scripts or HTML via a crafted payload injected into
CVE-2024-21063	Vulnerability in the PeopleSoft Enterprise HCM Benefits Administration product of Oracle PeopleSoft (component: Benefits Administration). The supported version that attacker with logon to the infrastructure where PeopleSoft Enterprise HCM Benefits Administration executes to compromise PeopleSoft Enterprise HCM Benefits Admir other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all PeopleSoft Enterprise HCM B insert or delete access to some of PeopleSoft Enterprise HCM Benefits Administration accessible data and unauthorized ability to cause a partial denial of service (part 3.1 Base Score 6.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:L/A:L).
CVE-2024-30878	A cross-site scripting (XSS) vulnerability in RageFrame2 v2.6.43, allows remote attackers to execute arbitrary web scripts or HTML and obtain sensitive information via
CVE-2023-44856	Cross Site Scripting (XSS) vulnerability in Cobham SAILOR VSAT Ku v.164B019, allows a remote attacker to execute arbitrary code via a crafted script to the rstat, ser acu_web file.

CVE Number	Description
CVE-2024-21065	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Workflow). Supported versions that are affected are 8.59, 8.60 and 8. network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the attacker and v may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some c unauthorized read access to a subset of PeopleSoft Enterprise PeopleTools accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS V
CVE-2024-30885	Reflected Cross-Site Scripting (XSS) vulnerability in HadSky v7.6.3, allows remote attackers to execute arbitrary code and obtain sensitive information via the chklogin.
CVE-2024-21046	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-30879	Reflected Cross Site Scripting (XSS) vulnerability in RageFrame2 v2.6.43, allows remote attackers to execute arbitrary web scripts or HTML and obtain sensitive inform image cropping function.
CVE-2024-21043	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21039	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21042	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21041	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21040	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21044	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-29220	Ninja Forms prior to 3.8.1 contains a cross-site scripting vulnerability in custom fields for labels. If this vulnerability is exploited, an arbitrary script may be executed on tl product.
CVE-2024-21038	Vulnerability in the Oracle Complex Maintenance, Repair, and Overhaul product of Oracle E-Business Suite (component: LOV). Supported versions that are affected ar attacker with network access via HTTP to compromise Oracle Complex Maintenance, Repair, and Overhaul. Successful attacks require human interaction from a persc Maintenance, Repair, and Overhaul, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthori Maintenance, Repair, and Overhaul accessible data as well as unauthorized read access to a subset of Oracle Complex Maintenance, Repair, and Overhaul accessible CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-24891	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in openEuler kernel on Linux allows Resource Leak Exposure. This vulnerability is associated 1.0-LTS/drivers/staging/gmjstcm/tcm.C. This issue affects kernel: from 4.19.90-2109.1.0.0108 before 4.19.90-2403.4.0.0244.
CVE-2024-24898	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in openEuler kernel on Linux allows Resource Leak Exposure. This vulnerability is associated 1.0-LTS/drivers/staging/gmjstcm/tcm.C. This issue affects kernel: from 4.19.90-2109.1.0.0108 before 4.19.90-2403.4.0.0244.

CVE Number	Description
CVE-2024-30402	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Layer 2 Address Learning Daemon (l2ald) of Juniper Networks Junos OS and Junos OS E of Service (DoS). When telemetry requests are sent to the device, and the Dynamic Rendering Daemon (drend) is suspended, the l2ald crashes and restarts due to fac causes a sustained DoS condition. This issue affects: Junos OS: * All versions earlier than 20.4R3-S10; * 21.2 versions earlier than 21.2R3-S7; * 21.4 versions earlier t earlier than 22.2R3-S3; * 22.3 versions earlier than 22.3R3-S1; * 22.4 versions earlier than 22.4R3; * 23.2 versions earlier than 23.2R1-S2, 23.2R2. Junos OS Evolved: than 22.1R3-S4-EVO; * 22.2-EVO versions earlier than 22.2R3-S3-EVO; * 22.3-EVO versions earlier than 22.3R3-S1-EVO; * 22.4-EVO versions earlier than 22.4R3-E
CVE-2024-27966	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in ExpressTech Quiz And Survey Master allows Stored XSS.This issu
CVE-2024-31361	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in bunny.Net allows Stored XSS.This issue affects bunny.Net: from n/
CVE-2024-31387	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Popup LikeBox Team Popup Like box allows Stored XSS.This issu
CVE-2024-31926	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in BracketSpace Advanced Cron Manager – debug & control allows S control: from n/a through 2.5.2.
CVE-2024-32428	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Moss Web Works MWW Disclaimer Buttons allows Stored XSS.Th
CVE-2024-0157	Dell Storage Resource Manager, 4.9.0.0 and below, contain(s) a Session Fixation Vulnerability in SRM Windows Host Agent. An adjacent network unauthenticated atta targeted user's application session.
CVE-2024-31925	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in FAKTOR VIER F4 Improvements allows Stored XSS.This issue aff
CVE-2024-31929	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Polevaultweb Intagrate Lite allows Stored XSS.This issue affects Ir
CVE-2024-31927	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Aminur Islam WP Login and Logout Redirect allows Stored XSS.Th
CVE-2024-31928	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WP Darko Top Bar allows Stored XSS.This issue affects Top Bar: t
CVE-2023-50949	IBM QRadar SIEM 7.5 could allow an unauthorized user to perform unauthorized actions due to improper certificate validation. IBM X-Force ID: 275706.
CVE-2024-31930	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Pdfcrowd Save as PDF plugin by Pdfcrowd allows Stored XSS.This
CVE-2024-31931	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Save as Image plugin by Pdfcrowd allows Stored XSS.This issue a
CVE-2024-31937	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Visitor Analytics TWIPLA (Visitor Analytics IO) allows Stored XSS.T
CVE-2024-32083	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Varun Kumar Easy Logo allows Stored XSS.This issue affects Eas
CVE-2024-30401	An Out-of-bounds Read vulnerability in the advanced forwarding management process aftman of Juniper Networks Junos OS on MX Series with MPC10E, MPC11, MX attacker to exploit a stack-based buffer overflow, leading to a reboot of the FPC. Through code review, it was determined that the interface definition code for aftman co overflow. This issue affects Junos OS on MX Series and EX9200-15C: * from 21.2 before 21.2R3-S1, * from 21.4 before 21.4R3, * from 22.1 before 22.1R2, * from 22.2 to 20.3R1; * any version of Junos OS 20.4.
CVE-2024-32429	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in WPChill Remove Footer Credit allows Stored XSS.This issue affec

CVE Number	Description
CVE-2024-3859	On 32-bit versions there were integer-overflows that led to an out-of-bounds-read that potentially could be triggered by a malformed OpenType font. This vulnerability a
CVE-2024-31497	In PuTTY 0.68 through 0.80 before 0.81, biased ECDSA nonce generation allows an attacker to recover a user's NIST P-521 secret key via a quick attack in approxima adversary is able to read messages signed by PuTTY or Pageant. The required set of signed messages may be publicly readable because they are stored in a public G signatures were made by Pageant through an agent-forwarding mechanism. In other words, an adversary may already have enough signature information to compromi PuTTY versions. After a key compromise, an adversary may be able to conduct supply-chain attacks on software maintained in Git. A second, independent scenario is authenticates (for remote login or file copy), even though this server is not fully trusted by the victim, and the victim uses the same private key for SSH connections to o (who would otherwise have no way to determine the victim's private key) can derive the victim's private key, and then use it for unauthorized access to those other serv possible to conduct supply-chain attacks on software maintained in Git. This also affects, for example, FileZilla before 3.67.0, WinSCP before 6.3.3, TortoiseGit before
CVE-2024-32453	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in POEditor allows Stored XSS.This issue affects POEditor: from n/a
CVE-2024-3772	Regular expression denial of service in Pydanic < 2.4.0, < 1.10.13 allows remote attackers to cause denial of service via a crafted email string.
CVE-2024-3706	Information exposure vulnerability in OpenGnsys affecting version 1.1.1d (Espeto). This vulnerability allows an attacker to view a php backup file (controlaccess.php-LA
CVE-2024-32080	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Nick Pelton Search Keyword Redirect allows Stored XSS.This issu
CVE-2022-40211	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in GiveWP allows Stored XSS.This issue affects GiveWP: from n/a th
CVE-2024-28402	TOTOLINK X2000R before V1.0.0-B20231213.1013 contains a Stored Cross-site scripting (XSS) vulnerability in IP/Port Filtering under the Firewall Page.
CVE-2024-21109	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.16. Difficult to exploit HTTP to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle V impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2024-30410	An Incorrect Behavior Order in the routing engine (RE) of Juniper Networks Junos OS on EX4300 Series allows traffic intended to the device to reach the RE instead o The intended function is that the lo0 firewall filter takes precedence over the revenue interface firewall filter. This issue affects only IPv6 firewall filter. This issue only af this vulnerability. This issue affects Juniper Networks Junos OS: * All versions before 20.4R3-S10, * from 21.2 before 21.2R3-S7, * from 21.4 before 21.4R3-S6.
CVE-2024-30389	An Incorrect Behavior Order vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on EX4300 Series allows an unauthenticated, network the vulnerable device. When an output firewall filter is applied to an interface it doesn't recognize matching packets but permits any traffic. This issue affects Junos OS affect Junos OS releases earlier than 21.4R1.
CVE-2024-21084	Vulnerability in the Oracle BI Publisher product of Oracle Analytics (component: Service Gateway). Supported versions that are affected are 7.0.0.0.0 and 12.2.1.4.0. E network access via HTTP to compromise Oracle BI Publisher. While the vulnerability is in Oracle BI Publisher, attacks may significantly impact additional products (sco unauthorized read access to a subset of Oracle BI Publisher accessible data. CVSS 3.1 Base Score 5.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L
CVE-2024-32625	In OffloadAMRWriter, a scalar field is not initialized so will contain an arbitrary value left over from earlier computations
CVE-2023-43790	iTop is an IT service management platform. By manipulating HTTP queries, a user can inject malicious content in the fields used for the object friendlyname value. This
CVE-2024-20771	Bridge versions 13.0.6, 14.0.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could levera this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-22526	Buffer Overflow vulnerability in bandisoft bandiview v7.0, allows local attackers to cause a denial of service (DoS) via exr image file.
CVE-2024-30917	An issue was discovered in eProsima FastDDS v.2.14.0 and before, allows a local attacker to cause a denial of service (DoS) and obtain sensitive information via a cra
CVE-2024-20794	Animate versions 23.0.4, 24.0.1 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service. An attacker cou denial of service. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

CVE Number	Description
CVE-2023-52144	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in RexTheme Product Feed Manager.This issue affects Product Feed Manag
CVE-2024-20798	Illustrator versions 28.3, 27.9.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could lever this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-3567	A flaw was found in QEMU. An assertion failure was present in the update_sctp_checksum() function in hw/net/net_tx_pkt.c when trying to calculate the checksum of a crash QEMU and cause a denial of service condition.
CVE-2024-20766	InDesign Desktop versions 18.5.1, 19.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker co Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-30384	An Improper Check for Unusual or Exceptional Conditions vulnerability in the Packet Forwarding Engine (PFE) of Juniper Networks Junos OS on EX4300 Series allows Service (Dos). If a specific CLI command is issued, a PFE crash will occur. This will cause traffic forwarding to be interrupted until the system self-recovers. This issue 21.2R3-S7, 21.4 versions before 21.4R3-S6.
CVE-2024-21015	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior and 8.3.0 and prior. E network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or freque unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (C
CVE-2024-28345	An issue discovered in Sipwise C5 NGCP Dashboard below mr11.5.1 allows a low privileged user to access the Journal endpoint by directly visit the URL.
CVE-2024-20737	After Effects versions 24.1, 23.6.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could le Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2021-47181	In the Linux kernel, the following vulnerability has been resolved: usb: musb: tusb6010: check return value after calling platform_get_resource() It will cause null-ptr-der value.
CVE-2021-47193	In the Linux kernel, the following vulnerability has been resolved: scsi: pm80xx: Fix memory leak during rmmod Driver failed to release all memory allocated. This would the module is removed.
CVE-2024-30406	A Cleartext Storage in a File on Disk vulnerability in Juniper Networks Junos OS Evolved ACX Series devices using the Paragon Active Assurance Test Agent software high privileges to read all other users login credentials. This issue affects only Juniper Networks Junos OS Evolved ACX Series devices using the Paragon Active Assu through 23.2R2-EVO. This issue does not affect releases before 23.1R1-EVO.
CVE-2024-20796	Animate versions 23.0.4, 24.0.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leve of this issue requires user interaction in that a victim must open a malicious file.
CVE-2021-47195	In the Linux kernel, the following vulnerability has been resolved: spi: fix use-after-free of the add_lock mutex Commit 6098475d4cb4 ("spi: Fix deadlock when adding S mutex_unlock() of said lock is called after the controller is already freed: spi_unregister_controller(ctlr) -> put_device(&ctlr->dev) -> spi_controller_release(dev) -> mutex mutex_unlock().
CVE-2024-20770	Photoshop Desktop versions 24.7.2, 25.3.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacke Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-30378	A Use After Free vulnerability in command processing of Juniper Networks Junos OS on MX Series allows a local, authenticated attacker to cause the broadband edge specific CLI commands, creating a Denial of Service (DoS) condition. The process crashes and restarts automatically. When specific CLI commands are executed, the socket) that was already closed, causing the process to crash. This process manages and controls the configuration of broadband subscriber sessions and services. V connect to the device, causing a temporary Denial of Service condition. This issue only occurs if Graceful Routing Engine Switchover (GRES) and Subscriber Managen 20.4R3-S5, * from 21.1 before 21.1R3-S4, * from 21.2 before 21.2R3-S3, * from 21.3 before 21.3R3-S5, * from 21.4 before 21.4R3-S5, * from 22.1 before 22.1R3, * fro
CVE-2024-2666	The Premium Addons for Elementor plugin for WordPress is vulnerable to DOM-Based Stored Cross-Site Scripting via the plugin's Bullet List Widget in all versions up t 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 attempts to edit the content.
CVE-2024-26098	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject m executed in a victim's browser when they browse to the page containing the vulnerable field.
CVE-2024-26046	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject m executed in a victim's browser when they browse to the page containing the vulnerable field.
CVE-2024-26047	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject m executed in a victim's browser when they browse to the page containing the vulnerable field.

CVE Number	Description
CVE-2024-1746	The Testimonial Slider WordPress plugin before 2.3.8 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perfor capability is disallowed (for example in multisite setup)
CVE-2024-26019	Ninja Forms prior to 3.8.1 contains a cross-site scripting vulnerability in submit processing. If this vulnerability is exploited, an arbitrary script may be executed on the w product.
CVE-2024-2731	Users with low privileges (all permissions deselected in the administrator permissions settings) can view certain pages that expose sensitive information such as compa campaigns and their descriptions. In addition, unprivileged users can see and edit the descriptions of tags. At the time of publication of the CVE no patch is available.
CVE-2024-1306	The Smart Forms WordPress plugin before 2.6.94 does not have CSRF checks in some places, which could allow attackers to make logged-in users perform unwantec medium risk.
CVE-2024-1849	The WP Customer Reviews WordPress plugin before 3.7.1 does not validate a parameter allowing contributor and above users to redirect a page to a malicious URL
CVE-2023-6067	The WP User Profile Avatar WordPress plugin through 1.0.1 does not validate and escape some of its shortcode attributes before outputting them back in a page/post v contributor role and above to perform Stored Cross-Site Scripting attacks
CVE-2024-31434	Cross-Site Request Forgery (CSRF) vulnerability in Stefano Lissa & The Newsletter Team Newsletter.This issue affects Newsletter: from n/a through 8.0.6.
CVE-2024-31933	Cross-Site Request Forgery (CSRF) vulnerability in Live Composer Team Page Builder: Live Composer.This issue affects Page Builder: Live Composer: from n/a throu
CVE-2024-30880	Reflected Cross Site Scripting (XSS) vulnerability in RageFrame2 v2.6.43, allows remote attackers to execute arbitrary web scripts or HTML and obtain sensitive inform image cropping function.
CVE-2024-26122	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject m executed in a victim's browser when they browse to the page containing the vulnerable field.
CVE-2024-20780	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject m executed in a victim's browser when they browse to the page containing the vulnerable field.
CVE-2024-26097	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject m executed in a victim's browser when they browse to the page containing the vulnerable field.
CVE-2024-26087	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject m executed in a victim's browser when they browse to the page containing the vulnerable field.
CVE-2024-26084	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject m executed in a victim's browser when they browse to the page containing the vulnerable field.
CVE-2024-26079	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject m executed in a victim's browser when they browse to the page containing the vulnerable field.
CVE-2024-26076	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject m executed in a victim's browser when they browse to the page containing the vulnerable field.
CVE-2024-32103	Cross-Site Request Forgery (CSRF) vulnerability in Siteimprove.This issue affects Siteimprove: from n/a through 2.0.6.
CVE-2024-2733	The Bold Page Builder plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's "Separator" element in all versions up to, and including, 4.8.8 c 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
CVE-2024-31238	Cross-Site Request Forgery (CSRF) vulnerability in Zaytech Smart Online Order for Clover.This issue affects Smart Online Order for Clover: from n/a through 1.5.5.

CVE Number	Description
CVE-2024-20779	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject m executed in a victim's browser when they browse to the page containing the vulnerable field.
CVE-2023-27607	Missing Authorization vulnerability in WP Swings Points and Rewards for WooCommerce.This issue affects Points and Rewards for WooCommerce: from n/a through 1
CVE-2024-25922	Missing Authorization vulnerability in Peach Payments Peach Payments Gateway.This issue affects Peach Payments Gateway: from n/a through 3.1.9.
CVE-2024-2583	The WP Shortcodes Plugin — Shortcodes Ultimate WordPress plugin before 7.0.5 does not properly escape some of its shortcodes attributes before they are echoed b conduct Stored XSS attacks.
CVE-2024-32096	Cross-Site Request Forgery (CSRF) vulnerability in DAEV.Tech WP Migration Plugin DB & Files – WP Synchro.This issue affects WP Migration Plugin DB & Files – WI
CVE-2024-25907	Missing Authorization vulnerability in JoomUnited WP Media folder.This issue affects WP Media folder: from n/a through 5.7.2.
CVE-2024-32093	Cross-Site Request Forgery (CSRF) vulnerability in Nose Graze Novelist.This issue affects Novelist: from n/a through 1.2.2.
CVE-2024-32092	Cross-Site Request Forgery (CSRF) vulnerability in Michael Bester Kimili Flash Embed.This issue affects Kimili Flash Embed: from n/a through 2.5.3.
CVE-2024-32452	Cross-Site Request Forgery (CSRF) vulnerability in WP EasyCart.This issue affects WP EasyCart: from n/a through 5.5.19.
CVE-2023-50307	IBM Sterling B2B Integrator 6.0.0.0 through 6.0.3.9, 6.1.0.0 through 6.1.2.3, and 6.2.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arl functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 273338.
CVE-2024-31389	Cross-Site Request Forgery (CSRF) vulnerability in Ertano MihanPanel.This issue affects MihanPanel: from n/a before 12.7.
CVE-2024-22357	IBM Sterling B2B Integrator 6.0.0.0 through 6.0.3.9, 6.1.0.0 through 6.1.2.3, and 6.2.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arl functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 280894.
CVE-2024-32085	Cross-Site Request Forgery (CSRF) vulnerability in AitThemes Citadela Listing.This issue affects Citadela Listing: from n/a before 5.20.0.
CVE-2024-31941	Cross-Site Request Forgery (CSRF) vulnerability in CodePeople CP Media Player.This issue affects CP Media Player: from n/a through 1.1.3.
CVE-2024-31279	Cross-Site Request Forgery (CSRF) vulnerability in Catch Plugins Generate Child Theme.This issue affects Generate Child Theme: from n/a through 2.0.
CVE-2024-31263	Cross-Site Request Forgery (CSRF) vulnerability in aerin Loan Repayment Calculator and Application Form.This issue affects Loan Repayment Calculator and Applica
CVE-2024-31262	Cross-Site Request Forgery (CSRF) vulnerability in Jcodex WooCommerce Checkout Field Editor (Checkout Manager).This issue affects WooCommerce Checkout Fie
CVE-2024-31649	A cross-site scripting (XSS) in Cosmetics and Beauty Product Online Store v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injecte
CVE-2024-32097	Cross-Site Request Forgery (CSRF) vulnerability in Eyal Fitoussi GEO my WordPress.This issue affects GEO my WordPress: from n/a through 4.1.

CVE Number	Description
CVE-2024-31301	Cross-Site Request Forgery (CSRF) vulnerability in Themeisle Multiple Page Generator Plugin – MPG.This issue affects Multiple Page Generator Plugin – MPG: from r
CVE-2024-31985	XWiki Platform is a generic wiki platform. Starting in version 3.1 and prior to versions 4.10.20, 15.5.4, and 15.10-rc-1, it is possible to schedule/trigger/unschedule existi predictable URL, for example by embedding such an URL in any content as an image. The vulnerability has been fixed in XWiki 14.10.19, 15.5.5, and 15.9. As a worka page.
CVE-2024-31936	Cross-Site Request Forgery (CSRF) vulnerability in AyeCode Ltd UsersWP.This issue affects UsersWP: from n/a before 1.2.6.
CVE-2024-32446	Cross-Site Request Forgery (CSRF) vulnerability in WP Swings Wallet System for WooCommerce.This issue affects Wallet System for WooCommerce: from n/a throug
CVE-2024-21064	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Analytics Web Answers). Supported versions that are affec low privileged attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction fron Business Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unaut Intelligence Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-21070	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Search Framework). Supported versions that are affected are 8.59, 8 attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks require human interaction from a person other than the a unauthorized update, insert or delete access to some of PeopleSoft Enterprise PeopleTools accessible data as well as unauthorized read access to a subset of People (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).
CVE-2020-22540	Stored Cross-Site Scripting (XSS) vulnerability in Codoforum v4.9, allows attackers to execute arbitrary code and obtain sensitive information via crafted payload to Cat
CVE-2024-0881	The Post Grid, Form Maker, Popup Maker, WooCommerce Blocks, Post Blocks, Post Carousel WordPress plugin before 2.2.76 does not have proper authorization, res unauthenticated AJAX actions, allowing unauthenticated users to read such posts
CVE-2024-31425	Cross-Site Request Forgery (CSRF) vulnerability in TMS Amelia.This issue affects Amelia: from n/a through 1.0.95.
CVE-2024-27985	Deserialization of Untrusted Data vulnerability in PropertyHive.This issue affects PropertyHive: from n/a through 2.0.9.
CVE-2024-31932	Cross-Site Request Forgery (CSRF) vulnerability in CreativeThemes Blocksy Companion.This issue affects Blocksy Companion: from n/a through 2.0.28.
CVE-2024-27970	Missing Authorization vulnerability in BogdanFix WP SendFox.This issue affects WP SendFox: from n/a through 1.3.0.
CVE-2024-32445	Cross-Site Request Forgery (CSRF) vulnerability in Saleswonder Team WebinarIgnition.This issue affects WebinarIgnition: from n/a through 3.05.8.
CVE-2024-31378	Cross-Site Request Forgery (CSRF) vulnerability in MailMunch MailChimp Forms by MailMunch.This issue affects MailChimp Forms by MailMunch: from n/a through 3.
CVE-2024-20778	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject m executed in a victim's browser when they browse to the page containing the vulnerable field.
CVE-2024-32449	Cross-Site Request Forgery (CSRF) vulnerability in MagniGenie RestroPress.This issue affects RestroPress: from n/a through 3.1.2.
CVE-2024-21001	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: BI Platform Security). The supported version that is affecte attacker with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks require human interaction from a person oth Intelligence Enterprise Edition, attacks may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized up Enterprise Edition accessible data as well as unauthorized read access to a subset of Oracle Business Intelligence Enterprise Edition accessible data. CVSS 3.1 Base (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N).
CVE-2024-31373	Cross-Site Request Forgery (CSRF) vulnerability in E2Pdf.This issue affects e2pdf: from n/a through 1.20.27.

CVE Number	Description
CVE-2024-31242	Missing Authorization vulnerability in Bricksforge.This issue affects Bricksforge: from n/a through 2.0.17.
CVE-2024-31247	Insertion of Sensitive Information into Log File vulnerability in Frédéric GILLES FG Drupal to WordPress.This issue affects FG Drupal to WordPress: from n/a through 3
CVE-2024-31230	Missing Authorization vulnerability in ShortPixel ShortPixel Adaptive Images.This issue affects ShortPixel Adaptive Images: from n/a through 3.8.2.
CVE-2024-32035	ImageSharp is a 2D graphics API. A vulnerability discovered in the ImageSharp library, where the processing of specially crafted files can lead to excessive memory us attempts to process image files that are designed to exploit this flaw. This flaw can be exploited to cause a denial of service (DoS) by depleting process memory, theret processing tasks. Users and administrators are advised to update to the latest version of ImageSharp that addresses this vulnerability to mitigate the risk of exploitation
CVE-2024-29296	A user enumeration vulnerability was found in Portainer CE 2.19.4. This issue occurs during user authentication process, where a difference in response time could allo not.
CVE-2024-3386	An incorrect string comparison vulnerability in Palo Alto Networks PAN-OS software prevents Predefined Decryption Exclusions from functioning as intended. This can Decryption Exclusions to be unintentionally excluded from decryption.
CVE-2024-31245	Insertion of Sensitive Information into Log File vulnerability in ConvertKit.This issue affects ConvertKit: from n/a through 2.4.5.
CVE-2024-3387	A weak (low bit strength) device certificate in Palo Alto Networks Panorama software enables an attacker to perform a meddler-in-the-middle (MitM) attack to capture e firewalls it manages. With sufficient computing resources, the attacker could break encrypted communication and expose sensitive information that is shared between t
CVE-2024-32036	ImageSharp is a 2D graphics API. A data leakage flaw was found in ImageSharp's JPEG and TGA decoders. This vulnerability is triggered when an attacker passes a s ImageSharp, potentially disclosing sensitive information from other parts of the software in the resulting image buffer. The problem has been patched in v3.1.4 and v2.1
CVE-2024-31432	Missing Authorization vulnerability in StellarWP Restrict Content.This issue affects Restrict Content: from n/a through 3.2.8.
CVE-2024-31249	Insertion of Sensitive Information into Log File vulnerability in WPKube Subscribe To Comments Reloaded.This issue affects Subscribe To Comments Reloaded: from
CVE-2024-2966	The Element Pack Elementor Addons (Header Footer, Template Library, Dynamic Grid & Carousel, Remote Arrows) plugin for WordPress is vulnerable to Sensitive Inf element_pack_ajax_search function. This makes it possible for unauthenticated attackers to extract sensitive data including password protected post details.
CVE-2023-52211	Missing Authorization vulnerability in Automattic WP Job Manager.This issue affects WP Job Manager: from n/a through 2.0.0.
CVE-2024-3707	Information exposure vulnerability in OpenGnsys affecting version 1.1.1d (Espeto). This vulnerability allows an attacker to enumerate all files in the web tree by accessi
CVE-2024-31298	Insertion of Sensitive Information into Log File vulnerability in Joel Hardi User Spam Remover.This issue affects User Spam Remover: from n/a through 1.0.
CVE-2024-31302	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in CodePeople Contact Form Email.This issue affects Contact Form Email: from n/a through 1.
CVE-2024-31353	Insertion of Sensitive Information into Log File vulnerability in Tribulant Slideshow Gallery.This issue affects Slideshow Gallery: from n/a through 1.7.8.
CVE-2024-24850	Missing Authorization vulnerability in Mark Stockton Quicksand Post Filter jQuery Plugin.This issue affects Quicksand Post Filter jQuery Plugin: from n/a through 3.1.1.
CVE-2024-28957	Generation of predictable identifiers issue exists in Cente middleware TCP/IP Network Series. If this vulnerability is exploited, a remote unauthenticated attacker may in device.

CVE Number	Description
CVE-2024-2730	Mautic uses predictable page indices for unpublished landing pages, their content can be accessed by unauthenticated users under public preview URLs which could e available
CVE-2024-21093	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 19.3-19.22 and 21.3-21.13. Difficult to exploit vulnerability privilege with network access via Oracle Net to compromise Java VM. Successful attacks of this vulnerability can result in unauthorized access to critical data or compl (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N).
CVE-2024-28894	Out-of-bounds read vulnerability caused by improper checking of the option length values in IPv6 headers exists in Cente middleware TCP/IP Network Series, which m sending a specially crafted packet.
CVE-2024-21117	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Core). Supported versions that are affected are 8.5.6 ar with logon to the infrastructure where Oracle Outside In Technology executes to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to ca Technology. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).
CVE-2024-21118	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Core). Supported versions that are affected are 8.5.6 ar with logon to the infrastructure where Oracle Outside In Technology executes to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to ca Technology. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).
CVE-2024-21119	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Core). Supported versions that are affected are 8.5.6 ar with logon to the infrastructure where Oracle Outside In Technology executes to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to ca Technology. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).
CVE-2024-21120	Vulnerability in the Oracle Outside In Technology product of Oracle Fusion Middleware (component: Outside In Core). Supported versions that are affected are 8.5.6 ar with logon to the infrastructure where Oracle Outside In Technology executes to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to ca Technology. CVSS 3.1 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).
CVE-2024-21590	An Improper Input Validation vulnerability in Juniper Tunnel Driver (jtd) and ICMP module of Juniper Networks Junos OS Evolved allows an unauthenticated attacker w to the Routing Engine (RE) to cause a Denial of Service (DoS). When specifically crafted transit MPLS IPv4 packets are received by the Packet Forwarding Engine (PI of these packets may create a sustained Denial of Service (DoS) condition. This issue affects Juniper Networks Junos OS: * All versions before 21.2R3-S8-EVO; * from EVO; * from 22.3-EVO before 22.3R3-S3-EVO; * from 22.4-EVO before 22.4R3-EVO; * from 23.2-EVO before 23.2R2-EVO. * from 23.4-EVO before 23.4R1-S1-EVO.
CVE-2023-45503	SQL Injection vulnerability in Macrob7 Macs CMS 1.1.4f, allows remote attackers to execute arbitrary code, cause a denial of service (DoS), escalate privileges, and ob forgotPasswordProcess, saveUser, saveRole, deleteUser, deleteRole, deleteComment, deleteUser, allowComment, saveRole, forgotPasswordProcess, resetPasswor
CVE-2024-1481	A flaw was found in FreeIPA. This issue may allow a remote attacker to craft a HTTP request with parameters that can be interpreted as command arguments to kinit o
CVE-2024-30409	An Improper Check for Unusual or Exceptional Conditions vulnerability in telemetry processing of Juniper Networks Junos OS and Junos OS Evolved allows a network telemetry daemon (fibtd) to crash, leading to a limited Denial of Service. This issue affects Juniper Networks Junos OS: * from 22.1 before 22.1R1-S2, 22.1R2. Junos (
CVE-2024-23083	Time4J Base v5.9.3 was discovered to contain a NullPointerException via the component net.time4j.format.internal.FormatUtils::useDefaultWeekmodel(Locale). NOTE reasonable evidence to determine the existence of a vulnerability. The submission may have been based on a tool that is not sufficiently robust for vulnerability identific
CVE-2021-47192	In the Linux kernel, the following vulnerability has been resolved: scsi: core: sysfs: Fix hang when device state is set via sysfs This fixes a regression added with: comm device") The problem is that after iSCSI recovery, iscsid will call into the kernel to set the dev's state to running, and with that patch we now call scsi_rescan_device() w to test the device in scsi_send_eh_cmnd() then it's going to try to grab the state_mutex. We are then stuck, because when scsi_rescan_device() tries to send its I/O scs scsi_host_in_recovery() which will return true (the host state is still in recovery) and I/O will just be requeued. scsi_send_eh_cmnd() will then never be able to grab the rescan-related code to after we drop the state_mutex. This also adds a check for if we are already in the running state. This prevents extra scans and helps the iscsid c recovery process then we don't need userspace to do it again plus possibly block that daemon.
CVE-2024-3775	aEnrich Technology a+HRD's functionality for downloading files using youtube-dl.exe does not properly restrict user input. This allows attackers to pass arbitrary argum files.
CVE-2024-3774	aEnrich Technology a+HRD's functionality for front-end retrieval of system configuration values lacks proper restrictions on a specific parameter, allowing attackers to r values.
CVE-2024-31451	DocsGPT is a GPT-powered chat for documentation. DocsGPT is vulnerable to unauthenticated limited file write in routes.py. This vulnerability is fixed in 0.8.1.
CVE-2024-3862	The MarkStack assignment operator, part of the JavaScript engine, could access uninitialized memory if it were used in a self-assignment. This vulnerability affects Fire

CVE Number	Description
CVE-2024-3235	The Essential Grid Gallery WordPress Plugin plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.1.1 via the on_ attackers to view private and password protected posts that may have private or sensitive information.
CVE-2024-30390	An Improper Restriction of Excessive Authentication Attempts vulnerability in Juniper Networks Junos OS Evolved allows an unauthenticated, network-based attacker t When an incoming connection was blocked because it exceeded the connections-per-second rate-limit, the system doesn't consider existing connections anymore for s exceeded. This issue affects Junos OS Evolved: * All versions before 21.4R3-S4-EVO, * 22.1-EVO versions before 22.1R3-S3-EVO, * 22.2-EVO versions before 22.2F
CVE-2024-20990	Vulnerability in the Oracle Applications Technology product of Oracle E-Business Suite (component: Templates). Supported versions that are affected are 12.2.3-12.2.1 network access via HTTP to compromise Oracle Applications Technology. Successful attacks of this vulnerability can result in unauthorized read access to a subset of 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).
CVE-2024-30386	A Use-After-Free vulnerability in the Layer 2 Address Learning Daemon (l2ald) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated, adjac In an EVPN-VXLAN scenario, when state updates are received and processed by the affected system, the correct order of some processing steps is not ensured, whicl depends on system internal timing which is outside the attackers control. This issue affects: Junos OS: * All versions before 20.4R3-S8, * 21.2 versions before 21.2R3- S4, * 22.1 versions before 22.1R3-S3, * 22.2 versions before 22.2R3-S1, * 22.3 versions before 22.3R3,, * 22.4 versions before 22.4R2; Junos OS Evolved: * All versi EVO, * 21.3-EVO versions before 21.3R3-S5-EVO, * 21.4-EVO versions before 21.4R3-S4-EVO, * 22.1-EVO versions before 22.1R3-S3-EVO, * 22.2-EVO versions be EVO versions before 22.4R2-EVO.
CVE-2024-20991	Vulnerability in the Oracle HTTP Server product of Oracle Fusion Middleware (component: Web Listener). The supported version that is affected is 12.2.1.4.0. Easily ex access via HTTP to compromise Oracle HTTP Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle HTTP Serve CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2024-20994	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.36 and prior and 8 attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a h 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).
CVE-2024-23734	Cross Site Request Forgery vulnerability in in the upload functionality of the User Profile pages in savignano S/Notify before 2.0.1 for Bitbucket allow attackers to replac
CVE-2024-30656	An issue in Fireboltt Dream Wristphone BSW202_FB_AAC_v2.0_20240110-20240110-1956 allows attackers to cause a Denial of Service (DoS) via a crafted deauth fr
CVE-2023-38511	iTop is an IT service management platform. Dashboard editor : can load multiple files and URL, and full path disclosure on dashboard config file. This vulnerability is fix
CVE-2024-3448	Users with low privileges can perform certain AJAX actions. In this vulnerability instance, improper access to ajax?action=plugin:focus:checkIframeAvailability leads to a returned from the back-end. Allowing an attacker to perform a port scan in the back-end. At the time of publication of the CVE no patch is available.
CVE-2024-21615	An Incorrect Default Permissions vulnerability in Juniper Networks Junos OS and Junos OS Evolved allows a local, low-privileged attacker to access confidential inform when NETCONF traceoptions are configured, and a super-user performs specific actions via NETCONF, then a low-privileged user can access sensitive information cc OS: * all versions before 21.2R3-S7, * from 21.4 before 21.4R3-S5, * from 22.1 before 22.1R3-S5, * from 22.2 before 22.2R3-S3, * from 22.3 before 22.3R3-S2, * fr Evolved: * all versions before 21.2R3-S7-EVO, * from 21.3 before 21.3R3-S5-EVO, * from 21.4 before 21.4R3-S5-EVO, * from 22.1 before 22.1R3-S5-EVO, * from 2 22.4 before 22.4R3-EVO, * from 23.2 before 23.2R1-S2.
CVE-2024-20993	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior and 8.2.0 and p network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or freque 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).
CVE-2024-21060	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Data Dictionary). Supported versions that are affected are 8.0.36 and prior and 8.3.0 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 fr 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).
CVE-2024-21009	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and p network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or freque 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).
CVE-2024-21055	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior. Easily exploitab multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable cras (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2024-21052	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vu multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable cras (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2024-21056	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vu multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable cras (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2024-21051	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vu multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable cras (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVE Number	Description
CVE-2024-21050	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vu multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable cras (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2024-21049	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vu multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable cras (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2024-21047	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. Easily access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repe 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).
CVE-2024-21057	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.35 and prior. Easily exploitab multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable cras (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2024-21058	Vulnerability in the Unified Audit component of Oracle Database Server. Supported versions that are affected are 19.3-19.22 and 21.3-21.13. Easily exploitable vulnera network access via Oracle Net to compromise Unified Audit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access 4.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:N).
CVE-2024-21053	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.34 and prior. Easily exploitable vu multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable cras (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2024-21054	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and p network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or freque 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).
CVE-2024-20998	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and p network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or freque 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).
CVE-2024-21061	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 8.0.35 and prior and 8.2.0 an network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or freque 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).
CVE-2024-21062	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and p network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or freque 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).
CVE-2024-21069	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and prior. E network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or freque 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).
CVE-2024-21087	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.36 and prior a attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a h 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).
CVE-2024-1310	The WooCommerce WordPress plugin before 8.6 does not prevent users with at least the contributor role from leaking products they shouldn't have access to. (e.g. pri
CVE-2024-21096	Vulnerability in the MySQL Server product of Oracle MySQL (component: Client: mysqldump). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, inse unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CV impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L).
CVE-2024-21097	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Security). Supported versions that are affected are 8.59, 8.60 and 8.6 network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in unauthorized access to critical data o data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).
CVE-2024-21102	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Thread Pooling). Supported versions that are affected are 8.0.36 and prior and 8.3.0 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 fr 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).
CVE-2024-31990	Argo CD is a declarative, GitOps continuous delivery tool for Kubernetes. The API server does not enforce project sourceNamespaces which allows attackers to use th vulenrability is fixed in 2.10.7, 2.9.12, and 2.8.16.
CVE-2023-44853	\An issue was discovered in Cobham SAILOR VSAT Ku v.164B019, allows a remote attacker to execute arbitrary code via a crafted script to the sub_219C4 function in
CVE-2023-45186	IBM Sterling B2B Integrator 6.0.0.0 through 6.0.3.9, 6.1.0.0 through 6.1.2.3, and 6.2.0.0 is vulnerable to cross-site scripting. This vulnerability allows a privileged user to intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 268691.

CVE Number	Description
CVE-2023-47714	IBM Sterling File Gateway 6.0.0.0 through 6.0.3.9, 6.1.0.0 through 6.1.2.3, and 6.2.0.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbi functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 271531.
CVE-2024-31839	Cross Site Scripting vulnerability in tiagorlampert CHAOS v.5.0.1 allows a remote attacker to escalate privileges via the sendCommandHandler function in the handler.g
CVE-2024-30391	A Missing Authentication for Critical Function vulnerability in the Packet Forwarding Engine (pfe) of Juniper Networks Junos OS on MX Series with SPC3, and SRX Ser impact to the integrity or availability of the device. If a device is configured with IPsec authentication algorithm hmac-sha-384 or hmac-sha-512, tunnels are established is sent with the encrypted data on egress, and no authentication information is expected on ingress. So if the peer is an unaffected device transit traffic is going to fail in works, but without authentication, and configuration and CLI operational commands indicate authentication is performed. This issue affects Junos OS: * All versions bef 21.2R2-S1, 21.2R3, * 21.3 versions before 21.3R1-S2, 21.3R2.
CVE-2024-1660	The Top Bar WordPress plugin before 3.0.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored (disallowed (for example in multisite setup)
CVE-2024-2836	The Social Share, Social Login and Social Comments Plugin WordPress plugin before 7.13.64 does not sanitise and escape some of its settings, which could allow hig even when unfiltered_html is disallowed
CVE-2024-2858	The Simple Buttons Creator WordPress plugin through 1.04 does not have CSRF checks in some places, which could allow attackers to make logged in users perform
CVE-2024-27476	Leantime 3.0.6 is vulnerable to HTML Injection via /dashboard/show#/tickets/newTicket.
CVE-2024-32129	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Freshworks Freshdesk (official).This issue affects Freshdesk (official): from n/a through 2.3.6.
CVE-2024-31282	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Appcheap.Io App Builder.This issue affects App Builder: from n/a through 3.8.7.
CVE-2024-31253	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in WP OAuth Server OAuth Server.This issue affects OAuth Server: from n/a through 4.3.3.
CVE-2024-2428	The Ultimate Video Player For WordPress WordPress plugin before 2.2.3 does not have proper capability check when updating its settings via a REST route, allowing (lack of escaping in one of the settings, this also allows them to perform Stored XSS attacks
CVE-2024-21081	Vulnerability in the Oracle Partner Management product of Oracle E-Business Suite (component: Attribute Admin Setup). Supported versions that are affected are 12.2 attacker with network access via HTTP to compromise Oracle Partner Management. Successful attacks require human interaction from a person other than the attacke may significantly impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some c 4.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:L/A:N).
CVE-2024-22448	Dell BIOS contains an Out-of-Bounds Write vulnerability. A local authenticated malicious user with admin privileges could potentially exploit this vulnerability, leading to
CVE-2024-3617	A vulnerability, which was classified as critical, has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0. This issue affects some unkno 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 identifier VDB-26027
CVE-2024-31760	An issue in sanluan flipped-aurora gin-vue-admin 2.4.x allows an attacker to escalate privileges via the Session Expiration component.
CVE-2024-1754	The NPS computy WordPress plugin through 2.7.5 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform S capability is disallowed (for example in multisite setup)
CVE-2024-3618	A vulnerability, which was classified as critical, was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. Affected is an unknown function of leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-260274 is the identifier assigned t
CVE-2024-3619	A vulnerability has been found in SourceCodester Kortex Lite Advocate Office Management System 1.0 and classified as critical. Affected by this vulnerability is an unk manipulation of the argument cname leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The as

CVE Number	Description
CVE-2024-3620	A vulnerability was found in SourceCodester Kortex Lite Advocate Office Management System 1.0 and classified as critical. Affected by this issue is some unknown fun name/gender/dob/email/mobile/address leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Th
CVE-2024-3621	A vulnerability was found in SourceCodester Kortex Lite Advocate Office Management System 1.0. It has been classified as critical. This affects an unknown part of the title/case_no/client_name/court/case_type/case_stage/legel_acts/description/filling_date/hearing_date/opposite_lawyer/total_fees/unpaid leads to sql injection. It is pos public and may be used. The identifier VDB-260277 was assigned to this vulnerability.
CVE-2024-30883	Reflected Cross Site Scripting (XSS) vulnerability in RageFrame2 v2.6.43, allows remote attackers to execute arbitrary web scripts or HTML and obtain sensitive inform the image cropping function.
CVE-2024-1712	The Carousel Slider WordPress plugin before 2.2.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform capability is disallowed (for example in multisite setup)
CVE-2023-32228	A firmware bug which may lead to misinterpretation of data in the AMC2-4WCF and AMC2-2WCF allowing an adversary to grant access to the last authorized user.
CVE-2021-47185	In the Linux kernel, the following vulnerability has been resolved: tty: tty_buffer: Fix the softlockup issue in flush_to_ldisc When running ltp testcase(ltp/testcases/kernel Workqueue: events_unbound flush_to_ldisc Call trace: dump_backtrace+0x0/0x1ec show_stack+0x24/0x30 dump_stack+0xd0/0x128 panic+0x15c/0x374 watchdog_ti __hrtimer_run_queues+0xa4/0x120 hrtimer_interrupt+0xfc/0x270 arch_timer_handler_phys+0x40/0x50 handle_percpu_devid_irq+0x94/0x220 __handle_domain_irq+0 slip_unesc+0x80/0x214 [slip] tty_ldisc_receive_buf+0x64/0x80 tty_port_default_receive_buf+0x50/0x90 flush_to_ldisc+0xbc/0x110 process_one_work+0x1d4/0x4b0 w The first process call the write syscall to send data to the pty master. At the same time, the workqueue will do the flush_to_ldisc to pop data in a loop until there is no m the sender sends data fastly in full time which will result in workqueue doing work in loop for a long time and occuring softlockup in flush_to_ldisc with kernel configured the flush_to_ldisc loop to avoid it.
CVE-2023-6494	The WPC Smart Quick View for WooCommerce plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including 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 installations where unfiltered_html has been disabled.
CVE-2024-21008	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and p network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or freque 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).
CVE-2024-21013	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.36 and prior and 8.3.0 and p network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or freque 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).
CVE-2024-20992	Vulnerability in the Oracle WebCenter Portal product of Oracle Fusion Middleware (component: Content integration). The supported version that is affected is 12.2.1.4.(network access via HTTP to compromise Oracle WebCenter Portal. Successful attacks require human interaction from a person other than the attacker and while the v impact additional products (scope change). Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebCer subset of Oracle WebCenter Portal accessible data. CVSS 3.1 Base Score 4.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S
CVE-2024-32430	Server-Side Request Forgery (SSRF) vulnerability in ActiveCampaign.This issue affects ActiveCampaign: from n/a through 8.1.14.
CVE-2024-23560	HCL DevOps Deploy / HCL Launch could be vulnerable to incomplete revocation of permissions when deleting a custom security resource type.
CVE-2024-32454	Server-Side Request Forgery (SSRF) vulnerability in Wappointment Appointment Bookings for Zoom GoogleMeet and more – Wappointment.This issue affects Appoin n/a through 2.6.0.
CVE-2024-32431	Deserialization of Untrusted Data vulnerability in WP All Import Import Users from CSV.This issue affects Import Users from CSV: from n/a through 1.2.
CVE-2024-22334	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.20, 7.1 through 7.1.2.16, 7.2 through 7.2.3.9, 7.3 through 7.3.2.4 and IBM DevOps Deploy 8.0 through 8.0.0.1 could b custom security resource type. When deleting a custom security type, associated permissions of objects using that type may not be fully revoked. This could lead to inc being retained. IBM X-Force ID: 279974.
CVE-2024-31364	Cross-Site Request Forgery (CSRF) vulnerability in ELEXtensions ELEX WooCommerce Dynamic Pricing and Discounts.This issue affects ELEX WooCommerce Dyna
CVE-2024-3686	A vulnerability has been found in DedeCMS 5.7.112-UTF8 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file update_gui '../filedir'. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-260473 was assigned to this vulneral did not respond in any way.
CVE-2023-51499	Missing Authorization vulnerability in WooCommerce WooCommerce Shipping Per Product.This issue affects WooCommerce Shipping Per Product: from n/a through 2

CVE Number	Description
CVE-2024-31363	Cross-Site Request Forgery (CSRF) vulnerability in LifterLMS.This issue affects LifterLMS: from n/a through 7.5.0.
CVE-2024-31362	Cross-Site Request Forgery (CSRF) vulnerability in Metagauss ProfileGrid.This issue affects ProfileGrid : from n/a through 5.7.8.
CVE-2024-31995	`@digitalbazaar/zcap` provides JavaScript reference implementation for Authorization Capabilities. Prior to version 9.0.1, when invoking a capability with a chain depth property is not properly checked against the current date or other `date` param. This can allow invocations outside of the original intended time period. A zcap still cann material. `@digitalbazaar/zcap` v9.0.1 fixes expiration checking. As a workaround, one may revoke a zcap at any time.
CVE-2024-21610	An Improper Handling of Exceptional Conditions vulnerability in the Class of Service daemon (cosd) of Juniper Networks Junos OS on MX Series allows an authenticat of Service (DoS). In a scaled subscriber scenario when specific low privileged commands, received over NETCONF, SSH or telnet, are handled by cosd on behalf of m stuck. In case of (Netconf over) SSH this leads to stuck SSH sessions, so that when the connection-limit for SSH is reached new sessions can't be established anymor be monitored by executing the following command: user@host> show system processes extensive | match mgd | match sbwait This issue affects Juniper Networks Ju versions earlier than 21.2R3-S7; 21.3 versions earlier than 21.3R3-S5; 21.4 versions earlier than 21.4R3-S5; 22.1 versions earlier than 22.1R3-S4; 22.2 versions earlie earlier than 22.4R3; 23.2 versions earlier than 23.2R1-S2, 23.2R2.
CVE-2024-31939	Cross-Site Request Forgery (CSRF) vulnerability in Soflyy Import any XML or CSV File to WordPress.This issue affects Import any XML or CSV File to WordPress: fror
CVE-2024-31430	Cross-Site Request Forgery (CSRF) vulnerability in realmag777 WOLF – WordPress Posts Bulk Editor and Manager Professional, realmag777 BEAR – Bulk Editor and Pluginus.Net.This issue affects WOLF – WordPress Posts Bulk Editor and Manager Professional: from n/a through 1.0.8.1; BEAR – Bulk Editor and Products Manager 1.1.4.1.
CVE-2024-31386	Cross-Site Request Forgery (CSRF) vulnerability in Hidekazu Ishikawa X-T9, Hidekazu Ishikawa Lightning, themeinwp Default Mag, Out the Box Namaha, Out the Box Decode, Wayneconnor Sliding Door, Out the Box Shopstar!, Modernthemesnet Gridsby, TT Themes HappenStance, Marsian i-excel, Out the Box Panoramic, Moderntl Lightning: from n/a through 15.18.0; Default Mag: from n/a through 1.3.5; Namaha: from n/a through 1.0.40; CityLogic: from n/a through 1.1.29; i-max: from n/a through 3.15.3; Sliding Door: from n/a through 3.3; Shopstar!: from n/a through 1.1.33; Gridsby: from n/a through 1.3.0; HappenStance: from n/a through 3.0.1; i-excel: from n/a n/a through 1.3.1.
CVE-2024-3662	The WPZOOM Social Feed Widget & Block plugin for WordPress is vulnerable to unauthorized access due to a missing capability check on the wpzoom_instagram_cle makes it possible for authenticated attackers, with subscriber-level access and above, to delete all Instagram images installed on the site.
CVE-2024-22339	IBM UrbanCode Deploy (UCD) 7.0 through 7.0.5.20, 7.1 through 7.1.2.16, 7.2 through 7.2.3.9, 7.3 through 7.3.2.4 and IBM DevOps Deploy 8.0 through 8.0.0.1 is vulne sensitive values from some log files. IBM X-Force ID: 279979.
CVE-2024-32000	matrix-appservice-irc is a Node.js IRC bridge for the Matrix messaging protocol. matrix-appservice-irc before version 2.0.0 can be exploited to leak the truncated body c don't have access to. As a precondition to the attack, the malicious user needs to know the event ID of the message they want to leak, as well as to be joined to both th containing the leaked message content is visible to IRC channel members when this happens. matrix-appservice-irc 2.0.0 checks whether the user has permission to v to this version. It's possible to limit the amount of information leaked by setting a reply template that doesn't contain the original message. See these lines `601-604` in t
CVE-2024-32455	Missing Authorization vulnerability in Very Good Plugins Fatal Error Notify.This issue affects Fatal Error Notify: from n/a through 1.5.2.
CVE-2024-3873	A vulnerability was found in SMI SMI-EX-5414W up to 1.0.03. It has been classified as problematic. This affects an unknown part of the component Web Interface. The the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-260907.
CVE-2024-31354	Cross-Site Request Forgery (CSRF) vulnerability in Tribulant Slideshow Gallery.This issue affects Slideshow Gallery: from n/a through 1.7.8.
CVE-2024-3736	A vulnerability was found in cym1102 nginxWebUI up to 3.9.9. It has been declared as problematic. Affected by this vulnerability is the function upload of the file /admin attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-260575.
CVE-2024-3869	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 'woocommerce_ with subscriber level access to view coupon codes.
CVE-2024-3243	The Customer Reviews for WooCommerce plugin for WordPress is vulnerable to unauthorized email sending due to a missing capability check on the send_test_email possible for authenticated attackers, with subscriber-level access and above, to send arbitrary test emails.
CVE-2024-31924	Cross-Site Request Forgery (CSRF) vulnerability in Exactly WWW EWWW Image Optimizer.This issue affects EWWW Image Optimizer: from n/a through 7.2.3.
CVE-2024-1204	The Meta Box WordPress plugin before 5.9.4 does not prevent users with at least the contributor role from access arbitrary custom fields assigned to other user's posts

CVE Number	Description
CVE-2024-31944	Cross-Site Request Forgery (CSRF) vulnerability in Octolize WooCommerce UPS Shipping – Live Rates and Access Points.This issue affects WooCommerce UPS Sh
CVE-2024-31943	Cross-Site Request Forgery (CSRF) vulnerability in Octolize USPS Shipping for WooCommerce – Live Rates.This issue affects USPS Shipping for WooCommerce – L
CVE-2024-23561	HCL DevOps Deploy / HCL Launch is vulnerable to sensitive information disclosure vulnerability due to insufficient obfuscation of sensitive values.
CVE-2024-31360	Cross-Site Request Forgery (CSRF) vulnerability in Coded Commerce, LLC Benchmark Email Lite.This issue affects Benchmark Email Lite: from n/a through 4.1.
CVE-2024-32437	Cross-Site Request Forgery (CSRF) vulnerability in impleCode eCommerce Product Catalog.This issue affects eCommerce Product Catalog: from n/a through 3.3.28.
CVE-2024-31305	Cross-Site Request Forgery (CSRF) vulnerability in rtCamp Transcoder.This issue affects Transcoder: from n/a through 1.3.5.
CVE-2024-32106	Cross-Site Request Forgery (CSRF) vulnerability in WP Compress WP Compress – Image Optimizer [All-In-One].This issue affects WP Compress – Image Optimizer [
CVE-2024-25935	Missing Authorization vulnerability in Metagauss RegistrationMagic.This issue affects RegistrationMagic: from n/a through 5.2.5.9.
CVE-2024-27967	Cross-Site Request Forgery (CSRF) vulnerability in Michael Leithold DSGVO All in one for WP.This issue affects DSGVO All in one for WP: from n/a through 4.3.
CVE-2024-32105	Cross-Site Request Forgery (CSRF) vulnerability in ELEXtensions ELEX WooCommerce Dynamic Pricing and Discounts.This issue affects ELEX WooCommerce Dyna
CVE-2024-32109	Cross-Site Request Forgery (CSRF) vulnerability in Julien Berthelot / MPEmbed.Com WP Matterport Shortcode allows Cross Site Request Forgery.This issue affects W
CVE-2024-32108	Cross-Site Request Forgery (CSRF) vulnerability in Stephanie Leary Convert Post Types.This issue affects Convert Post Types: from n/a through 1.4.
CVE-2024-32107	Cross-Site Request Forgery (CSRF) vulnerability in XLPlugins Finale Lite.This issue affects Finale Lite: from n/a through 2.18.0.
CVE-2024-31935	Cross-Site Request Forgery (CSRF) vulnerability in BracketSpace Simple Post Notes.This issue affects Simple Post Notes: from n/a through 1.7.6.
CVE-2024-27592	Open Redirect vulnerability in Corezoid Process Engine v6.5.0 allows attackers to redirect to arbitrary websites via appending a crafted link to /login/ in the login page U
CVE-2024-31934	Cross-Site Request Forgery (CSRF) vulnerability in Link Whisper Link Whisper Free.This issue affects Link Whisper Free: from n/a through 0.6.9.
CVE-2024-32112	Cross-Site Request Forgery (CSRF) vulnerability in Leadinfo leadinfo. The patch was released under the same version which was reported as vulnerable. We consider through 1.0.
CVE-2024-30915	An issue was discovered in OpenDDS commit b1c534032bb62ad4ae32609778de6b8d6c823a66, allows a local attacker to cause a denial of service and obtain sensiti DataReaderQoS component.
CVE-2024-21086	Vulnerability in the Oracle CRM Technical Foundation product of Oracle E-Business Suite (component: Preferences). Supported versions that are affected are 12.2.3-1 with network access via HTTP to compromise Oracle CRM Technical Foundation. Successful attacks require human interaction from a person other than the attacker. S insert or delete access to some of Oracle CRM Technical Foundation accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC

CVE Number	Description
CVE-2024-21099	Vulnerability in the Oracle Business Intelligence Enterprise Edition product of Oracle Analytics (component: Data Visualization). The supported version that is affected i with network access via HTTP to compromise Oracle Business Intelligence Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read ac 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).
CVE-2024-29402	cskefu v7 suffers from Insufficient Session Expiration, which allows attackers to exploit the old session for malicious activity.
CVE-2024-25908	Missing Authorization vulnerability in JoomUnited WP Media folder.This issue affects WP Media folder: from n/a through 5.7.2.
CVE-2024-24883	Missing Authorization vulnerability in BdThemes Prime Slider – Addons For Elementor.This issue affects Prime Slider – Addons For Elementor: from n/a through 3.11.1
CVE-2024-31303	Cross-Site Request Forgery (CSRF) vulnerability in Fetch Designs Sign-up Sheets.This issue affects Sign-up Sheets: from n/a through 2.2.11.1.
CVE-2024-31250	Cross-Site Request Forgery (CSRF) vulnerability in Saumya Majumder WP Server Health Stats.This issue affects WP Server Health Stats: from n/a through 1.7.3.
CVE-2024-31293	Cross-Site Request Forgery (CSRF) vulnerability in Easy Digital Downloads.This issue affects Easy Digital Downloads: from n/a through 3.2.6.
CVE-2024-31271	Cross-Site Request Forgery (CSRF) vulnerability in Supsystic Ultimate Maps by Supsystic.This issue affects Ultimate Maps by Supsystic: from n/a through 1.2.16.
CVE-2024-31269	Cross-Site Request Forgery (CSRF) vulnerability in Supsystic Easy Google Maps.This issue affects Easy Google Maps: from n/a through 1.11.11.
CVE-2024-31268	Cross-Site Request Forgery (CSRF) vulnerability in AppPresser Team AppPresser.This issue affects AppPresser: from n/a through 4.3.0.
CVE-2024-31264	Unauthenticated Cross Site Request Forgery (CSRF) in Post Views Counter <= 1.4.4 versions.
CVE-2024-31251	Cross-Site Request Forgery (CSRF) vulnerability in PeepSo Community by PeepSo.This issue affects Community by PeepSo: from n/a through 6.3.1.1.
CVE-2024-31239	Cross-Site Request Forgery (CSRF) vulnerability in Nudgify Nudgify Social Proof, Sales Popup & FOMO.This issue affects Nudgify Social Proof, Sales Popup & FOMO
CVE-2023-6489	A denial of service vulnerability was identified in GitLab CE/EE, versions 16.7.7 prior to 16.8.6, 16.9 prior to 16.9.4 and 16.10 prior to 16.10.2 which allows an attacker t degradation via chat integration feature.
CVE-2024-31235	Cross-Site Request Forgery (CSRF) vulnerability in WebToffee WordPress Comments Import & Export.This issue affects WordPress Comments Import & Export: from
CVE-2024-31372	Cross-Site Request Forgery (CSRF) vulnerability in Arnan de Gans No-Bot Registration.This issue affects No-Bot Registration: from n/a through 1.9.1.
CVE-2024-31371	Cross-Site Request Forgery (CSRF) vulnerability in Xylus Themes WP Event Aggregator.This issue affects WP Event Aggregator: from n/a through 1.7.6.
CVE-2024-21048	Vulnerability in the Oracle Web Applications Desktop Integrator product of Oracle E-Business Suite (component: XML input). Supported versions that are affected are 1 attacker with network access via HTTP to compromise Oracle Web Applications Desktop Integrator. Successful attacks of this vulnerability can result in unauthorized re 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).
CVE-2022-47604	Missing Authorization vulnerability in junkcoder, ristoniinemets AJAX Thumbnail Rebuild.This issue affects AJAX Thumbnail Rebuild: from n/a through 1.13.

CVE Number	Description
CVE-2023-6678	An issue has been discovered in GitLab EE affecting all versions before 16.8.6, all versions starting from 16.9 before 16.9.4, all versions starting from 16.10 before 16.1 malicious crafted content in a junit test report file.
CVE-2024-31289	Cross-Site Request Forgery (CSRF) vulnerability in Elementor Hello Elementor.This issue affects Hello Elementor: from n/a through 3.0.0.
CVE-2024-32436	Cross-Site Request Forgery (CSRF) vulnerability in Codemenschen Gift Vouchers.This issue affects Gift Vouchers: from n/a through 4.4.0.
CVE-2024-31384	Cross-Site Request Forgery (CSRF) vulnerability in Rara Theme Spa and Salon.This issue affects Spa and Salon: from n/a through 1.2.7.
CVE-2024-31379	Cross-Site Request Forgery (CSRF) vulnerability in Smash Balloon Smash Balloon Social Post Feed.This issue affects Smash Balloon Social Post Feed: from n/a throu
CVE-2024-32101	Cross-Site Request Forgery (CSRF) vulnerability in Omnisend Email Marketing for WooCommerce by Omnisend.This issue affects Email Marketing for WooCommerce
CVE-2024-32451	Cross-Site Request Forgery (CSRF) vulnerability in wpWax Legal Pages.This issue affects Legal Pages: from n/a through 1.4.2.
CVE-2024-31376	Cross-Site Request Forgery (CSRF) vulnerability in Andrew Rapps Dashboard To-Do List.This issue affects Dashboard To-Do List: from n/a through 1.3.1.
CVE-2024-32089	Cross-Site Request Forgery (CSRF) vulnerability in Supsystic Digital Publications by Supsystic.This issue affects Digital Publications by Supsystic: from n/a through 1.7
CVE-2024-31922	Cross-Site Request Forgery (CSRF) vulnerability in Anton Aleksandrov WordPress Hosting Benchmark tool.This issue affects WordPress Hosting Benchmark tool: fron
CVE-2024-31426	Cross-Site Request Forgery (CSRF) vulnerability in Data443 Inline Related Posts.This issue affects Inline Related Posts: from n/a through 3.3.1.
CVE-2024-32450	Cross-Site Request Forgery (CSRF) vulnerability in MagePeople Team WpTravelly.This issue affects WpTravelly: from n/a through 1.6.0.
CVE-2024-32442	Cross-Site Request Forgery (CSRF) vulnerability in Zoho Campaigns.This issue affects Zoho Campaigns: from n/a through 2.0.7.
CVE-2024-31374	Cross-Site Request Forgery (CSRF) vulnerability in AppPresser Team AppPresser.This issue affects AppPresser: from n/a through 4.3.0.
CVE-2024-31921	Cross-Site Request Forgery (CSRF) vulnerability in Etoile Web Design Ultimate Product Catalogue.This issue affects Ultimate Product Catalogue: from n/a through 5.2
CVE-2024-32102	Cross-Site Request Forgery (CSRF) vulnerability in Scott Kingsley Clark Crony Cronjob Manager.This issue affects Crony Cronjob Manager: from n/a through 0.5.0.
CVE-2024-30546	Cross-Site Request Forgery (CSRF) vulnerability in Pixelite Login With Ajax.This issue affects Login With Ajax: from n/a through 4.1.
CVE-2024-31920	Cross-Site Request Forgery (CSRF) vulnerability in Tyche Softwares Currency per Product for WooCommerce.This issue affects Currency per Product for WooComme
CVE-2024-32443	Cross-Site Request Forgery (CSRF) vulnerability in IP2Location Download IP2Location Country Blocker.This issue affects Download IP2Location Country Blocker: fron

CVE Number	Description
CVE-2024-31427	Cross-Site Request Forgery (CSRF) vulnerability in Marker.Io Marker.Io.This issue affects Marker.Io : from n/a through 1.1.8.
CVE-2024-32447	Cross-Site Request Forgery (CSRF) vulnerability in AWP Classifieds Team AWP Classifieds.This issue affects AWP Classifieds: from n/a through 4.3.1.
CVE-2024-31428	Cross-Site Request Forgery (CSRF) vulnerability in Rara Theme The Conference.This issue affects The Conference: from n/a through 1.2.0.
CVE-2024-31383	Cross-Site Request Forgery (CSRF) vulnerability in Pagelayer PopularFX.This issue affects PopularFX: from n/a through 1.2.4.
CVE-2024-32434	Cross-Site Request Forgery (CSRF) vulnerability in Tyche Softwares Order Delivery Date for WooCommerce.This issue affects Order Delivery Date for WooCommerce
CVE-2024-32448	Cross-Site Request Forgery (CSRF) vulnerability in VideoYield.Com Ads.Txt Admin.This issue affects Ads.Txt Admin: from n/a through 1.3.
CVE-2024-31429	Cross-Site Request Forgery (CSRF) vulnerability in Blossom Themes Sarada Lite.This issue affects Sarada Lite: from n/a through 1.1.2.
CVE-2024-31431	Cross-Site Request Forgery (CSRF) vulnerability in Tyche Softwares Product Input Fields for WooCommerce.This issue affects Product Input Fields for WooCommerce
CVE-2024-32090	Cross-Site Request Forgery (CSRF) vulnerability in Andy Moyle Church Admin.This issue affects Church Admin: from n/a through 4.0.27.
CVE-2024-31433	Cross-Site Request Forgery (CSRF) vulnerability in The Events Calendar.This issue affects The Events Calendar: from n/a through 6.3.0.
CVE-2024-32435	Cross-Site Request Forgery (CSRF) vulnerability in Affieasy Team AffiEasy.This issue affects AffiEasy: from n/a through 1.1.4.
CVE-2024-3505	JFrog Artifactory Self-Hosted versions below 7.77.3, are vulnerable to sensitive information disclosure whereby a low-privileged authenticated user can read the proxy c
CVE-2024-31923	Cross-Site Request Forgery (CSRF) vulnerability in PluginOps Feather Login Page.This issue affects Feather Login Page: from n/a through 1.1.5.
CVE-2024-31278	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Leap13 Premium Addons for Elementor.This issue affects Premium Addons for Elementor: f
CVE-2024-31942	Cross-Site Request Forgery (CSRF) vulnerability in Typps Calendarista Basic Edition.This issue affects Calendarista Basic Edition: from n/a through 3.0.2.
CVE-2024-31421	Missing Authorization vulnerability in Supsystic Popup by Supsystic.This issue affects Popup by Supsystic: from n/a through 1.10.27.
CVE-2024-32439	Cross-Site Request Forgery (CSRF) vulnerability in SwitchWP WP Client Reports.This issue affects WP Client Reports: from n/a through 1.0.22.
CVE-2024-32433	Cross-Site Request Forgery (CSRF) vulnerability in Themefic BEAF.This issue affects BEAF: from n/a through 4.5.4.
CVE-2024-32099	Cross-Site Request Forgery (CSRF) vulnerability in James Ward WP Mail Catcher.This issue affects WP Mail Catcher: from n/a through 2.1.6.

CVE Number	Description
CVE-2024-32441	Cross-Site Request Forgery (CSRF) vulnerability in Zoho Campaigns.This issue affects Zoho Campaigns: from n/a through 2.0.7.
CVE-2024-32095	Cross-Site Request Forgery (CSRF) vulnerability in MultiParcels MultiParcels Shipping For WooCommerce.This issue affects MultiParcels Shipping For WooCommerc
CVE-2024-31422	Cross-Site Request Forgery (CSRF) vulnerability in Philippe Bernard Favicon.This issue affects Favicon: from n/a through 1.3.29.
CVE-2024-31382	Cross-Site Request Forgery (CSRF) vulnerability in Creative Themes HQ Blocksy.This issue affects Blocksy: from n/a through 2.0.22.
CVE-2024-32438	Cross-Site Request Forgery (CSRF) vulnerability in cleverplugins.Com SEO Booster.This issue affects SEO Booster: from n/a through 3.8.9.
CVE-2024-32141	Cross-Site Request Forgery (CSRF) vulnerability in Libsyn Libsyn Publisher Hub.This issue affects Libsyn Publisher Hub: from n/a through 1.4.4.
CVE-2024-31219	Discourse-reactions is a plugin that allows user to add their reactions to the post. When whispers are enabled on a site via `whispers_allowed_groups` and reactions ar the reaction data are shown on the `/u/:username/activity/reactions` endpoint.
CVE-2024-32104	Cross-Site Request Forgery (CSRF) vulnerability in XLPlugins NextMove Lite.This issue affects NextMove Lite: from n/a through 2.18.1.
CVE-2024-31388	Cross-Site Request Forgery (CSRF) vulnerability in Pauple Table & Contact Form 7 Database – Tablesome.This issue affects Table & Contact Form 7 Database – Tab
CVE-2024-31385	Cross-Site Request Forgery (CSRF) vulnerability in Reservation Diary ReDi Restaurant Reservation.This issue affects ReDi Restaurant Reservation: from n/a through 2
CVE-2024-31940	Cross-Site Request Forgery (CSRF) vulnerability in RedNao Extra Product Options Builder for WooCommerce.This issue affects Extra Product Options Builder for Woo
CVE-2024-32084	Cross-Site Request Forgery (CSRF) vulnerability in Gold Plugins Before And After.This issue affects Before And After: from n/a through 3.9.
CVE-2024-31938	Cross-Site Request Forgery (CSRF) vulnerability in Themeinwp NewsXpress.This issue affects NewsXpress: from n/a through 1.0.7.
CVE-2024-32094	Cross-Site Request Forgery (CSRF) vulnerability in ChurchThemes Church Content – Sermons, Events and More.This issue affects Church Content – Sermons, Event
CVE-2024-31381	Cross-Site Request Forgery (CSRF) vulnerability in RebelCode Spotlight Social Media Feeds.This issue affects Spotlight Social Media Feeds: from n/a through 1.6.10.
CVE-2024-32088	Cross-Site Request Forgery (CSRF) vulnerability in SeedProd Coming Soon Page, Under Construction & Maintenance Mode by SeedProd.This issue affects Coming S n/a through 6.15.20.
CVE-2024-32440	Cross-Site Request Forgery (CSRF) vulnerability in Thomas Belser Asgaros Forum.This issue affects Asgaros Forum: from n/a through 2.8.0.
CVE-2024-29902	Cosign provides code signing and transparency for containers and binaries. Prior to version 2.2.4, a remote image with a malicious attachment can cause denial of serv on the machine that rely on having memory available such as a Redis database which can result in data loss. It can also impact the availability of other services on the The root cause of this issue is that Cosign reads the attachment from a remote image entirely into memory without checking the size of the attachment first. As such, a memory; If the attachments size is larger than the machine has memory available, the machine will be denied of service. The Go runtime will make a SigKill after a few escalation from a compromised registry to the Cosign user: If an attacher has compromised a registry or the account of an image vendor, they can include a malicious a for the vulnerability.

CVE Number	Description
CVE-2024-26023	OS command injection vulnerability in BUFFALO wireless LAN routers allows a logged-in user to execute arbitrary OS commands.
CVE-2024-29903	Cosign provides code signing and transparency for containers and binaries. Prior to version 2.2.4, maliciously-crafted software artifacts can cause denial of service of tl machine. The root cause is that Cosign creates slices based on the number of signatures, manifests or attestations in untrusted artifacts. As such, the untrusted artifact issue is Cosign allocates excessive memory on the lines that creates a slice of the same length as the manifests. Version 2.2.4 contains a patch for the vulnerability.
CVE-2024-21066	Vulnerability in the RDBMS component of Oracle Database Server. Supported versions that are affected are 19.3-19.22 and 21.3-21.13. Easily exploitable vulnerability logon to the infrastructure where RDBMS executes to compromise RDBMS. Successful attacks require human interaction from a person other than the attacker. Succe critical data or complete access to all RDBMS accessible data. CVSS 3.1 Base Score 4.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U
CVE-2023-45808	iTop is an IT service management platform. When creating or updating an object, extkey values aren't checked to be in the current user silo. In other words, by forging (for example a UserRequest in an out of scope Organization). Fixed in iTop 2.7.10, 3.0.4, 3.1.1, and 3.2.0.
CVE-2024-3388	A vulnerability in the GlobalProtect Gateway in Palo Alto Networks PAN-OS software enables an authenticated attacker to impersonate another user and send network attacker to receive response packets from those internal assets.
CVE-2024-32028	OpenTelemetry dotnet is a dotnet telemetry framework. In affected versions of `OpenTelemetry.Instrumentation.Http` and `OpenTelemetry.Instrumentation.AspNetCore enabled for outgoing http requests and `OpenTelemetry.Instrumentation.AspNetCore` writes the `url.query` attribute/tag on spans (`Activity`) when tracing is enabled fo Conventions for HTTP Spans. Up until version `1.8.1` the values written by `OpenTelemetry.Instrumentation.Http` & `OpenTelemetry.Instrumentation.AspNetCore` will This may lead to sensitive information (e.g. EUII - End User Identifiable Information, credentials, etc.) being leaked into telemetry backends (depending on the applicati incidents. Note: Older versions of `OpenTelemetry.Instrumentation.Http` & `OpenTelemetry.Instrumentation.AspNetCore` may use different tag names but have the sar `OpenTelemetry.Instrumentation.Http` & `OpenTelemetry.Instrumentation.AspNetCore` will now redact by default all values detected on transmitted or received query s for this vulnerability.
CVE-2024-32633	An unsigned value can never be negative, so eMMC full disk test will always evaluate the same way.
CVE-2024-3861	If an AlignedBuffer were assigned to itself, the subsequent self-move could result in an incorrect reference count and later use-after-free. This vulnerability affects Firefo
CVE-2024-21100	Vulnerability in the Oracle Commerce Platform product of Oracle Commerce (component: Platform). Supported versions that are affected are 11.3.0, 11.3.1 and 11.3.2. network access via HTTP to compromise Oracle Commerce Platform. While the vulnerability is in Oracle Commerce Platform, attacks may significantly impact additiona result in unauthorized update, insert or delete access to some of Oracle Commerce Platform accessible data. CVSS 3.1 Base Score 4.0 (Integrity impacts). CVSS Vect
CVE-2024-27086	The MSAL library enabled acquisition of security tokens to call protected APIs. MSAL.NET applications targeting Xamarin Android and .NET Android (e.g., MAUI) using vulnerability. A malicious application running on a customer Android device can cause local denial of service against applications that were built using MSAL.NET for au application from logging in) due to incorrect activity export configuration. MSAL.NET version 4.60.1 includes the fix. As a workaround, a developer may explicitly mark tl
CVE-2024-21000	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.36 and prior and 8. attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or de unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV
CVE-2024-3735	A vulnerability was found in Smart Office up to 20240405. It has been classified as problematic. Affected is an unknown function of the file Main.aspx. The manipulation leads to weak password requirements. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2024-20954	Vulnerability in the Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Compiler). Supported versions that are affecte Enterprise Edition: 20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle attacks of this vulnerability can result in unauthorized read access to a subset of Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition accessible data. CVSS 3. (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2024-3302	There was no limit to the number of HTTP/2 CONTINUATION frames that would be processed. A server could abuse this to create an Out of Memory condition in the b and Thunderbird < 115.10.
CVE-2024-21068	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2 and 22; Oracle GraalVM Enterprise Edition: 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to so 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 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 re impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2024-21085	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Concurrency). Supported versions that are affected are Enterprise Edition: 20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This vulner 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 applic (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
CVE-2024-31254	Insertion of Sensitive Information into Log File vulnerability in WebToffee WordPress Backup & Migration.This issue affects WordPress Backup & Migration: from n/a th

CVE Number	Description
CVE-2024-31265	Cross-Site Request Forgery (CSRF) vulnerability in SumoMe Sumo.This issue affects Sumo: from n/a through 1.34.
CVE-2024-3689	A vulnerability classified as problematic has been found in Zhejiang Land Zongheng Network Technology O2OA up to 20240403. Affected is an unknown function of the manipulation leads to information disclosure. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficul 260478 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2024-21012	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versio Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22; Oracle GraalVM Enterprise Edition: 20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker wi Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java ap 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., impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2024-21098	Vulnerability in the Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Compiler). Supported versions that are affecte Enterprise Edition: 20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle GraalVM for JDK, Oracle GraalVM Enterprise Ec (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2024-21011	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions 17.0.10, 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22; Oracle GraalVM Enterprise Edition: 20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthe compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to c 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 w 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 fr 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).
CVE-2023-50347	HCL DRYiCE MyXalytics is impacted by an insecure SQL interface vulnerability, potentially giving an attacker the ability to execute custom SQL queries. A malicious us configuration.
CVE-2024-21094	Vulnerability in the Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions 17.0.10, 21.0.2, 22; Oracle GraalVM for JDK: 17.0.10, 21.0.2, 22; Oracle GraalVM Enterprise Edition: 20.3.13 and 21.3.9. Difficult to exploit vulnerability allows unauthe compromise Oracle Java SE, Oracle GraalVM for JDK, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, ins 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 servic 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 fr 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).
CVE-2024-3531	A vulnerability was found in Campcodes Complete Online Student Management System 1.0. It has been rated as problematic. This issue affects some unknown proces FirstRecord leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-25990
CVE-2024-3542	A vulnerability classified as problematic was found in Campcodes Church Management System 1.0. This vulnerability affects unknown code of the file /admin/add_visit scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259912.
CVE-2024-3612	A vulnerability was found in SourceCodester Warehouse Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown fur nama_barang/merek leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VI
CVE-2024-3530	A vulnerability was found in Campcodes Complete Online Student Management System 1.0. It has been declared as problematic. This vulnerability affects unknown co FirstRecord leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulner
CVE-2024-3541	A vulnerability classified as problematic has been found in Campcodes Church Management System 1.0. This affects an unknown part of the file /admin/admin_user.ph scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB
CVE-2024-3613	A vulnerability was found in SourceCodester Warehouse Management System 1.0. It has been rated as problematic. Affected by this issue is some unknown functional nama_supplier/alamat_supplier/notelp_supplier leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and ma
CVE-2024-3529	A vulnerability was found in Campcodes Complete Online Student Management System 1.0. It has been classified as problematic. This affects an unknown part of the f leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this v
CVE-2024-3528	A vulnerability was found in Campcodes Complete Online Student Management System 1.0 and classified as problematic. Affected by this issue is some unknown func FirstRecord leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-259898 is the ident
CVE-2024-3526	A vulnerability has been found in Campcodes Online Event Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functior to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-259897 was assigned to

CVE Number	Description
CVE-2024-3614	A vulnerability classified as problematic has been found in SourceCodester Warehouse Management System 1.0. This affects an unknown part of the file customer.php nama_customer/alamat_customer/notelp_customer leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public 260271.
CVE-2024-22438	A potential security vulnerability has been identified in Hewlett Packard Enterprise OfficeConnect 1820 Network switches. The vulnerability could be remotely exploited
CVE-2024-3525	A vulnerability, which was classified as problematic, was found in Campcodes Online Event Management System 1.0. Affected is an unknown function of the file /views scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-259896.
CVE-2024-3524	A vulnerability, which was classified as problematic, has been found in Campcodes Online Event Management System 1.0. This issue affects some unknown processin leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulner
CVE-2024-3695	A vulnerability has been found in SourceCodester Computer Laboratory Management System 1.0 and classified as problematic. This vulnerability affects unknown code leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-260482 is the identifier assigned
CVE-2024-3687	A vulnerability was found in bihell Dice 3.1.0 and classified as problematic. Affected by this issue is some unknown functionality of the component Comment Handler. T launched remotely. The exploit has been disclosed to the public and may be used. VDB-260474 is the identifier assigned to this vulnerability.
CVE-2024-3616	A vulnerability classified as problematic was found in SourceCodester Warehouse Management System 1.0. This vulnerability affects unknown code of the file penggur admin_user/admin_nama/admin_alamat/admin_telepon leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public a
CVE-2024-3532	A vulnerability classified as problematic has been found in Campcodes Complete Online Student Management System 1.0. Affected is an unknown function of the file a leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-259902 is the identifier ass
CVE-2024-3533	A vulnerability classified as problematic was found in Campcodes Complete Online Student Management System 1.0. Affected by this vulnerability is an unknown funct argument FirstRecord leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associate
CVE-2024-21108	Vulnerability in the Oracle VM VirtualBox product of Oracle Virtualization (component: Core). Supported versions that are affected are Prior to 7.0.16. Easily exploitable infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox. Successful attacks of this vulnerability can result in unauthorized read acces Score 3.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2024-21005	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Orac 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Ente person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle Gra 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 c 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 Sco (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2024-21003	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Orac 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Ente person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle Gra 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 c 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 Sco (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2024-3872	Mattermost Mobile app versions 2.13.0 and earlier use a regular expression with polynomial complexity to parse certain deeplinks, which allows an unauthenticated ren link.
CVE-2024-28344	An Open Redirect vulnerability was found in Sipwise C5 NGCP Dashboard below mr11.5.1. The Open Redirect vulnerability allows attackers to control the "back" parar
CVE-2024-3764	** DISPUTED ** A vulnerability classified as problematic has been found in Tuya SDK up to 5.0.x. Affected is an unknown function of the component MQTT Packet Har the attack remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. Upgrading to v the affected component. The identifier of this vulnerability is VDB-260604. NOTE: The vendor explains that a malicious actor would have to crack TLS first or use a legi
CVE-2024-21004	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Orac 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition execut Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or d Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java app 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., impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).

CVE Number	Description
CVE-2024-21002	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JavaFX). Supported versions that are affected are Orac 21.3.9. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Oracle Java SE, Oracle GraalVM Enterprise Edition execut Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or d Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java ap 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., impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2024-20995	Vulnerability in the Oracle Database Sharding component of Oracle Database Server. Supported versions that are affected are 19.3-19.22 and 21.3-21.13. Easily explo with network access via Oracle Net to compromise Oracle Database Sharding. Successful attacks require human interaction from a person other than the attacker. Suc cause a partial denial of service (partial DOS) of Oracle Database Sharding. CVSS 3.1 Base Score 2.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H
CVE-2024-3762	A vulnerability was found in Emlog Pro 2.2.10. It has been declared as problematic. This vulnerability affects unknown code of the file /admin/twitter.php of the compone attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-260602 is the identifier assigned to this vulnerability. NOTE: The v any way.
CVE-2024-3766	A vulnerability, which was classified as problematic, has been found in slowlyo OwlAdmin up to 3.5.7. Affected by this issue is some unknown functionality of the file /ad manipulation of the argument file leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VD
CVE-2024-3763	A vulnerability was found in Emlog Pro 2.2.10. It has been rated as problematic. This issue affects some unknown processing of the file /admin/tag.php of the compone attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-260603. NOTE: Th in any way.
CVE-2024-32001	SpiceDB is a graph database purpose-built for storing and evaluating access control data. Use of a relation of the form: `relation folder: folder | folder#parent` with an a subjects found under subjects for either `folder` or `folder#parent`. This bug only manifests if the same subject type is used multiple types in a relation, relationships exi making a negative authorization decision based on the results of a LookupSubjects request with version before v1.30.1 is affected. Version 1.30.1 contains a patch for t authorization decisions and/or avoid using the broken schema.
CVE-2024-21101	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: General). Supported versions that are affected are 7.5.33 and prior, 7.6.29 and prior allows high privileged attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks of this vulnerability can result in unauthoriz 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).
CVE-2024-21105	Vulnerability in the Oracle Solaris product of Oracle Systems (component: Utility). The supported version that is affected is 11. Easily exploitable vulnerability allows hig executes to compromise Oracle Solaris. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can accessible data. CVSS 3.1 Base Score 2.0 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N).
CVE-2024-1902	lunary-ai/lunary is vulnerable to a session reuse attack, allowing a removed user to change the organization name without proper authorization. The vulnerability stems organization before allowing them to make changes. An attacker can exploit this by using an old authorization token to send a PATCH request, modifying the organizati due to incorrect synchronization and affects the orgs.patch route.
CVE-2024-30715	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30719	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30718	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2023-6257	The Inline Related Posts WordPress plugin before 3.6.0 is missing authorization in an AJAX action to ensure that users are allowed to see the content of the posts disp content of password protected posts
CVE-2024-29450	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-29449	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30716	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30713	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30722	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.

CVE Number	Description
CVE-2024-29448	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30712	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30711	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-2195	A critical Remote Code Execution (RCE) vulnerability was identified in the aimhubio/aim project, specifically within the `/api/runs/search/run/` endpoint, affecting versior the `aim/web/api/runs/views.py` file, where improper restriction of user access to the `RunView` object allows for the execution of arbitrary code via the `query` paramet server, potentially leading to full system compromise.
CVE-2024-2196	aimhubio/aim is vulnerable to Cross-Site Request Forgery (CSRF), allowing attackers to perform actions such as deleting runs, updating data, and stealing data like log from the lack of CSRF and CORS protection in the aim dashboard. An attacker can exploit this by tricking a user into executing a malicious script that sends unauthoriz unauthorized data manipulation.
CVE-2024-30710	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30708	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30707	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-29291	An issue in Laravel Framework 8 through 11 might allow a remote attacker to discover database credentials in storage/logs/laravel.log. NOTE: this is disputed by multip can choose to have debugging logs, but needs to set the access control appropriately for the type of data that may be logged.
CVE-2024-30721	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30723	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-29455	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-2029	A command injection vulnerability exists in the `TranscriptEndpoint` of mudler/localai, specifically within the `audioToWav` function used for converting audio files to WA sanitization of user-supplied filenames before passing them to ffmpeg via a shell command, allowing an attacker to execute arbitrary commands on the host system. Su or other detrimental impacts, depending on the privileges of the process executing the code.
CVE-2024-29454	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2023-44852	Cross Site Scripting (XSS) vulnerability in Cobham SAILOR VSAT Ku v.164B019, allows a remote attacker to execute arbitrary code via a crafted script to the c_set_tra
CVE-2024-1741	lunary-ai/lunary version 1.0.1 is vulnerable to improper authorization, allowing removed members to read, create, modify, and delete prompt templates using an old autl members can still perform operations on prompt templates by sending HTTP requests with their previously captured authorization token. This issue exposes organizatic
CVE-2023-6385	The WordPress Ping Optimizer WordPress plugin through 2.35.1.3.0 does not have CSRF checks in some places, which could allow attackers to make logged in users
CVE-2024-30614	An issue in Ametys CMS v4.5.0 and before allows attackers to obtain sensitive information via exposed resources to the error scope.
CVE-2024-1740	In lunary-ai/lunary version 1.0.1, a vulnerability exists where a user removed from an organization can still read, create, modify, and delete logs by re-using an old autho using an 'Authorization' token in the browser, which does not properly invalidate upon the user's removal from the organization. This allows the removed user to perforn details without valid permissions.

CVE Number	Description
CVE-2024-22718	Cross Site Scripting (XSS) vulnerability in Form Tools 3.1.1 allows attackers to run arbitrary code via the client_id parameter in the application URL.
CVE-2024-29447	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-29444	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-1728	gradio-app/gradio is vulnerable to a local file inclusion vulnerability due to improper validation of user-supplied input in the UploadButton component. Attackers can exp private SSH keys, by manipulating the file path in the request to the `/queue/join` endpoint. This issue could potentially lead to remote code execution. The vulnerability redirect file uploads to unintended locations on the server.
CVE-2024-1643	By knowing an organization's ID, an attacker can join the organization without permission and gain the ability to read and modify all data within that organization. This v information, posing a significant security risk. The flaw is due to insufficient verification of user permissions when joining an organization.
CVE-2024-30727	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30726	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30724	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-31861	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that
CVE-2024-30916	An issue was discovered in eProsima FastDDS v.2.14.0 and before, allows a local attacker to cause a denial of service (DoS) and obtain sensitive information via a cra
CVE-2024-29441	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30728	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-29452	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-3025	mintplex-labs/anything-llm is vulnerable to path traversal attacks due to insufficient validation of user-supplied input in the logo filename functionality. Attackers can exp outside of the restricted directory. This can lead to unauthorized reading or deletion of files by utilizing the `/api/system/upload-logo` and `/api/system/logo` endpoints. T filename, allowing attackers to target sensitive files such as the application's database.
CVE-2024-31576	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that
CVE-2024-3802	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2021-47191	In the Linux kernel, the following vulnerability has been resolved: scsi: scsi_debug: Fix out-of-bound read in resp_readcap16() The following warning was observed run SCSI command 0x9e-- guessing data in; [3813.830724] program syz-executor not setting count and/or reply_len properly [3813.836956] ========== 3813.839465] BUG: KASAN: stack-out-of-bounds in sg_copy_buffer+0x157/0x1e0 [3813.841773] Read of size 4096 at addr ffff8883cf80f540 by task syz-executor/154 3813.847524] print_address_description+0xa5/0x372 [3813.848243] kasan_report.cold+0x236/0x2a8 [3813.849439] check_memory_region+0x240/0x270 [3813.850 3813.853032] sg_copy_from_buffer+0x13/0x20 [3813.853660] fill_from_dev_buffer+0x135/0x370 [3813.854329] resp_readcap16+0x1ac/0x280 [3813.856917] sched scsi_debug_queuecommand+0xb32/0x17e0 [3813.862699] scsi_dispatch_cmd+0x330/0x950 [3813.863329] scsi_request_fn+0xd8e/0x1710 [3813.863946] __blk_ru blk_execute_rq_nowait+0x1d8/0x400 [3813.865220] sg_common_write.isra.0+0xe61/0x2420 [3813.871637] sg_write+0x6c8/0xef0 [3813.878853] __vfs_write+0xe4/ ksys_write+0x103/0x270 [3813.886268] __x64_sys_write+0x77/0xc0 [3813.886841] do_syscall_64+0x106/0x360 [3813.887415] entry_SYSCALL_64_after_hwframe log: r0 = openat(0xffffffffffffff9c, &(0x7f0000000040)='./file0\x00', 0x26e1, 0x0) r1 = syz_open_procfs(0xffffffffffffffff, &(0x7f0000000000)='fd/3\x00') open_by_handle_at(syz_open_dev$sg(&(0x7f0000000000), 0x0, 0x40782) write$binfmt_aout(r2, &(0x7f0000000340)=ANY= [@ANYBLOB="00000000deff00000000000000000000000000000000000000000000000000000047f007af9e107a41ec395f1bded7be24277a1501ff6196a83366f4e6362b 0x126) In resp_readcap16() we get "int alloc_len" value -1104926854, and then pass the huge arr_len to fill_from_dev_buffer(), but arr is only 32 bytes. This leads to O

CVE Number	Description
CVE-2024-1626	An Insecure Direct Object Reference (IDOR) vulnerability exists in the lunary-ai/lunary repository, version 0.3.0, within the project update endpoint. The vulnerability allo system without proper authorization checks, by directly referencing the project's ID in the PATCH request to the '/v1/projects/:projectId' endpoint. This issue arises beca currently authenticated user, enabling unauthorized modifications across different organizational projects.
CVE-2024-1646	parisneo/lollms-webui is vulnerable to authentication bypass due to insufficient protection over sensitive endpoints. The application checks if the host parameter is not 'l bound to a specific interface, allowing unauthorized access to endpoints such as '/restart_program', '/update_software', '/check_update', '/start_recording', and '/stop_re disabling or overriding of recordings, and potentially other impacts if certain features are enabled in the configuration.
CVE-2024-1665	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2024-1666	In lunary-ai/lunary version 1.0.0, an authorization flaw exists that allows unauthorized radar creation. The vulnerability stems from the lack of server-side checks to verif is only enforced in the web UI. As a result, attackers can bypass the intended account upgrade requirement by directly sending crafted requests to the server, enabling
CVE-2024-1738	An incorrect authorization vulnerability exists in the lunary-ai/lunary repository, specifically within the evaluations.get route in the evaluations API endpoint. This vulnera organization's evaluation by simply knowing the evaluation ID, due to the lack of project ID verification in the SQL query. As a result, attackers can gain access to poter
CVE-2024-1846	The Responsive Tabs WordPress plugin before 4.0.7 does not validate and escape some of its shortcode attributes before outputting them back in a page/post where t and above to perform Stored Cross-Site Scripting attacks
CVE-2024-1961	vertaai/modeldb is vulnerable to a path traversal attack due to improper sanitization of user-supplied file paths in its file upload functionality. Attackers can exploit this vu manipulating the 'artifact_path' parameter. This flaw can lead to Remote Code Execution (RCE) by overwriting critical files, such as the application's configuration file, e is present in the NFSController.java and NFSService.java components of the application.
CVE-2024-2083	A directory traversal vulnerability exists in the zenml-io/zenml repository, specifically within the /api/v1/steps endpoint. Attackers can exploit this vulnerability by manipul bypassing intended access restrictions. The vulnerability arises due to the lack of validation for directory traversal patterns, allowing attackers to access files outside of
CVE-2024-2260	A session fixation vulnerability exists in the zenml-io/zenml application, where JWT tokens used for user authentication are not invalidated upon logout. This flaw allows JWT token.
CVE-2024-3028	mintplex-labs/anything-llm is vulnerable to improper input validation, allowing attackers to read and delete arbitrary files on the server. By manipulating the 'logo_filenam construct requests to read sensitive files or the application's '.env' file, and even delete files by setting the 'logo_filename' to the path of the target file and invoking the 'r sanitization of user-supplied input.
CVE-2024-3029	In mintplex-labs/anything-llm, an attacker can exploit improper input validation by sending a malformed JSON payload to the '/system/enable-multi-user' endpoint. This users and disables the 'multi_user_mode'. The vulnerability allows an attacker to remove all existing users and potentially create a new admin user without requiring a p application.
CVE-2024-3271	A command injection vulnerability exists in the run-llama/llama_index repository, specifically within the safe_eval function. Attackers can bypass the intended security m generated by LLM, to execute arbitrary code. This is achieved by crafting input that does not contain an underscore but still results in the execution of OS commands. T hosting the application.
CVE-2024-3571	langchain-ai/langchain is vulnerable to path traversal due to improper limitation of a pathname to a restricted directory ('Path Traversal') in its LocalFileStore functionalit anywhere on the filesystem, potentially leading to information disclosure or remote code execution. The issue lies in the handling of file paths in the mset and mget met directory traversal sequences to reach unintended directories.
CVE-2024-3572	The scrapy/scrapy project is vulnerable to XML External Entity (XXE) attacks due to the use of lxml.etree.fromstring for parsing untrusted XML data without proper valid attacks, access local files, generate network connections, or circumvent firewalls by submitting specially crafted XML data.
CVE-2024-3573	mlflow/mlflow is vulnerable to Local File Inclusion (LFI) due to improper parsing of URIs, allowing attackers to bypass checks and read arbitrary files on the system. The URIs with empty or 'file' schemes, leading to the misclassification of URIs as non-local. Attackers can exploit this by crafting malicious model versions with specially cra least two directory levels from the server's root.
CVE-2024-3574	In scrapy version 2.10.1, an issue was identified where the Authorization header, containing credentials for server authentication, is leaked to a third-party site during a remove the Authorization header when redirecting across domains. The exposure of the Authorization header to unauthorized actors could potentially allow for account
CVE-2024-3575	Cross-site Scripting (XSS) - Stored in mindsdb/mindsdb
CVE-2024-31783	Cross Site Scripting (XSS) vulnerability in Typora v.1.6.7 and before, allows a local attacker to obtain sensitive information via a crafted script during markdown file crea
CVE-2021-47190	In the Linux kernel, the following vulnerability has been resolved: perf bpf: Avoid memory leak from perf_env__insert_btf() perf_env__insert_btf() doesn't insert if a dupli function to return a success/error value and then free the memory if insertion didn't happen. v2. Adds a return -1 when the insertion error occurs in perf_env__fetch_btf.

CVE Number	Description
CVE-2024-26816	In the Linux kernel, the following vulnerability has been resolved: x86, relocs: Ignore relocations in .notes section When building with CONFIG_XEN_PV=y, .text symbo "startup_xen" entry point. This information is used prior to booting the kernel, so relocations are not useful. In fact, performing relocations against the .notes section mea readable. To avoid leaking the KASLR base without breaking unprivileged tools that are expecting to read /sys/kernel/notes, skip performing relocations in the .notes se System.map.
CVE-2024-0902	The Fancy Product Designer WordPress plugin before 6.1.81 does not sanitise and escape some of its settings, which could allow high privilege users such as admin t unfiltered_html capability is disallowed (for example in multisite setup)
CVE-2024-1601	An SQL injection vulnerability exists in the `delete_discussion()` function of the parisneo/lollms-webui application, allowing an attacker to delete all discussions and mes request to the `/delete_discussion` endpoint, which internally calls the vulnerable `delete_discussion()` function. By sending a specially crafted payload in the 'id' param the 'discussion' and 'message' tables. This issue is due to improper neutralization of special elements used in an SQL command.
CVE-2024-1594	A path traversal vulnerability exists in the mlflow/mlflow repository, specifically within the handling of the `artifact_location` parameter when creating an experiment. Atta the artifact location URI to read arbitrary files on the server in the context of the server's process. This issue is similar to CVE-2023-6909 but utilizes a different compon
CVE-2024-1593	A path traversal vulnerability exists in the mlflow/mlflow repository due to improper handling of URL parameters. By smuggling path traversal sequences using the ';' cha URL to gain unauthorized access to files or directories. This vulnerability allows for arbitrary data smuggling into the 'params' part of the URL, enabling attacks similar t parameter smuggling. Successful exploitation could lead to unauthorized information disclosure or server compromise.
CVE-2021-47188	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Improve SCSI abort handling The following has been observed on a test setup: WARN ufshcd_queuecommand+0x468/0x65c Call trace: ufshcd_queuecommand+0x468/0x65c scsi_send_eh_cmnd+0x224/0x6a0 scsi_eh_test_devices+0x248/0x418 scsi_e kthread+0x150/0x1b4 ret_from_fork+0x10/0x30 That warning is triggered by the following statement: WARN_ON(lrbp->cmd); Fix this warning by clearing lrbp->cmd fro
CVE-2024-3101	In mintplex-labs/anything-llm, an improper input validation vulnerability allows attackers to escalate privileges by deactivating 'Multi-User Mode'. By sending a specially attacker can deactivate 'Multi-User Mode'. This action permits the creation of a new admin user without requiring a password, leading to unauthorized administrative ac
CVE-2024-3283	A vulnerability in mintplex-labs/anything-llm allows users with manager roles to escalate their privileges to admin roles through a mass assignment issue. The '/admin/s users to modify the 'multi_user_mode' system variable, enabling them to access the '/api/system/enable-multi-user' endpoint and create a new admin user. This issue r without proper validation of modifiable fields, leading to unauthorized modification of system settings and subsequent privilege escalation.
CVE-2024-3568	The huggingface/transformers library is vulnerable to arbitrary code execution through deserialization of untrusted data within the `load_repo_checkpoint()` function of t and commands by crafting a malicious serialized payload, exploiting the use of `pickle.load()` on data from potentially untrusted sources. This vulnerability allows for re seemingly harmless checkpoint during a normal training process, thereby enabling attackers to execute arbitrary code on the targeted machine.
CVE-2024-3569	A Denial of Service (DoS) vulnerability exists in the mintplex-labs/anything-llm repository when the application is running in 'just me' mode with a password. An attacker the [validatedRequest] middleware with a specially crafted 'Authorization:' header. This vulnerability leads to uncontrolled resource consumption, causing a DoS conditi
CVE-2024-3570	A stored Cross-Site Scripting (XSS) vulnerability exists in the chat functionality of the mintplex-labs/anything-llm repository, allowing attackers to execute arbitrary Java responses, an attacker can inject malicious scripts to perform actions on behalf of the user, such as creating a new admin account or changing the user's password, lea vulnerability stems from the improper sanitization of user and ChatBot input, specifically through the use of `dangerouslySetInnerHTML`. Successful exploitation require AnythingLLM instance.
CVE-2021-47182	In the Linux kernel, the following vulnerability has been resolved: scsi: core: Fix scsi_mode_sense() buffer length handling Several problems exist with scsi_mode_sens SENSE(10) command is 16-bits, occupying bytes 7 and 8 of the CDB. With this command, access to mode pages larger than 255 bytes is thus possible. However, the truncating buffer length larger than 255. 2) If scsi_mode_sense() is called with len smaller than 8 with sdev->use_10_for_ms set, or smaller than 4 otherwise, the buffer with these increased values, thus corrupting the memory following the buffer. Fix these 2 problems by using put_unaligned_be16() to set the allocation length field of M Furthermore, if len is larger than 255B, always try MODE SENSE(10) first, even if the device driver did not set sdev->use_10_for_ms. In case of invalid opcode error fo not retried using MODE SENSE(6). To avoid buffer length overflows for the MODE_SENSE(10) case, check that len is smaller than 65535 bytes. While at it, also fix the and block descriptor length fields of the mode sense reply header instead of using an open coded calculation. * Fix the kdoc dbd argument explanation: the DBD bit sta argument description was.
CVE-2021-47183	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Fix link down processing to address NULL pointer dereference If an FC link down transition outstanding ABTS requests may result in a NULL pointer dereference. Driver unload requests may hang with repeated "2878" log messages. The Link down processing WQEs are sent for the ELSs before the driver had set the link state to down. Thus the driver is sending the Abort with the expectation that an ABTS will be sent on the conditions the driver may auto-complete the ELSs thus if the link does come up, the Abort completions may reference an invalid structure. Fix by ensuring that Abort se failed.
CVE-2021-47184	In the Linux kernel, the following vulnerability has been resolved: i40e: Fix NULL ptr dereference on VSI filter sync Remove the reason of null pointer dereference in syn deleting and releasing of VSI resources to sync this thread with sync filters subtask. Without this patch it is possible to start update the VSI filter list after VSI is removed
CVE-2021-47187	In the Linux kernel, the following vulnerability has been resolved: arm64: dts: qcom: msm8998: Fix CPU/L2 idle state latency and residency The entry/exit latency and r first of all, for all of them the timings were written for CPU sleep but the min-residency-us param was miscalculated (supposedly, while porting this from downstream); T *and* the L2 cache, which have different timings: in the specific case of L2 the times are higher so these ones should be taken into account instead of the CPU ones. T on MSM8998 there was no CPU scaling at all, so cluster/L2 power collapse was rarely (if ever) hit. When CPU scaling is enabled, though, the wrong timings will produc sudden reboots and/or lockups. This set of parameters are stabilizing the SoC when CPU scaling is ON and when power collapse is frequently hit.
CVE-2024-2739	The Advanced Search WordPress plugin through 1.1.6 does not have CSRF checks in some places, which could allow attackers to make logged in users perform unwa

CVE Number	Description
CVE-2024-1569	parisneo/lollms-webui is vulnerable to a denial of service (DoS) attack due to uncontrolled resource consumption. Attackers can exploit the `/open_code_in_vs_code` a POST requests, leading to the opening of Visual Studio Code or the default folder opener (e.g., File Explorer, xdg-open) multiple times. This can render the host machi in the latest version of the software.
CVE-2024-0404	A mass assignment vulnerability exists in the `/api/invite/:code` endpoint of the mintplex-labs/anything-llm repository, allowing unauthorized creation of high-privileged a account creation process via an invitation link, an attacker can add a `role` property with `admin` value, thereby gaining administrative access. This issue arises due to exploit the system and perform actions as an administrator.
CVE-2024-0549	mintplex-labs/anything-llm is vulnerable to a relative path traversal attack, allowing unauthorized attackers with a default role account to delete files and folders within th The vulnerability stems from insufficient input validation and normalization in the handling of file and folder deletion requests. Successful exploitation results in the comp
CVE-2024-1135	Gunicorn fails to properly validate Transfer-Encoding headers, leading to HTTP Request Smuggling (HRS) vulnerabilities. By crafting requests with conflicting Transfer- access restricted endpoints. This issue is due to Gunicorn's handling of Transfer-Encoding headers, where it incorrectly processes requests with multiple, conflicting Tr final encoding specified. This vulnerability allows for a range of attacks including cache poisoning, session manipulation, and data exposure.
CVE-2024-1183	An SSRF (Server-Side Request Forgery) vulnerability exists in the gradio-app/gradio repository, allowing attackers to scan and identify open ports within an internal net can discern the status of internal ports based on the presence of a 'Location' header or a 'File not allowed' error in the response.
CVE-2024-1456	An S3 bucket takeover vulnerability was identified in the h2oai/h2o-3 repository. The issue involves the S3 bucket 'http://s3.amazonaws.com/h2o-training', which was fo
CVE-2024-1483	A path traversal vulnerability exists in mlflow/mlflow version 2.9.2, allowing attackers to access arbitrary files on the server. By crafting a series of HTTP POST requests local URI with '#' instead of '?', an attacker can traverse the server's directory structure. The issue occurs due to insufficient validation of user-supplied input in the serve
CVE-2024-1558	A path traversal vulnerability exists in the `_create_model_version()` function within `server/handlers.py` of the mlflow/mlflow repository, due to improper validation of th a `source` parameter that bypasses the `_validate_non_local_source_contains_relative_paths(source)` function's checks, allowing for arbitrary file read access on the s and the subsequent misuse of the original `source` value for model version creation, leading to the exposure of sensitive files when interacting with the `/model-version
CVE-2024-1560	A path traversal vulnerability exists in the mlflow/mlflow repository, specifically within the artifact deletion functionality. Attackers can bypass path validation by exploiting handler and `local_file_uri_to_path` function, allowing for the deletion of arbitrary directories on the server's filesystem. This vulnerability is due to an extra unquote ope fails to properly sanitize user-supplied paths. The issue is present up to version 2.9.2, despite attempts to fix a similar issue in CVE-2023-6831.
CVE-2024-1561	An issue was discovered in gradio-app/gradio, where the `/component_server` endpoint improperly allows the invocation of any method on a `Component` class with at `move_resource_to_block_cache()` method of the `Block` class, an attacker can copy any file on the filesystem to a temporary directory and subsequently retrieve it. TI significant risk especially when the application is exposed to the internet via `launch(share=True)`, thereby allowing remote attackers to read files on the host machine. potentially leading to the exposure of sensitive information such as API keys and credentials stored in environment variables.
CVE-2024-0399	The WooCommerce Customers Manager WordPress plugin before 29.7 does not properly sanitise and escape a parameter before using it in a SQL statement, leading
CVE-2021-47196	In the Linux kernel, the following vulnerability has been resolved: RDMA/core: Set send and receive CQ before forwarding to the driver Preset both receive and send C mlx4 is going to be changed do not overwrite ibqp properties. This change is needed for mlx5, because in case of QP creation failure, it will go to the path of QP destro create_qp.cold+0x164/0x16e [mlx5_ib] Write of size 8 at addr ffff8880064c55c0 by task a.out/246 CPU: 0 PID: 246 Comm: a.out Not tainted 5.15.0+ #291 Hardware na gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 Call Trace: dump_stack_lvl+0x45/0x59 print_address_description.constprop.0+0x1f/0x140 kasan_report.cold+0x83/0xdf mlx5_ib_create_qp+0x358/0x28a0 [mlx5_ib] create_qp.part.0+0x45b/0x6a0 [ib_core] ib_create_qp_user+0x97/0x150 [ib_core] ib_uverbs_handler_UVERBS_METHOD ib_uverbs_cmd_verbs+0x1c38/0x3150 [ib_uverbs] ib_uverbs_ioctl+0x169/0x260 [ib_uverbs] __x64_sys_ioctl+0x866/0x14d0 do_syscall_64+0x3d/0x90 entry_SYSCAL kasan_save_stack+0x1b/0x40 __kasan_kmalloc+0xa4/0xd0 create_qp.part.0+0x92/0x6a0 [ib_core] ib_create_qp_user+0x97/0x150 [ib_core] ib_uverbs_handler_UVE ib_uverbs_cmd_verbs+0x1c38/0x3150 [ib_uverbs] ib_uverbs_ioctl+0x169/0x260 [ib_uverbs] __x64_sys_ioctl+0x866/0x14d0 do_syscall_64+0x3d/0x90 entry_SYSCAL kasan_save_stack+0x1b/0x40 kasan_set_track+0x1c/0x30 kasan_set_free_info+0x20/0x30 __kasan_slab_free+0x10c/0x150 slab_free_freelist_hook+0xb4/0x1b0 kfre ib_create_qp_user+0x97/0x150 [ib_core] ib_uverbs_handler_UVERBS_METHOD_QP_CREATE+0x92c/0x1250 [ib_uverbs] ib_uverbs_cmd_verbs+0x1c38/0x3150 [ib_ __x64_sys_ioctl+0x866/0x14d0 do_syscall_64+0x3d/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae
CVE-2024-2221	qdrant/qdrant is vulnerable to a path traversal and arbitrary file upload vulnerability via the `/collections/{COLLECTION}/snapshots/upload` endpoint, specifically throug and overwrite any file on the filesystem, leading to potential remote code execution. This issue affects the integrity and availability of the system, enabling unauthorized
CVE-2021-47197	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: nullify cq->dbg pointer in mlx5_debug_cq_remove() Prior to this patch in case mlx5_core_c mlx5_core_destroy_cq() could be called again by user and cause additional call of mlx5_debug_cq_remove(). cq->dbg was not nullify in previous call and cause the cra destroy operations only if FW return 0 for MLX5_CMD_OP_DESTROY_CQ command. general protection fault, probably for non-canonical address 0x2000300004058: rc5_for_upstream_min_debug_2021_10_14_11_06 #1 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 8d 7f 70 e8 0a 2e 48 00 c7 85 d0 00 00 00 02 00 00 00 c6 45 70 00 fb 5d c3 c3 cc cc cc cc cc cc cc 53 <48> 8b 17 48 89 fb 85 d2 75 3d 48 89 d0 bf 64 00 00 00 48 0000000000000000 RBX: ffff888107d5f458 RCX: 00000000ffffffe RDX: 000000000002c2b0 RSI: ffffffff8155e2e0 RDI: 0002000300004058 RBP: ffff888137dd7a88 R0 R11: 0000000000000000 R12: ffff8881141d4000 R13: ffff888137dd7c68 R14: ffff888137dd7d58 R15: ffff888137dd7cc0 FS: 00007f4644f2a4c0(0000) GS:ffff8887a2d4 CR0: 0000000080050033 CR2: 000055b4500f4380 CR3: 0000000114f7a003 CR4: 0000000000170ea0 Call Trace: simple_recursive_removal+0x33/0x2e0 ? debugfs_ mlx5_debug_cq_remove+0x32/0x70 [mlx5_core] mlx5_core_destroy_cq+0x41/0x1d0 [mlx5_core] devx_obj_cleanup+0x151/0x330 [mlx5_ib] ? __pollwait+0xd0/0xd0 ? destroy_hw_idr_uobject+0x20/0x80 [ib_uverbs] uverbs_destroy_uobject+0x3b/0x360 [ib_uverbs] uobj_destroy+0x54/0xa0 [ib_uverbs] ib_uverbs_cmd_verbs+0xaf2/0x1 ib_uverbs_ioctl+0xc4/0x1b0 [ib_uverbs] __x64_sys_ioctl+0x3e4/0x8e0
CVE-2024-30733	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.

CVE Number	Description
CVE-2024-30730	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30729	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2021-47213	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2021-47214	In the Linux kernel, the following vulnerability has been resolved: hugetlb, userfaultfd: fix reservation restore on userfaultfd error Currently in the is_continue case in hug out_release_unlock;" in the cases where idx >= size, or !huge_pte_none(), the code will detect that new_pagecache_page == false, and so call restore_reserve_on_err and the following call to remove_inode_hugepages() will increment h->resv_hugepages causing a 100% reproducible leak. We should treat the is_continue case simila true, to indicate that there is no reservation to restore on the error path, and we need not call restore_reserve_on_error(). Rename new_pagecache_page to page_in_p
CVE-2021-47215	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: kTLS, Fix crash in RX resync flow For the TLS RX resync flow, we maintain a list of TLS co information to the HW. Here we fix list corruptions, by protecting the entries against movements coming from resync_handle_seq_match(), until their resync handling in
CVE-2021-47216	In the Linux kernel, the following vulnerability has been resolved: scsi: advansys: Fix kernel pointer leak Pointers should be printed with %p or %px rather than cast to 'u hashed pointer.
CVE-2021-47217	In the Linux kernel, the following vulnerability has been resolved: x86/hyperv: Fix NULL deref in set_hv_tscchange_cb() if Hyper-V setup fails Check for a valid hv_vp_i change callback. If Hyper-V setup failed in hyperv_init(), the kernel will still report that it's running under Hyper-V, but will have silently disabled nearly all functionality. E #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] SMP CPU: 4 PID: 1 Comm: swapper/0 Not tai ICH9, 2009), BIOS 0.0.0 02/06/2015 RIP: 0010:set_hv_tscchange_cb+0x15/0xa0 Code: <8b> 04 82 8b 15 12 17 85 01 48 c1 e0 20 48 0d ee 00 01 00 f6 c6 08 ... Call vmx_init+0xba/0x13a do_one_initcall+0x41/0x1c0 kernel_init_freeable+0x1f2/0x23b kernel_init+0x16/0x120 ret_from_fork+0x22/0x30
CVE-2021-47218	In the Linux kernel, the following vulnerability has been resolved: selinux: fix NULL-pointer dereference when hashtab allocation fails When the hash table slot array allo value, but the h->htable pointer is NULL. This may then cause a NULL pointer dereference, since the policydb code relies on the assumption that even after a failed ha on it. Yet, these detect an empty hashtab only by looking at the size. Fix this by making sure that hashtab_init() always leaves behind a valid empty hashtab when the a
CVE-2021-47219	In the Linux kernel, the following vulnerability has been resolved: scsi: scsi_debug: Fix out-of-bound read in resp_report_tgtpgs() The following issue was observed run include/linux/string.h:377 [inline] BUG: KASAN: slab-out-of-bounds in sg_copy_buffer+0x150/0x1c0 lib/scatterlist.c:831 Read of size 2132 at addr ffff8880aea95dc8 by tainted 4.19.202-00874-gfc0fe04215a9 #2 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.10.2-1ubuntu1 04/01/2014 Call Trace: __dump_stack li lib/dump_stack.c:118 print_address_description+0x73/0x280 mm/kasan/report.c:253 kasan_report_error mm/kasan/report.c:352 [inline] kasan_report+0x272/0x370 mn memcpy include/linux/string.h:377 [inline] sg_copy_buffer+0x150/0x1c0 lib/scatterlist.c:831 fill_from_dev_buffer+0x14f/0x340 drivers/scsi/scsi_debug.c:1021 resp_repo schedule_resp+0x464/0x12f0 drivers/scsi/scsi_debug.c:4429 scsi_debug_queuecommand+0x467/0x1390 drivers/scsi/scsi_debug.c:5835 scsi_dispatch_cmd+0x3fc/0x drivers/scsi/scsi_lib.c:2034 __blk_run_queue_uncond block/blk-core.c:464 [inline] __blk_run_queue+0x1a4/0x380 block/blk-core.c:484 blk_execute_rq_nowait+0x1c2/(drivers/scsi/sg.c:847 sg_write.part.23+0x6e0/0xd00 drivers/scsi/sg.c:716 sg_write+0x64/0xa0 drivers/scsi/sg.c:622 __vfs_write+0xed/0x690 fs/read_write.c:485 kill_bde fs/read_write.c:549 ksys_write+0x107/0x240 fs/read_write.c:599 do_syscall_64+0xc2/0x560 arch/x86/entry/common.c:293 entry_SYSCALL_64_after_hwframe+0x49/0 large length we will get a negative 'alen'. Switch n, alen, and rlen to u32.
CVE-2024-29502	An issue in Secure Lockdown Multi Application Edition v2.00.219 allows attackers to read arbitrary files via using UNC paths.
CVE-2024-3098	A vulnerability was identified in the `exec_utils` class of the `llama_index` package, specifically within the `safe_eval` function, allowing for prompt injection leading to ar input, which can be exploited to bypass method restrictions and execute unauthorized code. The vulnerability is a bypass of the previously addressed CVE-2023-39662 system by exploiting the flaw.
CVE-2024-1511	The parisneo/lollms-webui repository is susceptible to a path traversal vulnerability due to inadequate validation of user-supplied file paths. This flaw allows an unauthe arbitrary files on the server by exploiting various endpoints. The vulnerability can be exploited even when the service is bound to localhost, through cross-site requests
CVE-2024-1520	An OS Command Injection vulnerability exists in the '/open_code_folder' endpoint of the parisneo/lollms-webui application, due to improper validation of user-supplied i vulnerability by injecting malicious OS commands, leading to unauthorized command execution on the underlying operating system. This could result in unauthorized a
CVE-2024-1599	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2024-1600	A Local File Inclusion (LFI) vulnerability exists in the parisneo/lollms-webui application, specifically within the `/personalities` route. An attacker can exploit this vulnerab followed by the desired system file path, URL encoded. Successful exploitation allows the attacker to read any file on the filesystem accessible by the web server. This statement in the application.
CVE-2024-29439	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.

CVE Number	Description
CVE-2024-1602	parisneo/lollms-webui is vulnerable to stored Cross-Site Scripting (XSS) that leads to Remote Code Execution (RCE). The vulnerability arises due to inadequate sanitiz malicious JavaScript code. This code can be executed within the user's browser context, enabling the attacker to send a request to the `/execute_code` endpoint and e components of the application, including the handling of user input and model output.
CVE-2024-29443	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-29445	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-1625	An Insecure Direct Object Reference (IDOR) vulnerability exists in the lunary-ai/lunary application version 0.3.0, allowing unauthorized deletion of any organization's pr project deletion endpoint, where the endpoint fails to verify if the project ID provided in the request belongs to the requesting user's organization. As a result, an attacke DELETE request with the target project's ID. This issue affects the project deletion functionality implemented in the projects.delete route.
CVE-2024-30735	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30736	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2024-30737	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that vulnerability.
CVE-2021-47204	In the Linux kernel, the following vulnerability has been resolved: net: dpaa2-eth: fix use-after-free in dpaa2_eth_remove Access to netdev after free_netdev() will cause
CVE-2021-47199	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: CT, Fix multiple allocations and memleak of mod acts CT clear action offload adds additior registers which hold ct_state. When such flow also includes encap action, a neigh update event can cause the driver to unoffload the flow and then reoffload it. Each tir actions to reset ct_state until the max of mod hdr actions is reached. Also the driver never releases the allocated mod hdr actions and causing a memleak. Fix above tw phase and only use it when offloading the rule. The release of mod acts will be done in the normal flow_put(). backtrace: [<000000007316e2f3>] krealloc+0x83/0xd0 [< [<00000000970ce4ae>] mlx5e_tc_match_to_reg_set_and_get_id+0xd7/0x240 [mlx5_core] [<0000000067c5fa17>] mlx5e_tc_match_to_reg_set+0xa/0x20 [mlx5_core] mlx5_tc_ct_entry_set_registers.isra.0+0x36/0xc0 [mlx5_core] [<00000000fd23b869>] mlx5_tc_ct_flow_offload+0x272/0x1f10 [mlx5_core] [<000000004fc24acc>] mlx5e [<00000000dc741c17>] mlx5e_tc_encap_flows_add+0x489/0x690 [mlx5_core] [<00000000e92e49d7>] mlx5e_rep_update_flows+0x6e4/0x9b0 [mlx5_core] [<0000000
CVE-2021-47200	In the Linux kernel, the following vulnerability has been resolved: drm/prime: Fix use after free in mmap with drm_gem_ttm_mmap drm_gem_ttm_mmap() drops a refer entry to drm_gem_prime_mmap(), that drop will free the gem object, and the subsequent drm_gem_object_get() will be a UAF. Fix by grabbing a reference before calli dropping was adding in commit 9786b65bc61ac ("drm/ttm: fix mmap refcounting"): "For that to work properly the drm_gem_object_get() call in drm_gem_ttm_mmap() n otherwise the gem refcount would go down to zero."
CVE-2021-47201	In the Linux kernel, the following vulnerability has been resolved: iavf: free q_vectors before queues in iavf_disable_vf iavf_free_queues() clears adapter->num_active_ these two function calls in iavf_disable_vf(). This resolves a panic encountered when the interface is disabled and then later brought up again after PF communication i
CVE-2024-47202	In the Linux kernel, the following vulnerability has been resolved: thermal: Fix NULL pointer dereferences in of_thermal_ functions of_parse_thermal_zones() parses th subnode. However, if a thermal zone is consuming a thermal sensor and that thermal sensor device hasn't probed yet, an attempt to set trip_point_*_temp for that therr console:/sys/class/thermal/thermal_zone87 # echo 120000 > trip_point_0_temp ... Unable to handle kernel NULL pointer dereference at virtual address 000000000000 trip_point_temp_store+0xc0/0x1dc dev_attr_store+0x38/0x88 sysfs_kf_write+0x64/0xc0 kernfs_fop_write_iter+0x108/0x1d0 vfs_write+0x2f4/0x368 ksys_write+0x7c/0x el0_svc_common.llvm.7279915941325364641+0xbc/0x1bc do_el0_svc+0x28/0xa0 el0_svc+0x14/0x24 el0_sync_handler+0x88/0xec el0_sync+0x1c0/0x200 While at i of_thermal_get_temp(), of_thermal_set_emul_temp(), of_thermal_get_trend().
CVE-2024-26815	In the Linux kernel, the following vulnerability has been resolved: net/sched: taprio: proper TCA_TAPRIO_TC_ENTRY_INDEX check taprio_parse_tc_entry() is not corr Signed value tc = nla_get_u32(tb[TCA_TAPRIO_TC_ENTRY_INDEX]); if (tc >= TC_QOPT_MAX_QUEUE) { NL_SET_ERR_MSG_MOD(extack, "TC entry index out of negative values: UBSAN: shift-out-of-bounds in net/sched/sch_taprio.c:1722:18 shift exponent -2147418108 is negative CPU: 0 PID: 5066 Comm: syz-executor367 No Google Google Compute Engine/Google Compute Engine, BIOS Google 02/29/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0 [inline] __ubsan_handle_shift_out_of_bounds+0x3c7/0x420 lib/ubsan.c:386 taprio_parse_tc_entry net/sched/sch_taprio.c:1722 [inline] taprio_parse_tc_entries net/sche net/sched/sch_taprio.c:1877 taprio_init+0x9da/0xc80 net/sched/sch_taprio.c:2134 qdisc_create+0x9d4/0x1190 net/sched/sch_api.c:1355 tc_modify_qdisc+0xa26/0x1e net/core/rtnetlink.c:6617 netlink_rcv_skb+0x1e3/0x430 net/netlink/af_netlink.c:2543 netlink_unicast_kernel net/netlink/af_netlink.c:1341 [inline] netlink_unicast+0x7ea/0 net/netlink/af_netlink.c:1908 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x221/0x270 net/socket.c:745 ____sys_sendmsg+0x525/0x7d0 net/socl __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2667 do_syscall_64+0xf9/0x240 entry_SYSCALL_64_after_hwframe+0x6f/0x77 RIP: 0033:0x7f1b2dea3759 Code: 48 83 c 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffd4de452f8 EFLAGS: 00000246 OF 00007f1b2def0390 RCX: 00007f1b2dea3759 RDX: 0000000000000000 RSI: 00000000200007c0 RDI: 0000000000000004 RBP: 0000000000000003 R08: 000055550 0000000000000246 R12: 00007ffd4de45340 R13: 00007ffd4de45310 R14: 0000000000000001 R15: 00007ffd4de45340
CVE-2021-47203	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Fix list_add() corruption in lpfc_drain_txq() When parsing the txq list in lpfc_drain_txq(), the fails, a local "fail_msg" string is set and a log message output. The job is then added to a completions list for cancellation. Processing of any further jobs from the txq lis completions list regardless of whether a wqe was passed to the adapter. If successfully added to txcmplq, jobs are added to both lists resulting in list corruption. Fix by stops the subsequent jobs from being added to the completions list unless they had an appropriate failure.

CVE Number	Description
CVE-2024-27462	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that
CVE-2024-24863	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. CVE-2024-24863 has been replaced by CVE-2024-36014.
CVE-2024-24862	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2021-47205	In the Linux kernel, the following vulnerability has been resolved: clk: sunxi-ng: Unregister clocks/resets when unbinding Currently, unbinding a CCU driver unmaps the registered. This can cause a page fault later when some clock operation tries to perform MMIO. Fix this by separating the CCU initialization from the memory allocation This also fixes a memory leak of the `struct ccu_reset`, and uses the correct owner (the specific platform driver) for the clocks and resets. Early OF clock providers are mostly unchanged. The error reporting is made more consistent by moving the message inside of_sunxi_ccu_probe.
CVE-2021-47212	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Update error handler for UCTX and UMEM In the fast unload flow, the device state is set to In this case, when a destroy command is being executed, it should return MLX5_CMD_STAT_OK. Fix MLX5_CMD_OP_DESTROY_UCTX and MLX5_CMD_OP_DES umem release process - [2633.536695] Call Trace: [2633.537518] ib_uverbs_remove_one+0xc3/0x140 [ib_uverbs] [2633.538596] remove_client_context+0x8b/0xd0 2633.540615] __ib_unregister_device+0x35/0xa0 [ib_core] [2633.541640] ib_unregister_device+0x21/0x30 [ib_core] [2633.542663] __mlx5_ib_remove+0x38/0x90 [m 2633.544661] device_release_driver_internal+0x103/0x1f0 [2633.545679] bus_remove_device+0xf7/0x170 [2633.546640] device_del+0x181/0x410 [2633.547606] m 2633.548777] mlx5_unregister_device+0x27/0x40 [mlx5_core] [2633.549841] mlx5_uninit_one+0x21/0xc0 [mlx5_core] [2633.550864] remove_one+0x69/0xe0 [mlx5_ device_release_driver_internal+0x103/0x1f0 [2633.553746] unbind_store+0xf6/0x130 [2633.554657] kernfs_fop_write+0x116/0x190 [2633.555567] vfs_write+0xa5/0 do_syscall_64+0x5b/0x1a0 [2633.558071] entry_SYSCALL_64_after_hwframe+0x65/0xca [2633.559018] RIP: 0033:0x7f9977132648 [2633.559821] Code: 89 02 48 8b 00 85 c0 75 17 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 58 c3 0f 1f 80 00 00 00 00 41 54 49 89 d4 55 [2633.562332] RSP: 002b:00007fffb1a83888 EFLAGS: 00(ffffffffffffffda RBX: 000000000000000c RCX: 00007f9977132648 [2633.564541] RDX: 000000000000000c RSI: 000055b90546e230 RDI: 0000000000000001 [2633.5 00007f9977a54740 [2633.566653] R10: 0000000000000000 R11: 0000000000000246 R12: 00007f99774056e0 [2633.567692] R13: 000000000000000c R14: 00007 10b4fe52945e544d]---
CVE-2024-26817	In the Linux kernel, the following vulnerability has been resolved: amdkfd: use calloc instead of kzalloc to avoid integer overflow This uses calloc instead of doing the m
CVE-2024-2217	gaizhenbiao/chuanhuchatgpt is vulnerable to improper access control, allowing unauthorized access to the `config.json` file. This vulnerability is present in both authent attackers to obtain sensitive information such as API keys (`openai_api_key`, `google_palm_api_key`, `xmchat_api_key`, etc.), configuration details, and user credentia the `config.json` file, which does not properly restrict access based on user authentication.
CVE-2024-2952	BerriAI/litellm is vulnerable to Server-Side Template Injection (SSTI) via the `/completions` endpoint. The vulnerability arises from the `hf_chat_template` method proces through the Jinja template engine without proper sanitization. Attackers can exploit this by crafting malicious `tokenizer_config.json` files that execute arbitrary code on
CVE-2024-21676	Rejected reason: This CVE's publication may have been a false positive or a mistake. As a result, we have rejected this record.
CVE-2021-47206	In the Linux kernel, the following vulnerability has been resolved: usb: host: ohci-tmio: check return value after calling platform_get_resource() It will cause null-ptr-dere value.
CVE-2021-47207	In the Linux kernel, the following vulnerability has been resolved: ALSA: gus: fix null pointer dereference on pointer block The pointer block return from snd_gf1_dma_n issue. Fix this by adding a null check before dereference.
CVE-2021-47209	In the Linux kernel, the following vulnerability has been resolved: sched/fair: Prevent dead task groups from regaining cfs_rq's Kevin is reporting crashes which point to debugging revealed that we've live cfs_rq's (on_list=1) in an about to be kfree()'d task group in free_fair_sched_group(). However, it was unclear how that can happen. put the 'my_q' member directly into the middle of the object which makes it incidentally overlap with SLUB's freelist pointer. That, in combination with SLAB_FREELIST violation in form of a #GP which made the UAF fail fast. Michal seems to have run into the same issue[1]. He already correctly diagnosed that commit a7b359fc6a37 ("s preconditions for the UAF to happen by re-adding cfs_rq's also to task groups that have no more running tasks, i.e. also to dead ones. His analysis, however, misses th as the real offender is tg_unthrottle_up() getting called via sched_cfs_period_timer() via the timer interrupt at an inconvenient time. When unregister_fair_sched_group(from getting interrupted. If the timer interrupt triggers while we iterate over all CPUs or after unregister_fair_sched_group() has finished but prior to unlinking the task gr groups, trying to unthrottle cfs_rq's, i.e. re-add them to the dying task group. These will later -- in free_fair_sched_group() -- be kfree()'ed while still being linked, leading the dying task group gets unlinked first. However, simply switching the order of unregistering and unlinking the task group isn't sufficient, as concurrent RCU walkers mi do_sched_cfs_period_timer(): : : distribute_cfs_runtime(): : rcu_read_lock(); : : : unthrottle_cfs_rq(): sched_offline_group(): : : walk_tg_tree_from(…,tg_unthrottle_up,.. >children, siblings) : : (2) list_del_rcu(&tg->siblings); : : tg_unthrottle_up(): unregister_fair_sched_group(): struct cfs_rq *cfs_rq = tg->cfs_rq[cpu_of(rq)]; : : list_del_leaf_ >nr_running) (3) : list_add_leaf_cfs_rq(cfs_rq); : : : : : : : : : ---truncated---
CVE-2021-47210	In the Linux kernel, the following vulnerability has been resolved: usb: typec: tipd: Remove WARN_ON in tps6598x_block_read Calling tps6598x_block_read with a hig no need to crash systems with panic-on-warn enabled.
CVE-2021-47211	In the Linux kernel, the following vulnerability has been resolved: ALSA: usb-audio: fix null pointer dereference on pointer cs_desc The pointer cs_desc return from snd dereference issue. Fix this by adding a null check before dereference.

CVE Number	Description
CVE-2024-3863	The executable file warning was not presented when downloading .xrm-ms files. *Note: This issue only affected Windows operating systems. Other operating systems a 115.10, and Thunderbird < 115.10.