SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 21 August 2024

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-42472	Flatpak is a Linux application sandboxing and distribution framework. Prior to versions 1.14.0 and 1.15.10, a malicious or compromised Flatpak app using persistent directories could access and write files outside of what it would otherwise have access to, which is an attack on integrity and confidentiality. When `persistent=subdir` is used in the application permissions (represented as `--persist=subdir` in the command-line interface), that means that an application which otherwise doesn't have access to the real user home directory will see an empty home directory with a writeable subdirectory `subdir`. Behind the scenes, this directory is actually a bind mount and the data is stored in the per-application directory as `~/.var/app/$APPID/subdir`. This allows existing apps that are not aware of the per-application directory to still work as intended without general home directory access. However, the application does have write access to the application directory `~/.var/app/$APPID` where this directory is stored. If the source directory for the `persistent`/`--persist` option is replaced by a symlink, then the next time the application is started, the bind mount will follow the symlink and mount whatever it points to into the sandbox. Partial protection against this vulnerability can be provided by patching Flatpak using the patches in commits ceec2ffc and 98f79773. However, this leaves a race condition that could be exploited by two instances of a malicious app running in parallel. Closing the race condition requires updating or patching the version of bubblewrap that is used by Flatpak to add the new `--bind-fd` option using the patch and then patching Flatpak to use it. If Flatpak has been configured at build-time with `-Dsystem_bubblewrap=bwrap` (1.15.x) or `--with-system-bubblewrap=bwrap` (1.14.x or older), or a similar option, then the version of bubblewrap that needs to be patched is a system copy that is distributed separately, typically `/usr/bin/bwrap`. This configuration is the one that is typically used in Linux distributions. If Flatpak has been configured at build-time with `-Dsystem_bubblewrap=` (1.15.x) or with `--without-system-bubblewrap` (1.14.x or older), then it is the bundled version of bubblewrap that is included with Flatpak that must be patched. This is typically installed as `/usr/libexec/flatpak-bwrap`. This configuration is the default when building from source code. For the 1.14.x stable branch, these changes are included in Flatpak 1.14.10. The bundled version of bubblewrap included in this release has been updated to 0.6.3. For the 1.15.x development branch, these changes are included in Flatpak 1.15.10. The bundled version of bubblewrap in this release is a Meson "wrap" subproject, which has been updated to 0.10.0. The 1.12.x and 1.10.x branches will not be updated for this vulnerability. Long-term support OS distributions should backport the individual changes into their versions of Flatpak and bubblewrap, or update to newer versions if their stability policy allows it. As a workaround, avoid using applications using the `persistent` (`--persist`) permission.	10.0	More Details
CVE-2024-37099	Deserialization of Untrusted Data vulnerability in Liquid Web GiveWP allows Object Injection.This issue affects GiveWP: from n/a through 3.14.1.	10.0	More Details
CVE-2024-6500	The InPost for WooCommerce plugin and InPost PL plugin for WordPress are vulnerable to unauthorized access and deletion of data due to a missing capability check on the 'parse_request' function in all versions up to, and including, 1.4.0 (for InPost for WooCommerce) as well as 1.4.4 (for InPost PL). This makes it possible for unauthenticated attackers to read and delete arbitrary files on Windows servers. On Linux servers, only files within the WordPress install will be deleted, but all files can be read.	10.0	More Details
CVE-2024-5932	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 3.14.1 via deserialization of untrusted input from the 'give_title' parameter. This makes it possible for unauthenticated attackers to inject a PHP Object. The additional presence of a POP chain allows attackers to execute code remotely, and to delete arbitrary files.	10.0	More Details
CVE-2024-43249	Unrestricted Upload of File with Dangerous Type vulnerability in Bit Apps Bit Form Pro allows Command Injection.This issue affects Bit Form Pro: from n/a through 2.6.4.	9.9	More Details
CVE-2024-6847	The Chatbot with ChatGPT WordPress plugin before 2.4.5 does not properly sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by unauthenticated users when submitting messages to the chatbot.	9.8	More Details
CVE-2024-42559	An issue in the login component (process_login.php) of Hotel Management System commit 79d688 allows attackers to authenticate without providing a valid password.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-42558	Hotel Management System commit 91caab8 was discovered to contain a SQL injection vulnerability via the book_id parameter at admin_modify_room.php.	9.8	More Details
CVE-2024-42556	Hotel Management System commit 91caab8 was discovered to contain a SQL injection vulnerability via the room_type parameter at admin_room_removed.php.	9.8	More Details
CVE-2024-43202	Exposure of Remote Code Execution in Apache Dolphinscheduler. This issue affects Apache DolphinScheduler: before 3.2.2. We recommend users to upgrade Apache DolphinScheduler to version 3.2.2, which fixes the issue.	9.8	More Details
CVE-2024-43354	Deserialization of Untrusted Data vulnerability in myCred allows Object Injection.This issue affects myCred: from n/a through 2.7.2.	9.8	More Details
CVE-2024-42563	An arbitrary file upload vulnerability in ERP commit 44bd04 allows attackers to execute arbitrary code via uploading a crafted HTML file.	9.8	More Details
CVE-2024-43311	Improper Privilege Management vulnerability in Geek Code Lab Login As Users allows Privilege Escalation.This issue affects Login As Users: from n/a through 1.4.2.	9.8	More Details
CVE-2024-42815	In the TP-Link RE365 V1_180213, there is a buffer overflow vulnerability due to the lack of length verification for the USER_AGENT field in /usr/bin/httpd. Attackers who successfully exploit this vulnerability can cause the remote target device to crash or execute arbitrary commands.	9.8	More Details
CVE-2024-42813	In TRENDnet TEW-752DRU FW1.03B01, there is a buffer overflow vulnerability due to the lack of length verification for the service field in gena.cgi. Attackers who successfully exploit this vulnerability can cause the remote target device to crash or execute arbitrary commands.	9.8	More Details
CVE-2024-42812	In D-Link DIR-860L v2.03, there is a buffer overflow vulnerability due to the lack of length verification for the SID field in gena.cgi. Attackers who successfully exploit this vulnerability can cause the remote target device to crash or execute arbitrary commands.	9.8	More Details
CVE-2024-42562	Pharmacy Management System commit a2efc8 was discovered to contain a SQL injection vulnerability via the invoice_number parameter at preview.php.	9.8	More Details
CVE-2024-20082	In Modem, there is a possible memory corruption due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: MOLY01182594; Issue ID: MSV-1529.	9.8	More Details
CVE-2024-20083	In venc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08810810 / ALPS08805789; Issue ID: MSV-1502.	9.8	More Details
CVE-2024-42566	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the password parameter at login.php	9.8	More Details
CVE-2024-42567	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the sid parameter at /search.php?action=2.	9.8	More Details
CVE-2024-42568	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the transport parameter at vehicle.php.	9.8	More Details
CVE-2024-42569	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the medium parameter at paidclass.php.	9.8	More Details
CVE-2024-42570	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the medium parameter at admininsert.php.	9.8	More Details
CVE-2024-42571	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the medium parameter at insertattendance.php.	9.8	More Details
CVE-2024-42572	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the medium parameter at unitmarks.php.	9.8	More Details
CVE-2024-42573	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the medium parameter at dtmarks.php.	9.8	More Details
CVE-2024-42574	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the medium parameter at attendance.php.	9.8	More Details
CVE-2024-42575	School Management System commit bae5aa was discovered to contain a SQL injection vulnerability via the medium parameter at substaff.php.	9.8	More Details
CVE-2024-33872	Keyfactor Command 10.5.x before 10.5.1 and 11.5.x before 11.5.1 allows SQL Injection which could result in code execution and escalation of privileges.	9.8	More Details
CVE-2024-30949	An issue in newlib v.4.3.0 allows an attacker to execute arbitrary code via the time unit scaling in the _gettimeofday function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43404	MEGABOT is a fully customized Discord bot for learning and fun. The `/math` command and functionality of MEGABOT versions < 1.5.0 contains a remote code execution vulnerability due to a Python `eval()`. The vulnerability allows an attacker to inject Python code into the `expression` parameter when using `/math` in any Discord channel. This vulnerability impacts any discord guild utilizing MEGABOT. This vulnerability was fixed in release version 1.5.0.	9.8	More Details
CVE-2024-42919	eScan Management Console 14.0.1400.2281 is vulnerable to Incorrect Access Control via acteScanAVReport.	9.8	More Details
CVE-2024-42565	ERP commit 44bd04 was discovered to contain a SQL injection vulnerability via the id parameter at /index.php/basedata/contact/delete?action=delete.	9.8	More Details
CVE-2024-43245	Improper Privilege Management vulnerability in eyecix JobSearch allows Privilege Escalation.This issue affects JobSearch: from n/a through 2.3.4.	9.8	More Details
CVE-2024-42462	Improper Authentication vulnerability in upKeeper Solutions product upKeeper Manager allows Authentication Bypass.This issue affects upKeeper Manager: through 5.1.9.	9.8	More Details
CVE-2024-42466	Improper Restriction of Excessive Authentication Attempts vulnerability in upKeeper Solutions product upKeeper Manager allows Authentication Abuse.This issue affects upKeeper Manager: through 5.1.9.	9.8	More Details
CVE-2024-7731	Dr.ID Access Control System from SECOM does not properly validate a specific page parameter, allowing unauthenticated remote attackers to inject SQL commands to read, modify, and delete database contents.	9.8	More Details
CVE-2024-7732	Dr.ID Access Control System from SECOM does not properly validate a specific page parameter, allowing unauthenticated remote attackers to inject SQL commands to read, modify, and delete database contents.	9.8	More Details
CVE-2024-5914	A command injection issue in Palo Alto Networks Cortex XSOAR CommonScripts Pack allows an unauthenticated attacker to execute arbitrary commands within the context of an integration container.	9.8	More Details
CVE-2024-42360	SequenceServer lets you rapidly set up a BLAST+ server with an intuitive user interface for personal or group use. Several HTTP endpoints did not properly sanitize user input and/or query parameters. This could be exploited to inject and run unwanted shell commands. This vulnerability has been fixed in 3.1.2.	9.8	More Details
CVE-2024-42843	Projectworlds Online Examination System v1.0 is vulnerable to SQL Injection via the subject parameter in feed.php.	9.8	More Details
CVE-2024-42947	An issue in the handler function in /goform/telnet of Tenda FH1201 v1.2.0.14 (408) allows attackers to execute arbitrary commands via a crafted HTTP request.	9.8	More Details
CVE-2024-42966	Incorrect access control in TOTOLINK N350RT V9.3.5u.6139_B20201216 allows attackers to obtain the apmib configuration file, which contains the username and the password, via a crafted request to /cgi-bin/ExportSettings.sh.	9.8	More Details
CVE-2024-42967	Incorrect access control in TOTOLINK LR350 V9.3.5u.6369_B20220309 allows attackers to obtain the apmib configuration file, which contains the username and the password, via a crafted request to /cgi-bin/ExportSettings.sh.	9.8	More Details
CVE-2024-42978	An issue in the handler function in /goform/telnet of Tenda FH1206 v02.03.01.35 allows attackers to execute arbitrary commands via a crafted HTTP request.	9.8	More Details
CVE-2024-23168	Vulnerability in Xiexe XSOverlay before build 647 allows non-local websites to send the malicious commands to the WebSocket API, resulting in the arbitrary code execution.	9.8	More Details
CVE-2024-27730	Insecure Permissions vulnerability in Friendica v.2023.12 allows a remote attacker to obtain sensitive information and execute arbitrary code via the cid parameter of the calendar event feature.	9.8	More Details
CVE-2024-42757	Command injection vulnerability in Asus RT-N15U 3.0.0.4.376_3754 allows a remote attacker to execute arbitrary code via the netstat function page.	9.8	More Details
CVE-2024-6460	The Grow by Tradedoubler WordPress plugin through 2.0.21 is vulnerable to Local File Inclusion via the component parameter. This makes it possible for attackers to include and execute PHP files on the server, allowing the execution of any PHP code in those files.	9.8	More Details
CVE-2024-42465	Improper Restriction of Excessive Authentication Attempts vulnerability in upKeeper Solutions product upKeeper Manager allows Authentication Abuse.This issue affects upKeeper Manager: through 5.1.9.	9.8	More Details
CVE-2024-6800	An XML signature wrapping vulnerability was present in GitHub Enterprise Server (GHES) when using SAML authentication with specific identity providers utilizing publicly exposed signed federation metadata XML. This vulnerability allowed an attacker with direct network access to GitHub Enterprise Server to forge a SAML response to provision and/or gain access to a user with site administrator privileges. Exploitation of this vulnerability would allow unauthorized access to the instance without requiring prior authentication. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.14 and was fixed in versions 3.13.3, 3.12.8, 3.11.14, and 3.10.16. This vulnerability was reported via the GitHub Bug Bounty program.	9.8	More Details
CVE-2024-42634	A Command Injection vulnerability exists in formWriteFacMac of the httpd binary in Tenda AC9 v15.03.06.42. As a result, attacker can execute OS commands with root privileges.	9.8	More Details
CVE-2024-43042	Pluck CMS 4.7.18 does not restrict failed login attempts, allowing attackers to execute a brute force attack.	9.8	More Details
CVE-2024-42637	H3C R3010 v100R002L02 was discovered to contain a hardcoded password vulnerability in /etc/shadow, which allows attackers to log in as root.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6330	The GEO my WP WordPress plugin before 4.5.0.2 does not prevent unauthenticated attackers from including arbitrary files in PHP's execution context, which leads to Remote Code Execution.	9.8	More Details
CVE-2024-44076	In Microcks before 1.10.0, the POST /api/import and POST /api/export endpoints allow non-administrator access.	9.8	More Details
CVE-2024-6459	The News Element Elementor Blog Magazine WordPress plugin before 1.0.6 is vulnerable to Local File Inclusion via the template parameter. This makes it possible for unauthenticated attacker to include and execute PHP files on the server, allowing the execution of any PHP code in those files.	9.8	More Details
CVE-2024-42658	An issue in wishnet Nepstech Wifi Router NTPL-XPON1GFEVN v1.0 allows a remote attacker to obtain sensitive information via the cookie's parameter	9.8	More Details
CVE-2024-42850	An issue in the password change function of Silverpeas v6.4.2 and lower allows for the bypassing of password complexity requirements.	9.8	More Details
CVE-2024-42639	H3C GR1100-P v100R009 was discovered to use a hardcoded password in /etc/shadow, which allows attackers to log in as root.	9.8	More Details
CVE-2024-42638	H3C Magic B1ST v100R012 was discovered to contain a hardcoded password vulnerability in /etc/shadow, which allows attackers to log in as root.	9.8	More Details
CVE-2024-43261	Improper Control of Filename for Include/Require Statement in PHP Program ('PHP Remote File Inclusion') vulnerability in Hamed Naderfar Compute Links allows PHP Remote File Inclusion.This issue affects Compute Links: from n/a through 1.2.1.	9.6	More Details
CVE-2024-38175	An improper access control vulnerability in the Azure Managed Instance for Apache Cassandra allows an authenticated attacker to elevate privileges over a network.	9.6	More Details
CVE-2024-43240	Improper Privilege Management vulnerability in azzaroco Ultimate Membership Pro allows Privilege Escalation.This issue affects Ultimate Membership Pro: from n/a through 12.6.	9.4	More Details
CVE-2024-27185	The pagination class includes arbitrary parameters in links, leading to cache poisoning attack vectors.	9.1	More Details
CVE-2024-38652	Path traversal in the skin management component of Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to achieve denial of service via arbitrary file deletion.	9.1	More Details
CVE-2024-7777	The Contact Form by Bit Form: Multi Step Form, Calculation Contact Form, Payment Contact Form & Custom Contact Form builder plugin for WordPress is vulnerable to arbitrary file read and deletion due to insufficient file path validation in multiple functions in versions 2.0 to 2.13.9. This makes it possible for authenticated attackers, with Administrator-level access and above, to read and delete arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	9.0	More Details
CVE-2024-43242	Deserialization of Untrusted Data vulnerability in azzaroco Ultimate Membership Pro allows Object Injection.This issue affects Ultimate Membership Pro: from n/a through 12.6.	9.0	More Details
CVE-2024-43252	Deserialization of Untrusted Data vulnerability in Crew HRM allows Object Injection.This issue affects Crew HRM: from n/a through 1.1.1.	9.0	More Details
CVE-2024-39397	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution by an attacker. An attacker could exploit this vulnerability by uploading a malicious file which can then be executed on the server. Exploitation of this issue does not require user interaction, but attack complexity is high and scope is changed.	9.0	More Details
CVE-2024-35540	A stored cross-site scripting (XSS) vulnerability in Typecho v1.3.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	9.0	More Details
CVE-2024-43400	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It is possible for a user without Script or Programming rights to craft a URL pointing to a page with arbitrary JavaScript. This requires social engineer to trick a user to follow the URL. This has been patched in XWiki 14.10.21, 15.5.5, 15.10.6 and 16.0.0.	9.0	More Details
CVE-2024-43401	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. A user without script/programming right can trick a user with elevated rights to edit a content with a malicious payload using a WYSIWYG editor. The user with elevated rights is not warned beforehand that they are going to edit possibly dangerous content. The payload is executed at edit time. This vulnerability has been patched in XWiki 15.10RC1.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description
CVE-2024-7829	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-3 DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20 function cgi_del_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. The attack may be initiated rem disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted e product is end-of-life. It should be retired and replaced.

CVE Number	Description
CVE-2024-42580	A Cross-Site Request Forgery (CSRF) in the component edit_group.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges.
CVE-2024-21810	Improper input validation in the Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters before version 28.3 may allow an authenticated u escalation of privilege via local access.
CVE-2024-21807	Improper initialization in the Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters before version 28.3 may allow an authenticated user of privilege via local access.
CVE-2024-42561	Pharmacy Management System commit a2efc8 was discovered to contain a SQL injection vulnerability via the invoice_number parameter at sales_report.php.
CVE-2024-42576	A Cross-Site Request Forgery (CSRF) in the component edit_categorie.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges.
CVE-2024-42577	A Cross-Site Request Forgery (CSRF) in the component add_product.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges.
CVE-2024-42579	A Cross-Site Request Forgery (CSRF) in the component add_group.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges.
CVE-2024-42581	A Cross-Site Request Forgery (CSRF) in the component delete_group.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges.
CVE-2024-42608	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/submit_page.php.
CVE-2024-42582	A Cross-Site Request Forgery (CSRF) in the component delete_categorie.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges.
CVE-2024-42583	A Cross-Site Request Forgery (CSRF) in the component delete_user.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges.
CVE-2024-22218	XML External Entity (XXE) vulnerability in Terminalfour 8.0.0001 through 8.3.18 and XML JDBC versions up to 1.0.4 allows authenticated users to submit malicious XM could lead to various actions such as accessing the underlying server, remote code execution (RCE), or performing Server-Side Request Forgery (SSRF) attacks.
CVE-2024-42584	A Cross-Site Request Forgery (CSRF) in the component delete_product.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges.
CVE-2024-42585	A Cross-Site Request Forgery (CSRF) in the component delete_media.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges.
CVE-2024-42586	A Cross-Site Request Forgery (CSRF) in the component categorie.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges.
CVE-2024-42557	A Cross-Site Request Forgery (CSRF) in the component admin_modify_room.php of Hotel Management System commit 91caab8 allows attackers to escalate privilege
CVE-2024-42555	A Cross-Site Request Forgery (CSRF) in the component admin_room_removed.php of Hotel Management System commit 91caab8 allows attackers to escalate privile
CVE-2024-42554	Hotel Management System commit 91caab8 was discovered to contain a SQL injection vulnerability via the room_type parameter at admin_room_added.php.
CVE-2024-23497	Out-of-bounds write in Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters before version 28.3 may allow an authenticated user to po privilege via local access.

CVE Number	Description
CVE-2024-7827	The Shopping Cart & eCommerce Store plugin for WordPress is vulnerable to boolean-based SQL Injection via the 'model_number' parameter in all versions up to, and insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2024-23981	Wrap-around error in Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters before version 28.3 may allow an authenticated user to pot privilege via local access.
CVE-2024-43247	Missing Authorization vulnerability in creativeon WHMpress allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects WHMpress: from n/a th
CVE-2024-24986	Improper access control in Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters before version 28.3 may allow an authenticated user privilege via local access.
CVE-2024-42633	A Command Injection vulnerability exists in the do_upgrade_post function of the httpd binary in Linksys E1500 v1.0.06.001. As a result, an authenticated attacker can e privileges.
CVE-2024-7909	A vulnerability has been found in TOTOLINK EX1200L 9.3.5u.6146_B20201023 and classified as critical. Affected by this vulnerability is the function setLanguageCfg o bin/cstecgi.cgi. The manipulation of the argument langType leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2024-7908	A vulnerability, which was classified as critical, was found in TOTOLINK EX1200L 9.3.5u.6146_B20201023. Affected is the function setDefResponse of the file /www/cg manipulation of the argument IpAddress leads to stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been disclosed to the public a vendor was contacted early about this disclosure but did not respond in any way.
CVE-2024-7849	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, 322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 202408 cgi_create_album of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument current_path leads to buffer overflow. It is possible to initiate the attack rem disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted e product is end-of-life. It should be retired and replaced.
CVE-2024-7146	The JetTabs for Elementor plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.2.3 via the 'switcher_preset' parameter. This authenticated attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those f access controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.
CVE-2024-7828	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW 323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulr cgi_set_cover of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument album_name leads to buffer overflow. The attack can be initiated remotely. The the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and con life. It should be retired and replaced.
CVE-2024-7145	The JetElements plugin for WordPress is vulnerable to Local File Inclusion in all versions up to, and including, 2.6.20 via the 'progress_type' parameter. This makes it p attackers, with Contributor-level access and above, to include and execute arbitrary files on the server, allowing the execution of any PHP code in those files. This can l controls, obtain sensitive data, or achieve code execution in cases where images and other “safe” file types can be uploaded and included.
CVE-2024-43847	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix invalid memory access while processing fragmented packets The monitor ring and the ring mask index. When the driver receives an interrupt for the reo reinject ring, the monitor ring is also processed, leading to invalid memory access. Since monitor supp the ring mask for the monitor ring should be removed. Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.1.1-00209-QCAHKSWPL_SILICONZ-1
CVE-2024-7646	A security issue was discovered in ingress-nginx where an actor with permission to create Ingress objects (in the `networking.k8s.io` or `extensions` API group) can byp inject arbitrary commands and obtain the credentials of the ingress-nginx controller. In the default configuration, that credential has access to all secrets in the cluster.
CVE-2024-42681	Insecure Permissions vulnerability in xxl-job v.2.4.1 allows a remote attacker to execute arbitrary code via the Sub-Task ID component.
CVE-2024-42553	A Cross-Site Request Forgery (CSRF) in the component admin_room_added.php of Hotel Management System commit 91caab8 allows attackers to escalate privileges
CVE-2024-7830	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, 322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 202408 cgi_move_photo of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument photo_name leads to buffer overflow. It is possible to launch the attack remo disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted e product is end-of-life. It should be retired and replaced.
CVE-2024-42611	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) via admin/admin_page.php?link_id=1&mode=delete
CVE-2024-42616	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_widgets.php?action=remove&widget=Statistics

CVE Number	Description
CVE-2024-42621	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_editor.php
CVE-2024-42676	File Upload vulnerability in Huizhi enterprise resource management system v.1.0 and before allows a remote attacker to execute arbitrary code via the /nssys/common/ Action=DNPageAjaxPostBack component
CVE-2024-4389	The Slider and Carousel slider by Depicter plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the uploadFile function in all 3.1.1. This makes it possible for authenticated attackers, with contributor access or higher, to upload arbitrary files on the affected site's server which may make remote
CVE-2024-43406	LF Edge eKuiper is a lightweight IoT data analytics and stream processing engine running on resource-constraint edge devices. A user could utilize and exploit SQL Inj malicious SQL query via Get method in sqlKvStore. This vulnerability is fixed in 1.14.2.
CVE-2024-42619	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/domain_management.php?id=0&list=whitelist&remove=pligg
CVE-2024-31842	An issue was discovered in Italtel Embrace 1.6.4. The web application inserts the access token of an authenticated user inside GET requests. The query string for the U browser's history, passed through Referers to other web sites, stored in web logs, or otherwise recorded in other sources. If the query string contains sensitive informat then attackers can use this information to launch further attacks. Because the access token in sent in GET requests, this vulnerability could lead to complete account ta
CVE-2024-7832	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-32 326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affec cgi_get_fullscreen_photos of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument user leads to buffer overflow. The attack may be launched remotel disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted e product is end-of-life. It should be retired and replaced.
CVE-2024-42612	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/domain_management.php?whitelist_add
CVE-2024-42613	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_widgets.php?action=install&widget=akismet
CVE-2024-42610	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_backup.php?dobackup=files
CVE-2024-42618	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /module.php?module=karma
CVE-2024-42609	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_backup.php?dobackup=avatars
CVE-2024-42607	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_backup.php?dobackup=database
CVE-2024-42606	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_log.php?clear=1
CVE-2024-42605	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/edit_page.php?link_id=1
CVE-2024-42362	Hertzbeat is an open source, real-time monitoring system. Hertzbeat has an authenticated (user role) RCE via unsafe deserialization in /api/monitors/import. This vulne
CVE-2024-42604	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_group.php?mode=delete&group_id=3
CVE-2024-42363	Prior to 3385, the user-controlled role parameter enters the application in the Kubernetes::RoleVerificationsController. The role parameter flows into the RoleConfigFile Kubernetes::Util.parse_file method where it is unsafely deserialized using the YAML.load_stream method. This issue may lead to Remote Code Execution (RCE). This
CVE-2024-42603	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_backup.php?dobackup=clearall

CVE Number	Description
CVE-2024-43403	Kanister is a data protection workflow management tool. The kanister has a deployment called default-kanister-operator, which is bound with a ClusterRole called edit v ClusterRole is one of Kubernetes default-created ClusterRole, and it has the create/patch/udpate verbs of daemonset resources, create verb of serviceaccount/token re of serviceaccounts resources. A malicious user can leverage access the worker node which has this component to make a cluster-level privilege escalation.
CVE-2024-7831	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DN DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. the function cgi_get_cooliris of the file /cgi-bin/photocenter_mgr.cgi. The manipulation of the argument path leads to buffer overflow. The attack can be launched remot disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted e product is end-of-life. It should be retired and replaced.
CVE-2024-42617	Pligg CMS v2.0.2 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/admin_config.php?action=save&var_id=32
CVE-2024-7782	The Contact Form by Bit Form: Multi Step Form, Calculation Contact Form, Payment Contact Form & Custom Contact Form builder plugin for WordPress is vulnerable insufficient file path validation in the iconRemove function in versions 2.0 to 2.13.4. This makes it possible for authenticated attackers, with Administrator-level access a on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).
CVE-2024-6378	A reflected Cross-site Scripting (XSS) vulnerability affecting ENOVIA Collaborative Industry Innovator from Release 3DEXPERIENCE R2022x through Release 3DEXP attacker to execute arbitrary script code in user's browser session.
CVE-2024-43248	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Bit Apps Bit Form Pro allows File Manipulation.This issue affects Bit Form
CVE-2024-43357	ECMA-262 is the language specification for the scripting language ECMAScript. A problem in the ECMAScript (JavaScript) specification of async generators, introduce may lead to mis-implementation in a way that could present as a security vulnerability, such as type confusion and pointer dereference. The internal async generator m resolver functions on IteratorResult (`{ done, value }`) objects that it creates, assuming that the IteratorResult objects will not be then-ables. Unfortunately, these Iterato `Object.prototype`, so these IteratorResult objects can be made then-able, triggering arbitrary behaviour, including re-entering the async generator machinery in a way invariants. The ECMAScript specification is a living standard and the issue has been addressed at the time of this advisory's public disclosure. JavaScript engine imple specification and update their implementations to comply with the `AsyncGenerator` section. ## References - https://github.com/tc39/ecma262/commit/1e24a286d0a327d08e1154926b3ee79820232727 - https://bugzilla.mozilla.org/show_bug.cgi?id=1901411 - https://github.com dev/boa/security/advisories/GHSA-f67q-wr6w-23jq - https://bugs.webkit.org/show_bug.cgi?id=275407 - https://issues.chromium.org/issues/346692561 - https://www.cv 7652
CVE-2024-42552	Hotel Management System commit 91caab8 was discovered to contain a SQL injection vulnerability via the book_id parameter at admin_room_history.php.
CVE-2024-43232	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WP OnlineSupport, Essential Plugin Timeline and History slider allows PH affects Timeline and History slider: from n/a through 2.3.
CVE-2024-43221	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Crocoblock JetGridBuilder allows PHP Local File Inclusion.This issue affe through 1.1.2.
CVE-2024-43145	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in AyeCode Ltd GeoDirectory.This issue affects GeoDirectory: fro
CVE-2024-39825	Buffer overflow in some Zoom Workplace Apps and Rooms Clients may allow an authenticated user to conduct an escalation of privilege via network access.
CVE-2024-43286	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Squirrly SEO Plugin by Squirrly SEO.This issue affects SEO Pl through 12.3.19.
CVE-2024-43207	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Valiano Unite Gallery Lite.This issue affects Unite Gallery Lite: f
CVE-2024-43271	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Themelocation Woo Products Widgets For Elementor allows PHP Local Fi Woo Products Widgets For Elementor: from n/a through 2.0.0.
CVE-2024-44067	The T-Head XuanTie C910 CPU in the TH1520 SoC and the T-Head XuanTie C920 CPU in the SOPHON SG2042 have instructions that allow unprivileged attackers t memory locations, aka GhostWrite.
CVE-2024-39690	Capsule is a multi-tenancy and policy-based framework for Kubernetes. In Capsule v0.7.0 and earlier, the tenant-owner can patch any arbitrary namespace that has no (i.e., namespaces without the ownerReference field), thereby gaining control of that namespace.

CVE Number	Description
CVE-2024-39401	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command (vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed.
CVE-2024-39402	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Neutralization of Special Elements used in an OS Command (vulnerability that could lead in arbitrary code execution by an admin attacker. Exploitation of this issue requires user interaction and scope is changed.
CVE-2024-42995	VTiger CRM <= 8.1.0 does not correctly check user privileges. A low-privileged user can interact directly with the "Migration" administrative module to disable arbitrary r
CVE-2024-43328	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in WPDeveloper EmbedPress allows PHP Local File Inclusion.This issue affe through 4.0.9.
CVE-2024-43395	CraftOS-PC 2 is a rewrite of the desktop port of CraftOS from the popular Minecraft mod ComputerCraft using C++ and a modified version of PUC Lua, as well as SDL 2.8.3, users of CraftOS-PC 2 on Windows can escape the computer folder and access files anywhere without permission or notice by obfuscating `..`s to bypass the int directory traversal. Version 2.8.3 contains a patch for this issue.
CVE-2024-42336	Servision - CWE-287: Improper Authentication
CVE-2024-7868	In Xpdf 4.05 (and earlier), invalid header info in a DCT (JPEG) stream can lead to an uninitialized variable in the DCT decoder. The proof-of-concept PDF file causes a an invalid address.
CVE-2024-28947	Improper input validation in kernel mode driver for some Intel(R) Server Board S2600ST Family firmware before version 02.01.0017 may allow a privileged user to pote privilege via local access.
CVE-2024-6377	An URL redirection to untrusted site (open redirect) vulnerability affecting 3DPassport in 3DSwymer from Release 3DEXPERIENCE R2022x through Release 3DEXPE attacker to redirect users to an arbitrary website via a crafted URL.
CVE-2024-41657	Casdoor is a UI-first Identity and Access Management (IAM) / Single-Sign-On (SSO) platform. In Casdoor 1.577.0 and earlier, a logic vulnerability exists in the beego fil website to make cross domain requests to Casdoor as the logged in user. Due to the a logic error in checking only for a prefix when authenticating the Origin header, a subdomain with a valid subdomain prefix (Ex: localhost.example.com), allowing the website to make requests to Casdoor as the current signed-in user.
CVE-2024-41659	memos is a privacy-first, lightweight note-taking service. A CORS misconfiguration exists in memos 0.20.1 and earlier where an arbitrary origin is reflected with Access- true. This may allow an attacking website to make a cross-origin request, allowing the attacker to read private information or make privileged changes to the system as This vulnerability is fixed in 0.21.0.
CVE-2024-39400	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. This vulnerability co inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a vi Confidentiality and integrity impact is high as it affects other admin accounts.
CVE-2023-0714	The Metform Elementor Contact Form Builder for WordPress is vulnerable to Arbitrary File Upload due to insufficient file type validation in versions up to, and including, unauthenticated visitors to perform a "double extension" attack and upload files containing a malicious extension but ending with a benign extension, which may make r in some configurations.
CVE-2024-7628	The MStore API – Create Native Android & iOS Apps On The Cloud plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 4.15.2 comparison in the 'verify_id_token' function. This makes it possible for unauthenticated attackers to log in as any existing user on the site, such as an administrator, if th email address or phone number. This also requires firebase to be configured on the website and the user to have set up firebase for their account.
CVE-2024-7624	The Zephyr Project Manager plugin for WordPress is vulnerable to limited privilege escalation in all versions up to, and including, 3.3.101. This is due to the plugin not p capabilities before allowing them to enable access to the plugin's settings through the update_user_access() function. This makes it possible for authenticated attackers and above, to grant themselves full access to the plugin's settings.
CVE-2024-42578	A Cross-Site Request Forgery (CSRF) in the component edit_product.php of Warehouse Inventory System v2.0 allows attackers to escalate privileges.
CVE-2024-43399	Mobile Security Framework (MobSF) is a pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis. Before Libraries analysis section. Specifically, during the extraction of .a extension files, the measure intended to prevent Zip Slip attacks is improperly implemented. Since the bypassed, the vulnerability allows an attacker to extract files to any desired location within the server running MobSF. This vulnerability is fixed in 4.0.7.
CVE-2024-25576	improper access control in firmware for some Intel(R) FPGA products before version 24.1 may allow a privileged user to enable escalation of privilege via local access.
CVE-2024-42280	In the Linux kernel, the following vulnerability has been resolved: mISDN: Fix a use after free in hfcmulti_tx() Don't dereference *sp after calling dev_kfree_skb(*sp).

CVE Number	Description
CVE-2024-39423	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds write vulnerability that could result in context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-39422	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Use After Free vulnerability that could result in arbitra of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-7263	Improper path validation in promecefpluginhost.exe in Kingsoft WPS Office version ranging from 12.2.0.13110 to 12.2.0.17115 (exclusive) on Windows allows an attack library. The patch released in version 12.1.0.17119 to mitigate CVE-2024-7262 was not restrictive enough. Another parameter was not properly sanitized which leads to Windows library.
CVE-2024-2175	An insecure permissions vulnerability was reported in Lenovo Display Control Center (LDCC) and Lenovo Accessories and Display Manager (LADM) that could allow a privileges.
CVE-2024-41831	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Use After Free vulnerability that could result in arbitra of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-41830	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Use After Free vulnerability that could result in arbitra of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-4763	An insecure driver vulnerability was reported in Lenovo Display Control Center (LDCC) and Lenovo Accessories and Display Manager (LADM) that could allow a local a kernel.
CVE-2024-39424	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Use After Free vulnerability that could result in arbitra of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-34738	In multiple functions of AppOpsService.java, there is a possible way for unprivileged apps to read their own restrictRead app-op states due to a logic error in the code. T of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2024-42284	In the Linux kernel, the following vulnerability has been resolved: tipc: Return non-zero value from tipc_udp_addr2str() on error tipc_udp_addr2str() should return non-z address is invalid. Otherwise, a buffer overflow access can occur in tipc_media_addr_printf(). Fix this by returning 1 on an invalid UDP media address.
CVE-2024-5915	A privilege escalation (PE) vulnerability in the Palo Alto Networks GlobalProtect app on Windows devices enables a local user to execute programs with elevated privile
CVE-2024-39426	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability when parsing a cra read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this is that a victim must open a malicious file.
CVE-2024-7886	A vulnerability has been found in Scooter Software Beyond Compare up to 3.3.5.15075 and classified as critical. Affected by this vulnerability is an unknown functionali manipulation leads to uncontrolled search path. Attacking locally is a requirement. The real existence of this vulnerability is still doubted at the moment. NOTE: The ven be breached before exploiting this issue.
CVE-2024-42271	In the Linux kernel, the following vulnerability has been resolved: net/iucv: fix use after free in iucv_sock_close() iucv_sever_path() is called from process context and fr used as indicator whether somebody else is taking care of severing the path (or it is already removed / never existed). This needs to be done with atomic compare and window where iucv_sock_close() will try to work with a path that has already been severed and freed by iucv_callback_connrej() called by iucv_tasklet_fn(). Example: [4 [452744.123845] ([<0000001e87f03880>] 0x1e87f03880) [452744.123966] [<00000000d593001e>] iucv_path_sever+0x96/0x138 [452744.124330] [<000003ff801ddbc [af_iucv] [452744.124336] [<000003ff801e01b6>] iucv_sock_close+0xa6/0x310 [af_iucv] [452744.124341] [<000003ff801e08cc>] iucv_sock_release+0x3c/0xd0 [af_iuc [<00000000d574794e>] __sock_release+0x5e/0xe8 [452744.124815] [<00000000d5747a0c>] sock_close+0x34/0x48 [452744.124820] [<00000000d5421642>] __fput [<00000000d51b382c>] task_work_run+0xbc/0xf0 [452744.124832] [<00000000d5145710>] do_notify_resume+0x88/0x90 [452744.124841] [<00000000d5978096>] s [452744.125319] Last Breaking-Event-Address: [452744.125321] [<00000000d5930018>] iucv_path_sever+0x90/0x138 [452744.125324] [452744.125325] Kernel pan in interrupt Note that bh_lock_sock() is not serializing the tasklet context against process context, because the check for sock_owned_by_user() and corresponding har future clean-up patch: A) Correct usage of bh_lock_sock() in tasklet context, as described in Re-enqueue, if needed. This may require adding return values to the taskle all users of iucv. B) Change iucv tasklet into worker and use only lock_sock() in af_iucv.
CVE-2024-34734	In onForegroundServiceButtonClicked of FooterActionsViewModel.kt, there is a possible way to disable the active VPN app from the lockscreen due to an insecure defa local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2024-41840	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current us requires user interaction in that a victim must open a malicious file.
CVE-2024-34736	In setupVideoEncoder of StagefrightRecorder.cpp, there is a possible asynchronous playback when B-frame support is enabled. This could lead to local escalation of p execution privileges needed. User interaction is not needed for exploitation.

CVE Number	Description
CVE-2024-42679	SQL Injection vulnerability in Super easy enterprise management system v.1.0.0 and before allows a local attacker to execute arbitrary code via a crafted script to the/a
CVE-2024-31333	In _MMU_AllocLevel of mmu_common.c, there is a possible arbitrary code execution due to an integer overflow. This could lead to local escalation of privilege in the ke privileges needed. User interaction is not needed for exploitation.
CVE-2024-34739	In shouldRestrictOverlayActivities of UsbProfileGroupSettingsManager.java, there is a possible escape from SUW due to a logic error in the code. This could lead to loc additional execution privileges needed. User interaction is needed for exploitation.
CVE-2024-34740	In attributeBytesBase64 and attributeBytesHex of BinaryXmlSerializer.java, there is a possible arbitrary XML injection due to an integer overflow. This could lead to loca additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2024-34741	In setForceHideNonSystemOverlayWindowIfNeeded of WindowState.java, there is a possible way for message content to be visible on the screensaver while lock scre by the user due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed
CVE-2024-34743	In setTransactionState of SurfaceFlinger.cpp, there is a possible way to perform tapjacking due to a logic error in the code. This could lead to local escalation of privileg privileges needed. User interaction is not needed for exploitation.
CVE-2024-42301	In the Linux kernel, the following vulnerability has been resolved: dev/parport: fix the array out-of-bounds risk Fixed array out-of-bounds issues caused by sprintf by rep data copying, ensuring the destination buffer is not overflowed. Below is the stack trace I encountered during the actual issue: [66.575408s] [pid:5118,cpu4,QThread,4 stack-protector: Kernel stack is corrupted in: do_hardware_base_addr+0xcc/0xd0 [parport] [66.575408s] [pid:5118,cpu4,QThread,5]CPU: 4 PID: 5118 Comm: QThrea arm64-desktop #7100.57021.2 [66.575439s] [pid:5118,cpu4,QThread,6]TGID: 5087 Comm: EFileApp [66.575439s] [pid:5118,cpu4,QThread,7]Hardware name: HUAV W515x-B081/SP1PANGUXM, BIOS 1.00.07 04/29/2024 [66.575439s] [pid:5118,cpu4,QThread,8]Call trace: [66.575469s] [pid:5118,cpu4,QThread,9] dump_backtrace [pid:5118,cpu4,QThread,0] show_stack+0x14/0x20 [66.575469s] [pid:5118,cpu4,QThread,1] dump_stack+0xd4/0x10c [66.575500s] [pid:5118,cpu4,QThread,2] panic [pid:5118,cpu4,QThread,3] __stack_chk_fail+0x2c/0x38 [66.575500s] [pid:5118,cpu4,QThread,4] do_hardware_base_addr+0xcc/0xd0 [parport]
CVE-2024-41865	Dimension versions 3.4.11 and earlier are affected by an Untrusted Search Path vulnerability that could lead to arbitrary code execution. An attacker could exploit this v malicious file into the search path, which the application might execute instead of the legitimate file. This could occur if the application uses a search path to locate exec of this issue requires user interaction.
CVE-2024-41856	Illustrator versions 28.5, 27.9.4, 28.6, 27.9.5 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the con Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-43378	calamares-nixos-extensions provides Calamares branding and modules for NixOS, a distribution of GNU/Linux. Users who installed NixOS through the graphical install partitioning to create a setup where the system was booted via legacy BIOS rather than UEFI; some disk partitions are encrypted; but the partitions containing either `/` their LUKS disk encryption key file in plain text either in `/crypto_keyfile.bin`, or in a CPIO archive attached to their NixOS initrd. `nixos-install` is not affected, nor are UI default automatic partitioning configuration on legacy BIOS systems. The problem has been fixed in calamares-nixos-extensions 0.3.17, which was included in NixOS. ` the NixOS 24.05 and unstable (24.11) channels are unaffected. The fix reached 24.05 at 2024-08-13 20:06:59 UTC, and unstable at 2024-08-15 09:00:20 UTC. Installe those times may be vulnerable. The best solution for affected users is probably to back up their data and do a complete reinstallation. However, the mitigation procedur should work solely for the case where `/` is encrypted but `/boot` is not. If `/` is unencrypted, then the `/crypto_keyfile.bin` file will need to be deleted in addition to the re advisory. This issue is a partial regression of CVE-2023-36476 / GHSA-3rvf-24q2-24ww, which was more severe as it applied to the default configuration on BIOS syste
CVE-2024-41853	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the cc Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-7262	Improper path validation in promecefpluginhost.exe in Kingsoft WPS Office version ranging from 12.2.0.13110 to 12.2.0.16412 (exclusive) on Windows allows an attack library. The vulnerability was found weaponized as a single-click exploit in the form of a deceptive spreadsheet document
CVE-2024-41852	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the cc Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-41851	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in t Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-34737	In ensureSetPipAspectRatioQuotaTracker of ActivityClientController.java, there is a possible way to generate unmovable and undeletable pip windows due to a logic er to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2024-41850	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the cc Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-42285	In the Linux kernel, the following vulnerability has been resolved: RDMA/iwcm: Fix a use-after-free related to destroying CM IDs iw_conn_req_handler() associates a ne (conn_id) with an existing struct iw_cm_id (cm_id) as follows: conn_id->cm_id.iw = cm_id; cm_id->context = conn_id; cm_id->cm_handler = cma_iw_handler; rdma_de and the struct rdma_id_private. Make sure that cm_work_handler() does not trigger a use-after-free by only freeing of the struct rdma_id_private after all pending work

CVE Number	Description
CVE-2024-38163	Windows Update Stack Elevation of Privilege Vulnerability
CVE-2024-39394	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-43843	In the Linux kernel, the following vulnerability has been resolved: riscv, bpf: Fix out-of-bounds issue when preparing trampoline image We get the size of the trampoline and allocate memory based on that size. The allocated image will then be populated with instructions during the real patch phase. But after commit 26ef208c209a ("bpf arch_bpf_trampoline_size"), the `im` argument is inconsistent in the dry run and real patch phase. This may cause emit_imm in RV64 to generate a different number of 'im' address, potentially causing out-of-bounds issues. Let's emit the maximum number of instructions for the "im" address during dry run to fix this problem.
CVE-2024-41858	InCopy versions 18.5.2, 19.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of th this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-41864	Substance3D - Designer versions 13.1.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the issue requires user interaction in that a victim must open a malicious file.
CVE-2024-39393	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victi
CVE-2023-42667	Improper isolation in the Intel(R) Core(TM) Ultra Processor stream cache mechanism may allow an authenticated user to potentially enable escalation of privilege via lo
CVE-2023-49141	Improper isolation in some Intel(R) Processors stream cache mechanism may allow an authenticated user to potentially enable escalation of privilege via local access.
CVE-2024-28829	Least privilege violation and reliance on untrusted inputs in the mk_informix Checkmk agent plugin before Checkmk 2.3.0p12, 2.2.0p32, 2.1.0p47 and 2.0.0 (EOL) allow privileges.
CVE-2024-7305	A maliciously crafted DWF file, when parsed in AdDwfPdk.dll through Autodesk AutoCAD, can force an Out-of-Bounds Write. A malicious actor can leverage this vulner sensitive data, or execute arbitrary code in the context of the current process.
CVE-2024-32927	In sendDeviceState_1_6 of RadioExt.cpp, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional ex interaction is not needed for exploitation.
CVE-2024-26022	Improper access control in some Intel(R) UEFI Integrator Tools on Aptio V for Intel(R) NUC may allow an authenticated user to potentially enable escalation of privilege
CVE-2024-20789	Dimension versions 3.4.11 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Explo interaction in that a victim must open a malicious file.
CVE-2024-34117	Photoshop Desktop versions 24.7.3, 25.9.1 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the cu issue requires user interaction in that a victim must open a malicious file.
CVE-2024-43858	In the Linux kernel, the following vulnerability has been resolved: jfs: Fix array-index-out-of-bounds in diFree
CVE-2024-43852	In the Linux kernel, the following vulnerability has been resolved: hwmon: (ltc2991) re-order conditions to fix off by one bug LTC2991_T_INT_CH_NR is 4. The st->temp LTC2991_MAX_CHANNEL (4) elements. Thus if "channel" is equal to LTC2991_T_INT_CH_NR then we have read one element beyond the end of the array. Flip the c check if "channel" is valid before using it as an array index.
CVE-2024-34124	Dimension versions 3.4.11 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. requires user interaction in that a victim must open a malicious file.
CVE-2024-34133	Illustrator versions 28.5, 27.9.4 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 requires user interaction in that a victim must open a malicious file.
CVE-2024-39390	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of this issue requires user interaction in that a victim must open a malicious file.

CVE Number	Description
CVE-2024-43842	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: Fix array index mistake in rtw89_sta_info_get_iter() In rtw89_sta_info_get_iter() 'status->h But then 'rate->he_gi' is used as array index instead of 'status->he_gi'. This can lead to go beyond array boundaries in case of 'rate->he_gi' is not equal to 'status->he_ Looks like "copy-paste" mistake. Fix this mistake by replacing 'rate->he_gi' with 'status->he_gi'. Found by Linux Verification Center (linuxtesting.org) with SVACE.
CVE-2024-39389	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the c Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-39388	Substance3D - Stager versions 3.0.2 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current u requires user interaction in that a victim must open a malicious file.
CVE-2024-42302	In the Linux kernel, the following vulnerability has been resolved: PCI/DPC: Fix use-after-free on concurrent DPC and hot-removal Keith reports a use-after-free when a to hot-removal of the same portion of the hierarchy: The dpc_handler() awaits readiness of the secondary bus below the Downstream Port where the DPC event occurr space of the first child device on the secondary bus. If that child device is concurrently removed, accesses to its struct pci_dev cause the kernel to oops. That's becaus pci_bridge_wait_for_secondary_bus() neglects to hold a reference on the child device. Before v6.3, the function was only called on resume from system sleep or on run reference wasn't necessary back then because the pciehp IRQ thread could never run concurrently. (On resume from system sleep, IRQs are not enabled until after the runtime resume is always awaited before a PCI device is removed.) However starting with v6.3, pci_bridge_wait_for_secondary_bus() is also called on a DPC event. C ("PCI/DPC: Await readiness of secondary bus after reset"), which introduced that, failed to appreciate that pci_bridge_wait_for_secondary_bus() now needs to hold a re because dpc_handler() and pciehp may indeed run concurrently. The commit was backported to v5.10+ stable kernels, so that's the oldest one affected. Add the missir Abridged stack trace: BUG: unable to handle page fault for address: 00000000091400c0 CPU: 15 PID: 2464 Comm: irq/53-pcie-dpc 6.9.0 RIP: pci_bus_read_config_d pci_bridge_wait_for_secondary_bus() dpc_reset_link() pcie_do_recovery() dpc_handler()
CVE-2024-39383	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Use After Free vulnerability that could result in arbitra of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-42313	In the Linux kernel, the following vulnerability has been resolved: media: venus: fix use after free in vdec_close There appears to be a possible use after free with vdec_ buffer release work to the work queue through HFI callbacks as a normal part of decoding. Randomly closing the decoder device from userspace during normal decodi inst. Fix it by cancelling the work in vdec_close.
CVE-2024-42314	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix extent map use-after-free when adding pages to compressed bio At add_ra_bio_pages() we a calculate 'add_size' after we dropped our reference on the extent map, resulting in a use-after-free. Fix this by computing 'add_size' before dropping our extent map ref
CVE-2024-39386	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current us requires user interaction in that a victim must open a malicious file.
CVE-2024-39391	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-43839	In the Linux kernel, the following vulnerability has been resolved: bna: adjust 'name' buf size of bna_tcb and bna_ccb structures To have enough space to write all poss 'name' size is 16, but the first '%s' specifier may already need at least 16 characters, since 'bnad->netdev->name' is used there. For '%d' specifiers, assume that they re tx_info->tcb[i]->id' sum, BNAD_MAX_TXQ_PER_TX is 8 * 2 chars for 'rx_id + rx_info->rx_ctrl[i].ccb->id', BNAD_MAX_RXP_PER_RX is 16 And replace sprintf with snp analysis tool - Svace.
CVE-2024-43825	In the Linux kernel, the following vulnerability has been resolved: iio: Fix the sorting functionality in iio_gts_build_avail_time_table The sorting in iio_gts_build_avail_time intended. It could result in an out-of-bounds access when the time is zero. Here are more details: 1. When the gts->itime_table[i].time_us is zero, e.g., the time sequenc will not terminate and do out-of-bound writes. This is because once `times[j] > new`, the value `new` will be added in the current position and the `times[j]` will be moved the if-condition always hold. Meanwhile, idx will be added one, making the loop keep running without termination and out-of-bound write. 2. If none of the gts->itime_tab elements will just be copied without being sorted as described in the comment "Sort times from all tables to one and remove duplicates". For more details, please refer https://lore.kernel.org/all/6dd0d822-046c-4dd2-9532-79d7ab96ec05@gmail.com.
CVE-2024-43373	webcrack is a tool for reverse engineering javascript. An arbitrary file write vulnerability exists in the webcrack module when processing specifically crafted malicious co vulnerability is triggered when using the unpack bundles feature in conjunction with the saving feature. If a module name includes a path traversal sequence with Windo can exploit this to overwrite files on the host system. This vulnerability allows an attacker to write arbitrary `.js` files to the host system, which can be leveraged to hijack gain arbitrary code execution. This vulnerability has been patched in version 2.14.1.
CVE-2024-39399	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Trav lead to arbitrary file system read. A low-privileged attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. E require user interaction and scope is changed.
CVE-2024-6379	A reflected Cross-site Scripting (XSS) vulnerability affecting 3DSwymer from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2024x allows an a code in user's browser session.
CVE-2024-42564	ERP commit 44bd04 was discovered to contain a SQL injection vulnerability via the id parameter at /index.php/basedata/inventory/delete?action=delete.
CVE-2024-43282	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Themeum Tutor LMS.This issue affects Tutor LMS: from n/a thr

CVE Number	Description
CVE-2024-4785	BT: Missing Check in LL_CONNECTION_UPDATE_IND Packet Leads to Division by Zero
CVE-2024-39403	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. (to the attacker being able to exfiltrate sensitive information.
CVE-2024-42945	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromAddressNat function. This vulnerability allows attackers to via a crafted POST request.
CVE-2024-42954	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromwebExcptypemanFilter function. This vulnerability allows Service (DoS) via a crafted POST request.
CVE-2024-42953	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the PPW parameter in the fromWizardHandle function. This vulnerability allows attackers (DoS) via a crafted POST request.
CVE-2024-42952	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromqossetting function. This vulnerability allows attackers to via a crafted POST request.
CVE-2024-42951	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the mit_pptpusrpw parameter in the fromWizardHandle function. This vulnerability allows Service (DoS) via a crafted POST request.
CVE-2024-27187	Improper Access Controls allows backend users to overwrite their username when disallowed.
CVE-2024-42950	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the Go parameter in the fromSafeClientFilter function. This vulnerability allows attackers (DoS) via a crafted POST request.
CVE-2024-42949	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the qos parameter in the fromqossetting function. This vulnerability allows attackers to ca via a crafted POST request.
CVE-2024-42948	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the delno parameter in the fromPptpUserSetting function. This vulnerability allows attack (DoS) via a crafted POST request.
CVE-2024-42946	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromVirtualSer function. This vulnerability allows attackers to c via a crafted POST request.
CVE-2024-42944	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromNatlimit function. This vulnerability allows attackers to cau a crafted POST request.
CVE-2024-34458	Keyfactor Command 10.5.x before 10.5.1 and 11.5.x before 11.5.1 allows SQL Injection which could result in information disclosure.
CVE-2024-42943	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the PPPOEPassword parameter in the fromAdvSetWan function. This vulnerability allow Service (DoS) via a crafted POST request.
CVE-2024-42361	Hertzbeat is an open source, real-time monitoring system. Hertzbeat 1.6.0 and earlier declares a /api/monitor/{monitorId}/metric/{metricFull} endpoint to download job m executes a SQL query with user-controlled data, allowing for SQL injection.
CVE-2024-42662	An issue in apollocongif apollo v.2.2.0 allows a remote attacker to obtain sensitive information via a crafted request.
CVE-2024-42942	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the frmL7ImForm function. This vulnerability allows attackers to ca via a crafted POST request.
CVE-2024-42941	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the wanmode parameter in the fromAdvSetWan function. This vulnerability allows attack (DoS) via a crafted POST request.

CVE Number	Description
CVE-2024-42006	Keyfactor AWS Orchestrator through 2.0 allows Information Disclosure.
CVE-2024-42940	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromP2pListFilter function. This vulnerability allows attackers t (DoS) via a crafted POST request.
CVE-2024-42968	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the Go parameter in the fromSafeUrlFilter function. This vulnerability allows attackers to ca a crafted POST request.
CVE-2024-42955	Tenda FH1201 v1.2.0.14 (408) was discovered to contain a stack overflow via the page parameter in the fromSafeClientFilter function. This vulnerability allows attacke (DoS) via a crafted POST request.
CVE-2024-42980	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the frmL7ImForm function. This vulnerability allows attackers to cau a crafted POST request.
CVE-2024-42969	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromSafeUrlFilter function. This vulnerability allows attackers to via a crafted POST request.
CVE-2024-42973	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromSetIpBind function. This vulnerability allows attackers to cau a crafted POST request.
CVE-2024-6221	A vulnerability in corydolphin/flask-cors version 4.0.1 allows the `Access-Control-Allow-Private-Network` CORS header to be set to true by default, without any configur expose private network resources to unauthorized external access, leading to significant security risks such as data breaches, unauthorized access to sensitive informa intrusions.
CVE-2024-43315	Authorization Bypass Through User-Controlled Key vulnerability in Checkout Plugins Stripe Payments For WooCommerce by Checkout.This issue affects Stripe Payme Checkout: from n/a through 1.9.1.
CVE-2024-44069	Pi-hole before 6 allows unauthenticated admin/api.php?setTempUnit= calls to change the temperature units of the web dashboard. NOTE: the supplier reportedly does issue" but the specific motivation for letting arbitrary persons change the value (Celsius, Fahrenheit, or Kelvin), seen by the device owner, is unclear.
CVE-2024-44070	An issue was discovered in FRRouting (FRR) through 10.1. bgp_attr_encap in bgpd/bgp_attr.c does not check the actual remaining stream length before taking the TL
CVE-2024-44073	The Miniscript (aka rust-miniscript) library before 12.2.0 for Rust allows stack consumption because it does not properly track tree depth.
CVE-2024-44083	ida64.dll in Hex-Rays IDA Pro through 8.4 crashes when there is a section that has many jumps linked, and the final jump corresponds to the payload from where the a NOTE: in many use cases, this is an inconvenience but not a security issue.
CVE-2024-6348	Predictable seed generation in the security access mechanism of UDS in the Blind Spot Protection Sensor ECU in Nissan Altima (2022) allows attackers to predict the security controls via repeated ECU resets and seed requests.
CVE-2024-42657	An issue in wishnet Nepstech Wifi Router NTPL-XPON1GFEVN v1.0 allows a remote attacker to obtain sensitive information via the lack of encryption during login proc
CVE-2024-7592	There is a LOW severity vulnerability affecting CPython, specifically the 'http.cookies' standard library module. When parsing cookies that contained backslashes for qu value, the parser would use an algorithm with quadratic complexity, resulting in excess CPU resources being used while parsing the value.
CVE-2024-43345	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in PluginOps Landing Page Builder allows PHP Local File Inclusion.This issu from n/a through 1.5.2.0.
CVE-2024-34727	In sdpu_compare_uuid_with_attr of sdp_utils.cc, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure privileges needed. User interaction is not needed for exploitation.
CVE-2024-41700	Barix – CWE-200 Exposure of Sensitive Information to an Unauthorized Actor

CVE Number	Description
CVE-2024-43367	Boa is an embeddable and experimental Javascript engine written in Rust. Starting in version 0.16 and prior to version 0.19.0, a wrong assumption made when handlin `AsyncGenerator` operations can cause an uncaught exception on certain scripts. Boa's implementation of `AsyncGenerator` makes the assumption that the state of ar change while resolving a promise created by methods of `AsyncGenerator` such as `%AsyncGeneratorPrototype%.next`, `%AsyncGeneratorPrototype%.return`, or `%AsyncGeneratorPrototype%.throw`. However, a carefully constructed code could trigger a state transition from a getter method for the promise's `then` property, whi assertion of this assumption, causing an uncaught exception. This could be used to create a Denial Of Service attack in applications that run arbitrary ECMAScript code Version 0.19.0 is patched to correctly handle this case. Users unable to upgrade to the patched version would want to use `std::panic::catch_unwind` to ensure any exc don't impact the availability of the main application.
CVE-2024-43366	zkvyper is a Vyper compiler. Starting in version 1.3.12 and prior to version 1.5.3, since LLL IR has no Turing-incompletness restrictions, it is compiled to a loop with a m leads to a loss of funds or other unwanted behavior if the loop body contains it. However, more real-life use cases like iterating over an array are not affected. No contra which was fixed in version 1.5.3. Upgrading and redeploying affected contracts is the only way to avoid the vulnerability.
CVE-2024-42986	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the PPPOEPassword parameter in the fromAdvSetWan function. This vulnerability allows a Service (DoS) via a crafted POST request.
CVE-2024-42985	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromNatlimit function. This vulnerability allows attackers to cause crafted POST request.
CVE-2024-6918	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') vulnerability exists that could cause a crash of the Accutech Manager when receiving port 2536/TCP.
CVE-2024-42984	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromP2pListFilter function. This vulnerability allows attackers to via a crafted POST request.
CVE-2024-42983	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the pptpPPW parameter in the fromAdvSetWan function. This vulnerability allows attackers (DoS) via a crafted POST request.
CVE-2024-42982	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromVirtualSer function. This vulnerability allows attackers to cau a crafted POST request.
CVE-2024-42981	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the delno parameter in the fromPptpUserSetting function. This vulnerability allows attacker (DoS) via a crafted POST request.
CVE-2024-42979	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the frmL7ProtForm function. This vulnerability allows attackers to ca via a crafted POST request.
CVE-2024-42977	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the qos parameter in the fromqossetting function. This vulnerability allows attackers to caus a crafted POST request.
CVE-2024-42976	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromSafeClientFilter function. This vulnerability allows attackers (DoS) via a crafted POST request.
CVE-2024-42974	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the page parameter in the fromwebExcptypemanFilter function. This vulnerability allows att Service (DoS) via a crafted POST request.
CVE-2024-42987	Tenda FH1206 v02.03.01.35 was discovered to contain a stack overflow via the modino parameter in the fromPptpUserAdd function. This vulnerability allows attackers (DoS) via a crafted POST request.
CVE-2024-22281	** UNSUPPORTED WHEN ASSIGNED ** The Apache Helix Front (UI) component contained a hard-coded secret, allowing an attacker to spoof sessions by generating issue affects Apache Helix Front (UI): all versions. As this project is retired, we do not plan to release a version that fixes this issue. Users are recommended to find an the instance to trusted users. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.
CVE-2024-27120	A Local File Inclusion vulnerability has been found in ComfortKey, a product of Celsius Benelux. Using this vulnerability, an unauthenticated attacker may retrieve sensi underlying system. The vulnerability has been remediated in version 24.1.2.
CVE-2024-39792	When the NGINX Plus is configured to use the MQTT pre-read module, undisclosed requests can cause an increase in memory resource utilization. Note: Software ve of Technical Support (EoTS) are not evaluated.
CVE-2024-37399	A NULL pointer dereference in WLAvalancheService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS.

CVE Number	Description
CVE-2024-39818	Protection mechanism failure for some Zoom Workplace Apps and SDKs may allow an authenticated user to conduct information disclosure via network access.
CVE-2024-38653	XXE in SmartDeviceServer in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to read arbitrary files on the server.
CVE-2024-7729	The CAYIN Technology CMS lacks proper access control, allowing unauthenticated remote attackers to download arbitrary CGI files.
CVE-2024-36136	An off-by-one error in WLInfoRailService in Ivanti Avalanche 6.3.1 allows a remote unauthenticated attacker to crash the service, resulting in a DoS.
CVE-2024-34163	Improper input validation in firmware for some Intel(R) NUC may allow a privileged user to potentially enableescalation of privilege via local access.
CVE-2024-39809	The Central Manager user session refresh token does not expire when a user logs out. Note: Software versions which have reached End of Technical Support (EoTS)
CVE-2024-41727	In BIG-IP tenants running on r2000 and r4000 series hardware, or BIG-IP Virtual Edition (VEs) using Intel E810 SR-IOV NIC, undisclosed traffic can cause an increase Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.
CVE-2024-39778	When a stateless virtual server is configured on BIG-IP system with a High-Speed Bridge (HSB), undisclosed requests can cause TMM to terminate. Note: Software v of Technical Support (EoTS) are not evaluated.
CVE-2024-39398	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Restriction of Excessive Authentication Attempts vulnerability feature bypass. An attacker could exploit this vulnerability to perform brute force attacks and potentially gain unauthorized access to accounts. Exploitation of this issue interaction, but attack complexity is high.
CVE-2024-7898	A vulnerability classified as critical was found in Tosei Online Store Management System ネット店舗管理システム 4.02/4.03/4.04. This vulnerability affects unknown co The manipulation leads to use of default credentials. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The ve this disclosure but did not respond in any way.
CVE-2024-7927	A vulnerability classified as critical was found in ZZCMS 2023. Affected by this vulnerability is an unknown functionality of the file /admin/class.php?dowhat=modifyclass argument skin[] leads to path traversal. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7797	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been classified as critical. Affected is an unknown function of the file /simple-onli system/bidding/admin/ajax.php?action=login. The manipulation of the argument username leads to sql injection. It is possible to launch the attack remotely. The exploit and may be used.
CVE-2024-7798	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionalit bidding-system/bidding/admin/ajax.php?action=login2. The manipulation of the argument username leads to sql injection. The attack can be launched remotely. The ex public and may be used.
CVE-2024-7808	A vulnerability was found in code-projects Job Portal 1.0. It has been classified as critical. Affected is an unknown function of the file logindbc.php. The manipulation of injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2022-33162	IBM Security Directory Integrator 7.2.0 and Security Verify Directory Integrator 10.0.0 does not perform any authentication for functionality that requires a provable user significant amount of resources, at the privilege level of a standard unprivileged user. IBM X-Force ID: 228570.
CVE-2024-43688	cron/entry.c in vixie cron before 9cc8ab1, as used in OpenBSD 7.4 and 7.5, allows a heap-based buffer underflow and memory corruption. NOTE: this issue was introd refactoring.
CVE-2024-7926	A vulnerability classified as critical has been found in ZZCMS 2023. Affected is an unknown function of the file /admin/about_edit.php?action=modify. The manipulation path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7838	A vulnerability was found in itsourcecode Online Food Ordering System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file manipulation of the argument cname leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7947	A vulnerability classified as critical has been found in SourceCodester Point of Sales and Inventory Management System 1.0. This affects an unknown part of the file lo argument email leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.

CVE Number	Description
CVE-2024-7946	A vulnerability was found in itsourcecode Online Blood Bank Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality component User Signup. The manipulation of the argument user leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the pub
CVE-2024-7913	A vulnerability was found in itsourcecode Billing System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /addclient1.php. The m lname/fname/mi/address/contact/meterReader leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be use
CVE-2024-8005	A vulnerability was found in demozx gf_cms 1.0/1.0.1. It has been classified as critical. This affects the function init of the file internal/logic/auth/auth.go of the compone manipulation leads to hard-coded credentials. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. Upgrading to v this issue. The patch is named be702ada7cb6fdabc02689d90b38139c827458a5. It is recommended to upgrade the affected component.
CVE-2024-7933	A vulnerability was found in itsourcecode Project Expense Monitoring System 1.0. It has been classified as critical. Affected is an unknown function of the file login1.php Login. The manipulation of the argument user leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be
CVE-2024-7839	A vulnerability classified as critical has been found in itsourcecode Billing System 1.0. This affects an unknown part of the file addbill.php. The manipulation of the argur injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-43369	Ibexa RichText Field Type is a Field Type for supporting rich formatted text stored in a structured XML format. In versions on the 4.6 branch prior to 4.6.10, the validato blocklists `javascript:` and `vbscript:` in links to prevent XSS. This can leave other options open, and the check can be circumvented using upper case. Content editing is required to exploit this vulnerability, which typically means Editor role or higher. The fix implements an allowlist instead, which allows only approved link protocols. Th Version 4.6.10 contains a patch for this issue. No known workarounds are available.
CVE-2023-3419	The tagDiv Opt-In Builder plugin is vulnerable to Blind SQL Injection via the 'couponId' parameter of the 'recreate_stripe_subscription' REST API endpoint in versions u insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers with append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.
CVE-2022-1751	The Skitter Slideshow plugin for WordPress is vulnerable to Server-Side Request Forgery in all versions up to, and including, 2.5.2 via the /image.php file. This makes i attackers to make web requests to arbitrary locations originating from the web application and can be used to query and modify information from internal services.
CVE-2024-6451	AI Engine < 2.4.3 is susceptible to remote-code-execution (RCE) via Log Poisoning. The AI Engine WordPress plugin before 2.5.1 fails to validate the file extension of " Administrators to change log filetypes from .log to .php.
CVE-2024-7702	The Contact Form by Bit Form: Multi Step Form, Calculation Contact Form, Payment Contact Form & Custom Contact Form builder plugin for WordPress is vulnerable entryID parameter in versions 2.0 to 2.13.9 due to insufficient escaping on the user-supplied parameter and lack of sufficient preparation on the existing SQL query. Thi authenticated attackers, with Administrator-level access and above, to append additional SQL queries to already existing queries that can be used to extract sensitive i
CVE-2024-42994	VTiger CRM <= 8.1.0 does not properly sanitize user input before using it in a SQL statement, leading to a SQL Injection in the "CompanyDetails" operation of the "Mai
CVE-2024-37373	Improper input validation in the Central Filestore in Ivanti Avalanche 6.3.1 allows a remote authenticated attacker with admin rights to achieve RCE.
CVE-2024-7728	The specific CGI of the CAYIN Technology CMS does not properly validate user input, allowing a remote attacker with administrator privileges to inject OS commands i execute them on the remote server.
CVE-2024-7301	The WordPress File Upload plugin for WordPress is vulnerable to Stored Cross-Site Scripting via SVG File uploads in all versions up to, and including, 4.24.8 due to ins output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.
CVE-2022-1206	The AdRotate Banner Manager – The only ad manager you'll need plugin for WordPress is vulnerable to arbitrary file uploads due to missing file extension sanitization function in all versions up to, and including, 5.13.2. This makes it possible for authenticated attackers, with administrator-level access and above, to upload arbitrary file affected site's server which may make remote code execution possible. This is only exploitable on select instances where the configuration will execute the first extensi
CVE-2024-7780	The Contact Form by Bit Form: Multi Step Form, Calculation Contact Form, Payment Contact Form & Custom Contact Form builder plugin for WordPress is vulnerable id parameter in versions 2.0 to 2.13.9 due to insufficient escaping on the user-supplied parameter and lack of sufficient preparation on the existing SQL query. This mal attackers, with Administrator-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information fr
CVE-2024-43370	gettext.js is a GNU gettext port for node and the browser. There is a cross-site scripting (XSS) injection if `.po` dictionary definition files are corrupted. This vulnerability 2.0.3. As a workaround, control the origin of the definition catalog to prevent the use of this flaw in the definition of plural forms.
CVE-2024-24853	Incorrect behavior order in transition between executive monitor and SMI transfer monitor (STM) in some Intel(R) Processor may allow a privileged user to potentially e local access.
CVE-2023-3416	The tagDiv Opt-In Builder plugin is vulnerable to Blind SQL Injection via the 'subscriptionCouponId' parameter via the 'create_stripe_subscription' REST API endpoint in 1.4.4 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated a privileges to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.

CVE Number	Description
CVE-2024-43250	Incorrect Authorization vulnerability in Bit Apps Bit Form Pro bitformpro allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Bit Form Pr
CVE-2024-43306	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP-Lister Lite for eBay allows Reflected XSS.This issue af from n/a through 3.6.0.
CVE-2024-43276	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Svetoslav Marinov (Slavi) Child Theme Creator allows Refl Child Theme Creator: from n/a through 1.5.4.
CVE-2024-43313	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in FormFacade allows Reflected XSS.This issue affects Form
CVE-2024-21801	Insufficient control flow management in some Intel(R) TDX module software before version 1.5.05.46.698 may allow a privileged user to potentially enable denial of ser
CVE-2024-43348	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Iznyn Purity Of Soul allows Reflected XSS.This issue affec through 1.9.
CVE-2024-43256	Missing Authorization vulnerability in nouthemes Leopard - WordPress offload media allows Accessing Functionality Not Properly Constrained by ACLs.This issue affec media: from n/a through 2.0.36.
CVE-2024-43238	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in weDevs weMail allows Reflected XSS.This issue affects we
CVE-2024-43330	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in IdeaBox Creations PowerPack for Beaver Builder allows R PowerPack for Beaver Builder: from n/a before 2.37.4.
CVE-2024-43303	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in videousermanuals.Com White Label CMS allows Reflected Label CMS: from n/a through 2.7.4.
CVE-2024-43246	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in creativeon WHMpress allows Reflected XSS.This issue affe 6.2-revision-5.
CVE-2024-43244	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in favethemes Houzez allows Reflected XSS.This issue affec 3.2.4.
CVE-2024-43279	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Tribulant Newsletters allows Reflected XSS.This issue affe 4.9.8.
CVE-2024-43304	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Cool Plugins Cryptocurrency Widgets – Price Ticker & Coir issue affects Cryptocurrency Widgets – Price Ticker & Coins List: from n/a through 2.8.0.
CVE-2024-43241	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in azzaroco Ultimate Membership Pro allows Reflected XSS.T Membership Pro: from n/a through 12.6.
CVE-2024-43327	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Boone Gorges Invite Anyone allows Reflected XSS.This iss n/a through 1.4.7.
CVE-2024-39420	Acrobat Reader versions 20.005.30636, 24.002.21005, 24.001.30159, 20.005.30655, 24.002.20965, 24.002.20964, 24.001.30123, 24.003.20054 and earlier are affecte use (TOCTOU) Race Condition vulnerability that could lead to arbitrary code execution. This vulnerability arises when the timing of actions changes the state of a resou condition and the use of the resource, allowing an attacker to manipulate the resource in a harmful way. Exploitation of this issue requires user interaction in that a victi
CVE-2024-39425	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by a Time-of-check Time-of-use (TOCTOU) Race Conditi privilege escalation. Exploitation of this issue require local low-privilege access to the affected system and attack complexity is high.
CVE-2024-34731	In multiple functions of TranscodingResourcePolicy.cpp, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege w privileges needed. User interaction is not needed for exploitation.

CVE Number	Description
CVE-2023-5505	The BackWPup plugin for WordPress is vulnerable to Directory Traversal in versions up to, and including, 4.0.1 via the job-specific backup folder. This allows authentic in arbitrary folders on the server provided they can be written to by the server. Additionally, default settings will place an index.php and a .htaccess file into the chosen when the first backup job is run that are intended to prevent directory listing and file access. This means that an attacker could set the backup directory to the root of an environment and thus disable that site.
CVE-2023-38655	Improper buffer restrictions in firmware for some Intel(R) AMT and Intel(R) Standard Manageability may allow a privileged user to potentially enable denial of service via
CVE-2024-25008	Ericsson RAN Compute and Site Controller 6610 contains a vulnerability in the Control System where Improper Input Validation can lead to arbitrary code execution, fo with the same privileges as the attacker. The attacker would require elevated privileges for example a valid OAM user having the system administrator role to exploit th
CVE-2024-39406	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Trav lead to arbitrary file system read. An admin attacker could exploit this vulnerability to gain access to files and directories that are outside the restricted directory. Exploit require user interaction and scope is changed.
CVE-2024-31798	Identical Hardcoded Root Password for All Devices in GNCC's GC2 Indoor Security Camera 1080P allows an attacker with physical access to retrieve the root passwo
CVE-2024-42488	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. Prior to versions 1.14.14 and 1.15.8, a race condition in the Cilium agent can that should be applied to a node. This could in turn cause CiliumClusterwideNetworkPolicies intended for nodes with the ignored label to not apply, leading to policy by patched in Cilium v1.14.14 and v1.15.8 As the underlying issue depends on a race condition, users unable to upgrade can restart the Cilium agent on affected nodes u confirmed to be working as expected.
CVE-2024-31800	Authentication Bypass in GNCC's GC2 Indoor Security Camera 1080P allows an attacker with physical access to gain a privileged command shell via the UART Debug
CVE-2024-23907	Uncontrolled search path in some Intel(R) High Level Synthesis Compiler software before version 23.4 may allow an authenticated user to potentially enable escalation
CVE-2024-23908	Insecure inherited permissions in some Flexlm License Daemons for Intel(R) FPGA software before version v11.19.5.0 may allow an authenticated user to potentially e local access.
CVE-2024-23909	Uncontrolled search path in some Intel(R) FPGA SDK for OpenCL(TM) software technology may allow an authenticated user to potentially enable escalation of privileg
CVE-2023-43747	Incorrect default permissions for some Intel(R) Connectivity Performance Suite software installers before version 2.0 may allow an authenticated user to potentially ena local access.
CVE-2024-23489	Uncontrolled search path for some Intel(R) VROC software before version 8.6.0.1191 may allow an authenticated user to potentially enable escalation of privilege via lo
CVE-2024-26025	Incorrect default permissions for some Intel(R) Advisor software before version 2024.1 may allow an authenticated user to potentially enable escalation of privilege via l
CVE-2023-49144	Out of bounds read in OpenBMC Firmware for some Intel(R) Server Platforms before versions egs-1.15-0, bhs-0.27 may allow a privileged user to potentially enable int access.
CVE-2024-21766	Uncontrolled search path for some Intel(R) oneAPI Math Kernel Library software before version 2024.1 may allow an authenticated user to potentially enable escalatior
CVE-2024-23491	Uncontrolled search path in some Intel(R) Distribution for GDB software before version 2024.0.1 may allow an authenticated user to potentially enable escalation of priv
CVE-2024-21784	Uncontrolled search path for some Intel(R) IPP Cryptography software before version 2021.11 may allow an authenticated user to potentially enable escalation of privile
CVE-2024-23974	Incorrect default permissions in some Intel(R) ISH software installers may allow an authenticated user to potentially enable escalation of privilege via local access.
CVE-2024-23495	Incorrect default permissions in some Intel(R) Distribution for GDB software before version 2024.0.1 may allow an authenticated user to potentially enable escalation of

CVE Number	Description
CVE-2024-25561	Insecure inherited permissions in some Intel(R) HID Event Filter software installers before version 2.2.2.1 may allow an authenticated user to potentially enable escalat
CVE-2024-21857	Uncontrolled search path for some Intel(R) oneAPI Compiler software before version 2024.1 may allow an authenticated user to potentially enable escalation of privileg
CVE-2024-22184	Uncontrolled search path for some Intel(R) Quartus(R) Prime Pro Edition Design Software before version 24.1 may allow an authenticated user to potentially enable es access.
CVE-2024-22376	Uncontrolled search path element in some installation software for Intel(R) Ethernet Adapter Driver Pack before version 28.3 may allow an authenticated user to potent privilege via local access.
CVE-2024-22378	Incorrect default permissions in some Intel Unite(R) Client Extended Display Plugin software installers before version 1.1.352.157 may allow an authenticated user to p privilege via local access.
CVE-2024-24977	Uncontrolled search path for some Intel(R) License Manager for FLEXlm product software before version 11.19.5.0 may allow an authenticated user to potentially enab access.
CVE-2024-21769	Uncontrolled search path in some Intel(R) Ethernet Connection I219-LM install software may allow an authenticated user to potentially enable escalation of privilege via
CVE-2024-28876	Uncontrolled search path for some Intel(R) MPI Library software before version 2021.12 may allow an authenticated user to potentially enable escalation of privilege via
CVE-2024-28172	Uncontrolled search path for some Intel(R) Trace Analyzer and Collector software before version 2022.1 may allow an authenticated user to potentially enable escalatio
CVE-2024-26027	Uncontrolled search path for some Intel(R) Simics Package Manager software before version 1.8.3 may allow an authenticated user to potentially enable escalation of p
CVE-2024-28046	Uncontrolled search path in some Intel(R) GPA software before version 2024.1 may allow an authenticated user to potentially enable escalation of privilege via local ac
CVE-2024-28887	Uncontrolled search path in some Intel(R) IPP software before version 2021.11 may allow an authenticated user to potentially enable escalation of privilege via local ac
CVE-2024-28953	Uncontrolled search path in some EMON software before version 11.44 may allow an authenticated user to potentially enable escalation of privilege via local access.
CVE-2024-29015	Uncontrolled search path in some Intel(R) VTune(TM) Profiler software before versions 2024.1 may allow an authenticated user to potentially enable escalation of privil
CVE-2024-42598	SeaCMS 13.0 has a remote code execution vulnerability. The reason for this vulnerability is that although admin_editplayer.php imposes restrictions on edited files, atta restrictions and write code, allowing authenticated attackers to exploit the vulnerability to execute arbitrary commands and gain system privileges.
CVE-2024-43329	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Chill Allegiant allegiant allows Stored XSS.This issue a 1.2.7.
CVE-2024-35152	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 could allow an authenticated user to cause a denial of service with a specially crafted query allocation. IBM X-Force ID: 292639.
CVE-2024-7790	A stored cross site scripting vulnerabilities exists in DevikaAI from commit 6acce21fb08c3d1123ef05df6a33912bf0ee77c2 onwards via improperly decoded user input.
CVE-2024-37529	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 could allow an authenticated user to cause a denial of service with a specially cra memory allocation. IBM X-Force ID: 294295.

CVE Number	Description
CVE-2023-47728	IBM QRadar Suite Software 1.10.12.0 through 1.10.22.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 could allow a remote attacker to obtain sensitive in technical error message is returned in the request. This information could be used in further attacks against the system. IBM X-Force ID: 272201.
CVE-2024-25009	Ericsson Packet Core Controller (PCC) contains a vulnerability in Access and Mobility Management Function (AMF) where improper input validation can lead to denial service degradation.
CVE-2024-42849	An issue in Silverpeas v.6.4.2 and lower allows a remote attacker to cause a denial of service via the password change function.
CVE-2024-43321	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PickPlugins Team Showcase allows Stored XSS.This issue n/a through 1.22.23.
CVE-2024-25157	An authentication bypass vulnerability in GoAnywhere MFT prior to 7.6.0 allows Admin Users with access to the Agent Console to circumvent some permission checks pages. This could lead to unauthorized information disclosure or modification.
CVE-2024-43335	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CyberChimps Responsive Blocks – WordPress Gutenberg issue affects Responsive Blocks – WordPress Gutenberg Blocks: from n/a through 1.8.8.
CVE-2024-43320	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Livemesh Livemesh Addons for WPBakery Page Builder ad Stored XSS.This issue affects Livemesh Addons for WPBakery Page Builder: from n/a through 3.9.
CVE-2024-43318	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in E2Pdf.Com allows Stored XSS.This issue affects e2pdf: fro
CVE-2024-42439	Untrusted search path in the installer for Zoom Workplace Desktop App for macOS and Zoom Meeting SDK for macOS before 6.1.0 may allow a privileged user to conc local access.
CVE-2024-22217	A Server-Side Request Forgery (SSRF) vulnerability in Terminalfour before 8.3.19 allows authenticated users to use specific features to access internal services includ server that Terminalfour runs on.
CVE-2024-24580	Improper conditions check in some Intel(R) Data Center GPU Max Series 1100 and 1550 products may allow a privileged user to potentially enable denial of service via
CVE-2024-43262	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in webriti Busiprof allows Stored XSS.This issue affects Busip
CVE-2022-4532	The LOGIN AND REGISTRATION ATTEMPTS LIMIT plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 2.1. This is due to ins IP Address information is being retrieved for request logging and login restrictions. Attackers can supply the X-Forwarded-For header with with a different IP Address th used to bypass settings that may have blocked out an IP address from logging in.
CVE-2024-43368	The Trix editor, versions prior to 2.1.4, is vulnerable to XSS when pasting malicious code. This vulnerability is a bypass of the fix put in place for GHSA-qjqp-xr96-cj99. was added for Trix attachments with a `text/html` content type. However, Trix only checks the content type on the paste event's `dataTransfer` object. As long as the `d of `text/html`, Trix parses its contents and creates an `Attachment` with them, even if the attachment itself doesn't have a `text/html` content type. Trix then uses the att attachment element's `innerHTML`. An attacker could trick a user to copy and paste malicious code that would execute arbitrary JavaScript code within the context of th leading to unauthorized actions being performed or sensitive information being disclosed. This vulnerability was fixed in version 2.1.4.
CVE-2024-6004	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to deny printer connections unt
CVE-2024-43263	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Visual Composer Visual Composer Starter allows Stored X Composer Starter: from n/a through 3.3.
CVE-2024-41773	IBM Global Configuration Management 7.0.2 and 7.0.3 could allow an authenticated user to archive a global baseline due to improper access controls.
CVE-2024-40705	IBM InfoSphere Information Server could allow an authenticated user to consume file space resources due to unrestricted file uploads. IBM X-Force ID: 298279.
CVE-2024-6337	An Incorrect Authorization vulnerability was identified in GitHub Enterprise Server that allowed a GitHub App with only content: read and pull_request_write: write permi inside a private repository. This was only exploitable via user access token and installation access token was not impacted. This vulnerability affected all versions of Git 3.14 and was fixed in versions 3.13.3, 3.12.8, 3.11.14 and 3.10.16. This vulnerability was reported via the GitHub Bug Bounty program.

CVE Number	Description
CVE-2024-43267	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Qamar Sheeraz, Nasir Ahmad, GenialSouls Mega Addons XSS.This issue affects Mega Addons For Elementor: from n/a through 1.9.
CVE-2024-35539	Typecho v1.3.0 was discovered to contain a race condition vulnerability in the post commenting function. This vulnerability allows attackers to post several comments b if the comments are posted too frequently.
CVE-2024-43278	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Phi Phan Meta Field Block allows Stored XSS.This issue af through 1.2.13.
CVE-2024-38810	Missing Authorization When Using @AuthorizeReturnObject in Spring Security 6.3.0 and 6.3.1 allows attacker to render security annotations inaffective.
CVE-2024-6347	* Unprotected privileged mode access through UDS session in the Blind Spot Detection Sensor ECU firmware in Nissan Altima (2022) allows attackers to trigger denial unauthorized access to the ECU's programming session. * No preconditions implemented for ECU management functionality through UDS session in the Blind Spot De Altima (2022) allows attackers to disrupt normal ECU operations by triggering a control command without authentication.
CVE-2024-43284	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Travel WP Travel Gutenberg Blocks allows Stored XSS Gutenberg Blocks: from n/a through 3.5.1.
CVE-2024-43294	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BoldThemes Bold Timeline Lite allows Stored XSS.This iss from n/a through 1.2.0.
CVE-2024-23499	Protection mechanism failure in Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters E810 Series before version 28.3 may allow an u enable denial of service via network access.
CVE-2024-22374	Insufficient control flow management for some Intel(R) Xeon Processors may allow an authenticated user to potentially enable denial of service via local access.
CVE-2024-43409	Ghost is a Node.js content management system. Improper authentication on some endpoints used for member actions would allow an attacker to perform member-only information. This security vulnerability is present in Ghost v4.46.0-v5.89.4. v5.89.5 contains a fix for this issue.
CVE-2024-5210	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to prevent printer services from system is rebooted.
CVE-2024-42464	Authorization Bypass Through User-Controlled Key vulnerability in upKeeper Solutions product upKeeper Manager allows Utilizing REST's Trust in the System Resour issue affects upKeeper Manager: through 5.1.9.
CVE-2024-43342	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in BdThemes Ultimate Store Kit Elementor Addons allows Sto Ultimate Store Kit Elementor Addons: from n/a through 1.6.4.
CVE-2024-43344	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Icegram allows Stored XSS.This issue affects Icegram: fron
CVE-2024-43346	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wow-Company Modal Window allows Stored XSS.This issu n/a through 6.0.3.
CVE-2024-39822	Sensitive information exposure in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow an authenticated user to conduct an informati access.
CVE-2024-43353	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in myCred allows Stored XSS.This issue affects myCred: fron
CVE-2024-43349	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in AREOI All Bootstrap Blocks allows Stored XSS.This issue a n/a through 1.3.19.
CVE-2024-42436	Buffer overflow in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow an authenticated user to conduct a denial of service via netw

CVE Number	Description
CVE-2024-43351	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Bravada bravada allows Stored XSS.This through 1.1.2.
CVE-2024-43352	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Organic Themes GivingPress Lite allows Stored XSS.This from n/a through 1.8.6.
CVE-2024-5209	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to deny printing capabilities un
CVE-2024-42476	In the OAuth library for nim prior to version 0.11, the Authorization Code grant and Implicit grant both rely on the `state` parameter to prevent cross-site request forgery resource owner might have their session associated with protected resources belonging to an attacker. When this project is compiled with certain compiler flags set, it i parameter will not be checked at all, creating a CSRF vulnerability. Version 0.11 checks the `state` parameter using a regular `if` statement or `doAssert` instead of rely `doAssert` will achieve the desired behavior even if `-d:danger` or `--assertions:off` is set.
CVE-2024-42475	In the OAuth library for nim prior to version 0.11, the `state` values generated by the `generateState` function do not have sufficient entropy. These can be successfully them to perform a CSRF vs a user, associating the user's session with the attacker's protected resources. While `state` isn't exactly a cryptographic value, it should be secure way. `generateState` should be using a CSPRNG. Version 0.11 modifies the `generateState` function to generate `state` values of at least 128 bits of entropy w
CVE-2024-42463	Authorization Bypass Through User-Controlled Key vulnerability in upKeeper Solutions product upKeeper Manager allows Utilizing REST's Trust in the System Resour issue affects upKeeper Manager: through 5.1.9.
CVE-2024-42437	Buffer overflow in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow an authenticated user to conduct a denial of service via netw
CVE-2024-5940	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on t versions up to, and including, 3.13.0. This makes it possible for unauthenticated attackers to edit event ticket settings if the Events beta feature is enabled.
CVE-2024-43305	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Code Amp Custom Layouts – Post + Product grids made e issue affects Custom Layouts – Post + Product grids made easy: from n/a through 1.4.11.
CVE-2024-4782	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to disrupt the printer's functiona occurs.
CVE-2024-4781	A denial-of-service vulnerability was reported in some Lenovo printers that could allow an unauthenticated attacker on a shared network to crash printer communicatio
CVE-2024-42438	Buffer overflow in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow an authenticated user to conduct a denial of service via netw
CVE-2024-43309	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Socio WP Telegram Widget and Join Link allows Store Telegram Widget and Join Link: from n/a through 2.1.27.
CVE-2024-43308	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Gutentor Gutentor - Gutenberg Blocks - Page Builder for G XSS.This issue affects Gutentor - Gutenberg Blocks - Page Builder for Gutenberg Editor: from n/a through 3.3.5.
CVE-2024-24983	Protection mechanism failure in firmware for some Intel(R) Ethernet Network Controllers and Adapters E810 Series before version 4.4 may allow an unauthenticated us service via network access.
CVE-2024-43307	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Gordon Böhme, Antonio Leutsch Structured Content allows Structured Content: from n/a through 1.6.2.
CVE-2024-7064	The ElementsKit Pro plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several parameters in all versions up to, and including, 3.6.5 due to insufficie escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenev page.
CVE-2024-7144	The JetElements plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' and 'slide_id' parameters in all versions up to, and including, 2.6.20 due t and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execut injected page.
CVE-2024-5763	The The Plus Addons for Elementor – Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Stored Cross- attribute within the plugin's Video widget in all versions up to, and including, 5.6.2 due to insufficient input sanitization and output escaping. This makes it possible for a contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.

CVE Number	Description
CVE-2024-6575	The The Plus Addons for Elementor – Elementor Addons, Page Templates, Widgets, Mega Menu, WooCommerce plugin for WordPress is vulnerable to Stored Cross-S 'res_width_value' parameter within the plugin's tp_page_scroll widget in all versions up to, and including, 5.6.2 due to insufficient input sanitization and output escaping authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2024-5576	The Tutor LMS Elementor Addons plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'course_carousel_skin' attribute within the plugin's Course C to, and including, 2.1.4 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with con to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2024-6532	The Sheet to Table Live Sync for Google Sheet plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's STWT_Sheet_Table shortcode in all v 1.0.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level acce web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2024-21787	Inadequate encryption strength for some BMRA software before version 22.08 may allow an authenticated user to potentially enable escalation of privilege via local acc
CVE-2024-7136	The JetSearch plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'id' parameter in all versions up to, and including, 3.5.2 due to insufficient input 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-2024-6864	The WP Last Modified Info plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'template' attribute of the lmt-post-modified-info shortcode in all ver due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary execute whenever a user accesses an injected page.
CVE-2024-7147	The JetBlocks for Elementor plugin for WordPress is vulnerable to Stored Cross-Site Scripting via multiple placeholder parameters in all versions up to, and including, 1 sanitization and output escaping. This makes it possible for authenticated attackers, with Contributor-level access and above, to inject arbitrary web scripts in pages tha accesses an injected page.
CVE-2024-7588	The Gutenberg Blocks, Page Builder – ComboBlocks plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's Accordion block in all versions u insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and abov pages that will execute whenever a user accesses an injected page.
CVE-2024-7703	The ARMember – Membership Plugin, Content Restriction, Member Levels, User Profile & User signup plugin for WordPress is vulnerable to Stored Cross-Site Scriptin versions up to, and including, 4.0.37 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with Subscriber-level a arbitrary web scripts in pages that will execute whenever a user accesses the SVG file.
CVE-2024-7054	The Popup Maker – Boost Sales, Conversions, Optins, Subscribers with the Ultimate WP Popups Builder plugin for WordPress is vulnerable to Stored Cross-Site Scrip parameter in all versions up to, and including, 1.19.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with C above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.
CVE-2024-7935	A vulnerability was found in itsourcecode Project Expense Monitoring System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of th manipulation of the argument map_id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7911	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been classified as critical. This affects an unknown part of the file /simple-online- system/bidding/index.php. The manipulation of the argument page leads to file inclusion. It is possible to initiate the attack remotely. The exploit has been disclosed to t
CVE-2024-7897	A vulnerability classified as critical has been found in Tosei Online Store Management System ネット店舗管理システム 4.02/4.03/4.04. This affects an unknown part o The manipulation of the argument kikaibangou leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and vendor was contacted early about this disclosure but did not respond in any way.
CVE-2024-7943	A vulnerability was found in itsourcecode Laravel Property Management System 1.0 and classified as critical. This issue affects the function upload of the file Properties of the argument file leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7937	A vulnerability classified as critical was found in itsourcecode Project Expense Monitoring System 1.0. This vulnerability affects unknown code of the file printtransfer.ph argument transfer_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7936	A vulnerability classified as critical has been found in itsourcecode Project Expense Monitoring System 1.0. This affects an unknown part of the file transferred_report.p argument start/end/employee leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7906	A vulnerability classified as critical was found in DedeBIZ 6.3.0. This vulnerability affects the function get_mime_type of the file /admin/dialog/select_images_post.php c Settings. The manipulation of the argument upload leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and r was contacted early about this disclosure but did not respond in any way.
CVE-2024-7934	A vulnerability was found in itsourcecode Project Expense Monitoring System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functiona manipulation of the argument code leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7905	A vulnerability classified as critical has been found in DedeBIZ 6.3.0. This affects the function AdminUpload of the file admin/archives_do.php. The manipulation of the a unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early respond in any way.

CVE Number	Description
CVE-2024-7904	A vulnerability was found in DedeBIZ 6.3.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file admin/file_manage_control.php Handler. The manipulation of the argument upfile1 leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and vendor was contacted early about this disclosure but did not respond in any way.
CVE-2024-7931	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0 and classified as critical. This issue affects some unknown processing of the file /track The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7903	A vulnerability was found in DedeBIZ 6.3.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file admin/media_add.php of Handler. The manipulation of the argument upfile1 leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and vendor was contacted early about this disclosure but did not respond in any way.
CVE-2024-7930	A vulnerability has been found in SourceCodester Clinics Patient Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /p manipulation of the argument medicine_id leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7922	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-3 343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_ of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched remotely. The exploit has been disclosed to the public and n vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It sh
CVE-2024-7896	A vulnerability was found in Tosei Online Store Management System ネット店舗管理システム 4.02/4.03/4.04. It has been rated as critical. Affected by this issue is som file /cgi-bin/p1_ftpserver.php. The manipulation of the argument adr_txt leads to command injection. The attack may be launched remotely. The exploit has been disclo used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2024-7907	A vulnerability, which was classified as critical, has been found in TOTOLINK X6000R 9.4.0cu.852_20230719. This issue affects the function setSyslogCfg of the file /c manipulation of the argument rtLogServer leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be u contacted early about this disclosure but did not respond in any way.
CVE-2024-7944	A vulnerability was found in itsourcecode Laravel Property Management System 1.0. It has been classified as critical. Affected is the function UpdateDocumentsReques DocumentsController.php. The manipulation leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and r
CVE-2024-7792	A vulnerability was found in SourceCodester Task Progress Tracker 1.0. It has been classified as critical. Affected is an unknown function of the file /endpoint/delete-tas argument task leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7800	A vulnerability classified as critical has been found in SourceCodester Simple Online Bidding System 1.0. This affects an unknown part of the file /simple-online-bidding action=delete_product. The manipulation of the argument id leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the pub
CVE-2024-7949	A vulnerability, which was classified as critical, was found in SourceCodester Online Graduate Tracer System up to 1.0. Affected is an unknown function of the file /trac The manipulation of the argument request leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be us
CVE-2024-22219	XML External Entity (XXE) vulnerability in Terminalfour 8.0.0001 through 8.3.18 and XML JDBC versions up to 1.0.4 allows authenticated users to submit malicious XM could lead to various actions such as accessing the underlying server, remote code execution (RCE), or performing Server-Side Request Forgery (SSRF) attacks.
CVE-2024-32231	Stash up to v0.25.1 was discovered to contain a SQL injection vulnerability via the sort parameter.
CVE-2024-7811	A vulnerability classified as critical has been found in SourceCodester Daily Expenses Monitoring App 1.0. This affects an unknown part of the file /endpoint/delete-expe the argument expense leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7833	A vulnerability was found in D-Link DI-8100 16.07. It has been classified as critical. This affects the function upgrade_filter_asp of the file upgrade_filter.asp. The manip leads to command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7794	A vulnerability was found in itsourcecode Vehicle Management System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7810	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of th /tracking/admin/view_itprofile.php. The manipulation of the argument id leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to t
CVE-2024-7845	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the fil The manipulation of the argument request leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7853	A vulnerability was found in SourceCodester Yoga Class Registration System up to 1.0. It has been classified as critical. Affected is an unknown function of the file /adr page=categories/view_category. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed t

CVE Number	Description
CVE-2024-7754	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the f /ajax/check_medicine_name.php. The manipulation of the argument user_name leads to sql injection. The attack may be initiated remotely. The exploit has been disclo used.
CVE-2024-7841	A vulnerability classified as critical was found in SourceCodester Clinics Patient Management System 1.0. This vulnerability affects unknown code of the file /pms/ajax/c manipulation of the argument user_name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7851	A vulnerability has been found in SourceCodester Yoga Class Registration System 1.0 and classified as critical. This vulnerability affects unknown code of the file /class component Add User Handler. The manipulation leads to improper authorization. The attack can be initiated remotely. The exploit has been disclosed to the public and
CVE-2024-43408	Discourse Placeholder Forms will let you build dynamic documentation. Unsanitized and stored user input was injected in the html of the post. The vulnerability is fixed a62f711d5600e4e5d86f342d52932cb6221672e7.
CVE-2024-7867	In Xpdf 4.05 (and earlier), very large coordinates in a page box can cause an integer overflow and divide-by-zero.
CVE-2024-42441	Improper privilege management in the installer for Zoom Workplace Desktop App for macOS, Zoom Meeting SDK for macOS and Zoom Rooms Client for macOS befor user to conduct an escalation of privilege via local access.
CVE-2024-42440	Improper privilege management in the installer for Zoom Workplace Desktop App for macOS, Zoom Meeting SDK for macOS and Zoom Rooms Client for macOS befor user to conduct an escalation of privilege via local access.
CVE-2023-4604	The Slideshow, Image Slider by 2J plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the ‘post’ parameter in versions up to, and including, 1.3.54 sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a such as clicking on a link.
CVE-2024-27184	Inadequate validation of URLs could result into an invalid check whether an redirect URL is internal or not..
CVE-2024-27728	Cross Site Scripting vulnerability in Friendica v.2023.12 allows a remote attacker to obtain sensitive information via the text parameter of the babel debug feature.
CVE-2024-27186	The mail template feature lacks an escaping mechanism, causing XSS vectors in multiple extensions.
CVE-2024-27729	Cross Site Scripting vulnerability in Friendica v.2023.12 allows a remote attacker to obtain sensitive information via the location parameter of the calendar event feature
CVE-2024-27731	Cross Site Scripting vulnerability in Friendica v.2023.12 allows a remote attacker to obtain sensitive information via the lack of file type filtering in the file attachment par
CVE-2024-41697	Priority - CWE-80: Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS)
CVE-2024-24980	Protection mechanism failure in some 3rd, 4th, and 5th Generation Intel(R) Xeon(R) Processors may allow a privileged user to potentially enable escalation of privilege
CVE-2024-42560	A cross-site scripting (XSS) vulnerability in the component update_page_details.php of Blood Bank And Donation Management System commit dc9e039 allows attacke scripts or HTML via a crafted payload injected into the Page Details parameter.
CVE-2024-23729	The ColorOS Internet Browser com.heytap.browser application 45.10.3.4.1 for Android allows a remote attacker to execute arbitrary JavaScript code via the com.andro component.
CVE-2023-4507	The Admission AppManager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'q' parameter in versions up to, and including, 1.0.0 due to insu output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into perfor on a link.
CVE-2024-40743	The stripImages and stripIframes methods didn't properly process inputs, leading to XSS vectors.

CVE Number	Description
CVE-2024-42353	WebOb provides objects for HTTP requests and responses. When WebOb normalizes the HTTP Location header to include the request hostname, it does so by parsin redirected to with Python's urlparse, and joining it to the base URL. `urlparse` however treats a `//` at the start of a string as a URI without a scheme, and then treats the `urljoin` will then use that hostname from the second part as the hostname replacing the original one from the request. This vulnerability is patched in WebOb version 1
CVE-2024-42678	Cross Site Scripting vulnerability in Super easy enterprise management system v.1.0.0 and before allows a local attacker to execute arbitrary code via a crafted script t component.
CVE-2024-41658	Casdoor is a UI-first Identity and Access Management (IAM) / Single-Sign-On (SSO) platform. In Casdoor 1.577.0 and earlier, he purchase URL that is created to gene vulnerable to reflected XSS. When purchasing an item through casdoor, the product page allows you to pay via wechat pay. When using wechat pay, a QR code with th on the payment page, hosted on the domain of casdoor. This page takes a query parameter from the url successUrl, and redirects the user to that url after a successful no reason to think that the payment page contains sensitive information, they may share it with other or can be social engineered into sending it to others. An attacker c with a special url and send it back to the user, and once payment has gone though an XSS attack occurs.
CVE-2024-7850	The BP Profile Search plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 5.7.5. This is due to missing or incorrect no bps_ajax_field_selector(), bps_ajax_template_options(), and bps_ajax_field_row() functions. This makes it possible for unauthenticated attackers to inject malicious we granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2024-6843	The Chatbot with ChatGPT WordPress plugin before 2.4.5 does not sanitise and escape user inputs, which could allow unauthenticated users to perform Stored Cross- admins
CVE-2024-25939	Mirrored regions with different values in 3rd Generation Intel(R) Xeon(R) Scalable Processors may allow a privileged user to potentially enable denial of service via loca
CVE-2024-39283	Incomplete filtering of special elements in Intel(R) TDX module software before version TDX_1.5.01.00.592 may allow an authenticated user to potentially enable escal
CVE-2024-43292	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in EnvoThemes Envo's Elementor Templates & Widgets for W XSS.This issue affects Envo's Elementor Templates & Widgets for WooCommerce: from n/a through 1.4.16.
CVE-2024-27267	The Object Request Broker (ORB) in IBM SDK, Java Technology Edition 7.1.0.0 through 7.1.5.18 and 8.0.0.0 through 8.0.8.26 is vulnerable to remote denial of service the management of ORB listener threads. IBM X-Force ID: 284573.
CVE-2024-43347	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in VirusTran Button contact VR allows Stored XSS.This issue n/a through 4.7.3.
CVE-2024-43324	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CleverSoft Clever Addons for Elementor allows Stored XSS Addons for Elementor: from n/a through 2.2.0.
CVE-2024-32928	The libcurl CURLOPT_SSL_VERIFYPEER option was disabled on a subset of requests made by Nest production devices which enabled a potential man-in-the-middle cloud services by any host the traffic was routed through.
CVE-2024-43291	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in voidCoders Void Contact Form 7 Widget For Elementor Pa XSS.This issue affects Void Contact Form 7 Widget For Elementor Page Builder: from n/a through 2.4.1.
CVE-2024-41164	When TCP profile with Multipath TCP enabled (MPTCP) is configured on a Virtual Server, undisclosed traffic along with conditions beyond the attackers control can cau Software versions which have reached End of Technical Support (EoTS) are not evaluated.
CVE-2024-31905	IBM QRadar Network Packet Capture 7.5 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport S this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 289858.
CVE-2024-39666	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Automattic WooCommerce.This issue affects WooCommer
CVE-2024-43472	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2024-7420	The Insert PHP Code Snippet plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.3.6. This is due to missing or inco /admin/snippets.php file. This makes it possible for unauthenticated attackers to activate/deactivate and delete code snippets via a forged request granted they can tricl performing an action such as clicking on a link.
CVE-2024-38483	Dell BIOS contains an Improper Input Validation vulnerability in an externally developed component. A high privileged attacker with local access could potentially exploi Code execution.

CVE Number	Description
CVE-2024-7625	In HashiCorp Nomad and Nomad Enterprise from 0.6.1 up to 1.6.13, 1.7.10, and 1.8.2, the archive unpacking process is vulnerable to writes outside the allocation direc allocation directories when multiple archive headers target the same file. This vulnerability, CVE-2024-7625, is fixed in Nomad 1.6.14, 1.7.11, and 1.8.3. Access or com agent at the source allocation first is a prerequisite for leveraging this vulnerability.
CVE-2024-25562	Improper buffer restrictions in some Intel(R) Distribution for GDB software before version 2024.0.1 may allow an authenticated user to potentially enable denial of servic
CVE-2023-40067	Unchecked return value in firmware for some Intel(R) CSME may allow an unauthenticated user to potentially enable escalation of privilege via physical access.
CVE-2024-27461	Incorrect default permissions in software installer for Intel(R) MAS (GUI) may allow an authenticated user to potentially enable denial of service via local access.
CVE-2024-28799	IBM QRadar Suite Software 1.10.12.0 through 1.10.23.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 displays sensitive data improperly to a local privileg configurations, during back-end commands which may result in the unexpected disclosure of this information. IBM X-Force ID: 287173.
CVE-2024-43855	In the Linux kernel, the following vulnerability has been resolved: md: fix deadlock between mddev_suspend and flush bio Deadlock occurs when mddev is being suspe progress. It is a complex issue. T1. the first flush is at the ending stage, it clears 'mddev->flush_bio' and tries to submit data, but is blocked because mddev is suspende sets 'mddev->flush_bio', and attempts to queue md_submit_flush_data(), which is already running (T1) and won't execute again if on the same CPU as T1. T3. the third flush, but is blocked because 'mddev->flush_bio' is not NULL (set by T2). T4. mddev_suspend() is called and waits for active_io dec to 0 which is inc by T3. T1 T2 T3 T (suspend) md_submit_flush_data mddev->flush_bio = NULL; . . md_flush_request . mddev->flush_bio = bio . queue submit_flushes . . . . md_handle_request . . active_ wait !mddev->flush_bio . . . . mddev_suspend . . wait !active_io . . . submit_flushes . queue_work md_submit_flush_data . //md_submit_flush_data is already running (T resume The root issue is non-atomic inc/dec of active_io during flush process. active_io is dec before md_submit_flush_data is queued, and inc soon after md_submit_ md_flush_request active_io + 1 submit_flushes active_io - 1 md_submit_flush_data md_handle_request active_io + 1 make_request active_io - 1 If active_io is dec afte of within submit_flushes(), make_request() can be called directly intead of md_handle_request() in md_submit_flush_data(), and active_io will only inc and dec once in Deadlock will be fixed. Additionally, the only difference between fixing the issue and before is that there is no return error handling of make_request(). But after previous make_requst() only return error in raid5_make_request() by dm-raid, see commit 41425f96d7aa ("dm-raid456, md/raid456: fix a deadlock for dm-raid456 while io concu always splits data and flush operation into two separate io, io size of flush submitted by dm always is 0, make_request() will not be called in md_submit_flush_data(). T from introducing issues, add WARN_ON to ensure make_request() no error is returned in this context.
CVE-2024-43854	In the Linux kernel, the following vulnerability has been resolved: block: initialize integrity buffer to zero before writing it to media Metadata added by bio_integrity_prep leads to random kernel memory being written media. For PI metadata this is limited to the app tag that isn't used by kernel generated metadata, but for non-PI metadat memory. Fix this by adding the __GFP_ZERO flag to allocations for writes.
CVE-2024-34118	Illustrator versions 28.5, 27.9.4 and earlier are affected by an Improper Input Validation vulnerability that could lead to an application denial-of-service condition. An atta vulnerability to render the application unresponsive or terminate its execution. Exploitation of this issue requires user interaction in that a victim must open a malicious f
CVE-2024-41834	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability that could lead to d An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a maliciou
CVE-2024-41833	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability that could lead to d An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a maliciou
CVE-2024-41832	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability that could lead to d An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a maliciou
CVE-2024-43856	In the Linux kernel, the following vulnerability has been resolved: dma: fix call order in dmam_free_coherent dmam_free_coherent() frees a DMA allocation, which mak reuse, then calls devres_destroy() to remove and free the data structure used to track the DMA allocation. Between the two calls, it is possible for a concurrent task to r vaddr and add it to the devres list. If this happens, there will be two entries in the devres list with the same vaddr and devres_destroy() can free the wrong entry, trigger dmam_match. Fix by destroying the devres entry before freeing the DMA allocation. kokonut //net/encryption http://sponge2/b9145fe6-0f72-4325-ac2f-a84d81075b03
CVE-2024-43860	In the Linux kernel, the following vulnerability has been resolved: remoteproc: imx_rproc: Skip over memory region when node value is NULL In imx_rproc_addr_init() " of_count_phandle_with_args()" just counts number of phandles. But phandles may be empty. So of_parse_phandle() in the parsing loop (0 < a < nph) may return NULL Adjust this issue by adding NULL-return check. Found by Linux Verification Center (linuxtesting.org) with SVACE. [Fixed title to fit within the prescribed 70-75 charcters
CVE-2024-43857	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix null reference error when checking end of zone This patch fixes a potentially null pointer being is_end_zone_blkaddr() that checks the last block of a zone when f2fs is mounted as a single device.
CVE-2024-43859	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to truncate preallocated blocks in f2fs_file_open() chenyuwen reports a f2fs bug as below: Una pointer dereference at virtual address 0000000000000011 fscrypt_set_bio_crypt_ctx+0x78/0x1e8 f2fs_grab_read_bio+0x78/0x208 f2fs_submit_page_read+0x44/0x15 f2fs_get_read_data_page+0x288/0x5f4 f2fs_get_lock_data_page+0x60/0x190 truncate_partial_data_page+0x108/0x4fc f2fs_do_truncate_blocks+0x344/0x5f0 f2fs_tru f2fs_truncate+0xd8/0x200 f2fs_iget+0x20c/0x5ac do_garbage_collect+0x5d0/0xf6c f2fs_gc+0x22c/0x6a4 f2fs_disable_checkpoint+0xc8/0x310 f2fs_fill_super+0x14bc/ mount_bdev+0x1b4/0x21c f2fs_mount+0x20/0x30 legacy_get_tree+0x50/0xbc vfs_get_tree+0x5c/0x1b0 do_new_mount+0x298/0x4cc path_mount+0x33c/0x5fc __arm invoke_syscall+0x60/0x150 el0_svc_common+0xb8/0xf8 do_el0_svc+0x28/0xa0 el0_svc+0x24/0x84 el0t_64_sync_handler+0x88/0xec It is because inode.i_crypt_info path: - mount - f2fs_fill_super - f2fs_disable_checkpoint - f2fs_gc - f2fs_iget - f2fs_truncate So, let's relocate truncation of preallocated blocks to f2fs_file_open(), after f

CVE Number	Description
CVE-2024-41835	Acrobat Reader versions 20.005.30636, 24.002.20965, 24.002.20964, 24.001.30123 and earlier are affected by an out-of-bounds read vulnerability that could lead to d An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a maliciou
CVE-2024-34125	Dimension versions 3.4.11 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-41854	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacke vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-41861	Substance3D - Sampler versions 4.5 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-43861	In the Linux kernel, the following vulnerability has been resolved: net: usb: qmi_wwan: fix memory leak for not ip packets Free the unused skb when not ip packets arriv
CVE-2024-42677	An issue in Huizhi enterprise resource management system v.1.0 and before allows a local attacker to obtain sensitive information via the /nssys/common/filehandle. A
CVE-2024-42680	An issue in Super easy enterprise management system v.1.0.0 and before allows a local attacker to obtain the server absolute path by entering a single quotation mark
CVE-2024-25024	IBM QRadar Suite Software 1.10.12.0 through 1.10.23.0 and IBM Cloud Pak for Security 1.10.0.0 through 1.10.11.0 stores user credentials in plain clear text which car Force ID: 281430.
CVE-2024-41860	Substance3D - Sampler versions 4.5 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-20790	Dimension versions 3.4.11 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-42282	In the Linux kernel, the following vulnerability has been resolved: net: mediatek: Fix potential NULL pointer dereference in dummy net_device handling Move the freeing mtk_free_dev() to mtk_remove(). Previously, if alloc_netdev_dummy() failed in mtk_probe(), eth->dummy_dev would be NULL. The error path would then call mtk_free free_netdev() assuming dummy_dev was allocated (but it was not), potentially causing a NULL pointer dereference. By moving free_netdev() to mtk_remove(), we ensu mtk_probe() has succeeded and dummy_dev is fully allocated. This addresses a potential NULL pointer dereference detected by Smatch[1].
CVE-2023-43489	Improper access control for some Intel(R) CIP software before version 2.4.10717 may allow an authenticated user to potentially enable denial of service via local acces
CVE-2024-7866	In Xpdf 4.05 (and earlier), a PDF object loop in a pattern resource leads to infinite recursion and a stack overflow.
CVE-2024-41862	Substance3D - Sampler versions 4.5 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-41863	Substance3D - Sampler versions 4.5 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-42259	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gem: Fix Virtual Memory mapping boundaries calculation Calculating the size of the mapped between the requested size and the actual size does not consider the partial mapping offset. This can cause page fault access. Fix the calculation of the starting and en now deduced from the difference between the end and start addresses. Additionally, the calculations have been rewritten in a clearer and more understandable form. [Requires: 60a2066c5005 ("drm/i915/gem: Adjust vma offset for framebuffer mmap offset") (cherry picked from commit 97b6784753da06d9d40232328efc5c5367e5341
CVE-2024-34742	In shouldWrite of OwnersData.java, there is a possible edge case that prevents MDM policies from being persisted due to a logic error in the code. This could lead to lo additional execution privileges needed. User interaction is not needed for exploitation.
CVE-2024-41866	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (Do vulnerability to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious fi

CVE Number	Description
CVE-2024-43853	In the Linux kernel, the following vulnerability has been resolved: cgroup/cpuset: Prevent UAF in proc_cpuset_show() An UAF can happen when /proc/cpuset is read as reproduced by the following methods: 1.add an mdelay(1000) before acquiring the cgroup_lock In the cgroup_path_ns function. 2.$cat /proc/<pid>/cpuset repeatly. 3.$r /sys/fs/cgroup/cpuset/ $umount /sys/fs/cgroup/cpuset/ repeatly. The race that cause this bug can be shown as below: (umount) | (cat /proc/<pid>/cpuset) css_release | css_release_work_fn | css = task_get_css(tsk, cpuset_cgrp_id); css_free_rwork_fn | cgroup_path_ns(css->cgroup, ...); cgroup_destroy_root | mutex_lock(&cgroup_mu cgroup_free_root | | // cgrp was freed, UAF | cgroup_path_ns_locked(cgrp,..); When the cpuset is initialized, the root node top_cpuset.css.cgrp will point to &cgrp_dfl_r operation will allocate cgroup_root, and top_cpuset.css.cgrp will point to the allocated &cgroup_root.cgrp. When the umount operation is executed, top_cpuset.css.cgrp &cgrp_dfl_root.cgrp. The problem is that when rebinding to cgrp_dfl_root, there are cases where the cgroup_root allocated by setting up the root for cgroup v1 is cache Free (UAF) if it is subsequently freed. The descendant cgroups of cgroup v1 can only be freed after the css is released. However, the css of the root will never be relea be freed when it is unmounted. This means that obtaining a reference to the css of the root does not guarantee that css.cgrp->root will not be freed. Fix this problem by proc_cpuset_show(). As cgroup_root is kfree_rcu after commit d23b5c577715 ("cgroup: Make operations on the cgroup root_list RCU safe"), css->cgroup won't be free call cgroup_path_ns_locked, css_set_lock is needed, so it is safe to replace task_get_css with task_css. [1] https://syzkaller.appspot.com/bug?extid=9b1ff7be974a403
CVE-2024-34126	Dimension versions 3.4.11 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-43851	In the Linux kernel, the following vulnerability has been resolved: soc: xilinx: rename cpu_number1 to dummy_cpu_number The per cpu variable cpu_number1 is passe argument "dev_id", but it is not used in this function. So drop the initialization of this variable and rename it to dummy_cpu_number. This patch is to fix the following call CONFIG_DEBUG_ATOMIC_SLEEP is enabled: BUG: sleeping function called from invalid context at include/linux/sched/mm.h:274 in_atomic(): 1, irqs_disabled(): 0, n swapper/0 preempt_count: 1, expected: 0 CPU: 0 PID: 1 Comm: swapper/0 Not tainted 6.1.0 #53 Hardware name: Xilinx Versal vmk180 Eval board rev1.1 (QSPI) (DT) dump_backtrace+0xd0/0xe0 show_stack+0x18/0x40 dump_stack_lvl+0x7c/0xa0 dump_stack+0x18/0x34 __might_resched+0x10c/0x140 __might_sleep+0x4c/0xa0 __kmem_cache_alloc_node+0xf4/0x168 kmalloc_trace+0x28/0x38 __request_percpu_irq+0x74/0x138 xlnx_event_manager_probe+0xf8/0x298 platform_probe+0x68/0
CVE-2024-43819	In the Linux kernel, the following vulnerability has been resolved: kvm: s390: Reject memory region operations for ucontrol VMs This change rejects the KVM_SET_US KVM_SET_USER_MEMORY_REGION2 ioctls when called on a ucontrol VM. This is necessary since ucontrol VMs have kvm->arch.gmap set to 0 and would thus resu further in. Memory management needs to be performed in userspace and using the ioctls KVM_S390_UCAS_MAP and KVM_S390_UCAS_UNMAP. Also improve s39 KVM_SET_USER_MEMORY_REGION and KVM_SET_USER_MEMORY_REGION2. [frankja@linux.ibm.com: commit message spelling fix, subject prefix fix]
CVE-2024-43817	In the Linux kernel, the following vulnerability has been resolved: net: missing check virtio Two missing check in virtio_net_hdr_to_skb() allowed syzbot to crash kernels function the buffer may become non-linear (nr_frags != 0), but since the SKBTX_SHARED_FRAG flag is not set anywhere the __skb_linearize function will not be exec non-linear. Then the condition (offset >= skb_headlen(skb)) becomes true, which causes WARN_ON_ONCE in skb_checksum_help. 2. The struct sk_buff and struct vi mathematically related. (gso_size) must be greater than (needed) otherwise WARN_ON_ONCE. (remainder) must be greater than (needed) otherwise WARN_ON_ON division is without remainder. offset+2 (4191) > skb_headlen() (1116) WARNING: CPU: 1 PID: 5084 at net/core/dev.c:3303 skb_checksum_help+0x5e2/0x740 net/core CPU: 1 PID: 5084 Comm: syz-executor336 Not tainted 6.7.0-rc3-syzkaller-00014-gdf60cee26a2e #0 Hardware name: Google Compute Engine/Google Compute Engi 0010:skb_checksum_help+0x5e2/0x740 net/core/dev.c:3303 Code: 89 e8 83 e0 07 83 c0 03 38 d0 7c 08 84 d2 0f 85 52 01 00 00 44 89 e2 2b 53 74 4c 89 ee 48 c7 c7 <0f> 0b 90 90 e9 87 fe ff ff e8 40 0f 6e f9 e9 4b fa ff ff 48 89 ef RSP: 0018:ffffc90003a9f338 EFLAGS: 00010286 RAX: 0000000000000000 RBX: ffff888025125780 RC ffff888015393b80 RSI: ffffffff814db216 RDI: 0000000000000001 RBP: ffff8880251257f4 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000000000000 000000000000045c R13: 000000000000105f R14: ffff8880251257f0 R15: 000000000000105d FS: 0000555555c24380(0000) GS:ffff8880b9900000(0000) knlGS:0000 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000002000f000 CR3: 0000000023151000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ip_do_fragment+0xa1b/0x18b0 net/ipv4/ip_output.c:777 ip_fragment.c net/ipv4/ip_output.c:584 ip_finish_output_gso net/ipv4/ip_output.c:286 [inline] __ip_finish_output net/ipv4/ip_output.c:308 [inline] __ip_finish_output+0x49c/0x650 net/ip ip_finish_output+0x31/0x310 net/ipv4/ip_output.c:323 NF_HOOK_COND include/linux/netfilter.h:303 [inline] ip_output+0x13b/0x2a0 net/ipv4/ip_output.c:433 dst_outpu ip_local_out+0xaf/0x1a0 net/ipv4/ip_output.c:129 iptunnel_xmit+0x5b4/0x9b0 net/ipv4/ip_tunnel_core.c:82 ipip6_tunnel_xmit net/ipv6/sit.c:1034 [inline] sit_tunnel_xmit- __netdev_start_xmit include/linux/netdevice.h:4940 [inline] netdev_start_xmit include/linux/netdevice.h:4954 [inline] xmit_one net/core/dev.c:3545 [inline] dev_hard_sta net/core/dev.c:3561 __dev_queue_xmit+0x7c1/0x3d60 net/core/dev.c:4346 dev_queue_xmit include/linux/netdevice.h:3134 [inline] packet_xmit+0x257/0x380 net/pack net/packet/af_packet.c:3087 [inline] packet_sendmsg+0x24ca/0x5240 net/packet/af_packet.c:3119 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0 __sys_sendto+0x255/0x340 net/socket.c:2190 __do_sys_sendto net/socket.c:2202 [inline] __se_sys_sendto net/socket.c:2198 [inline] __x64_sys_sendto+0xe0/0x1b0 do_syscall_x64 arch/x86/entry/common.c:51 [inline] do_syscall_64+0x40/0x110 arch/x86/entry/common.c:82 entry_SYSCALL_64_after_hwframe+0x63/0x6b Found by (linuxtesting.org) with Syzkaller
CVE-2024-34137	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS) condition. vulnerability to crash the application, resulting in a DoS. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-43850	In the Linux kernel, the following vulnerability has been resolved: soc: qcom: icc-bwmon: Fix refcount imbalance seen during bwmon_remove The following warning is s to refcount imbalance, fix this by releasing the OPPs after use. Logs: WARNING: at drivers/opp/core.c:1640 _opp_table_kref_release+0x150/0x158 Hardware name: Q X1E80100 CRD (DT) ... Call trace: _opp_table_kref_release+0x150/0x158 dev_pm_opp_remove_table+0x100/0x1b4 devm_pm_opp_of_table_release+0x10/0x1c dev devres_release_all+0xa4/0x104 device_unbind_cleanup+0x18/0x60 device_release_driver_internal+0x1ec/0x228 driver_detach+0x50/0x98 bus_remove_driver+0x6c/ platform_driver_unregister+0x14/0x20 bwmon_driver_exit+0x18/0x524 [icc_bwmon] __arm64_sys_delete_module+0x184/0x264 invoke_syscall+0x48/0x118 el0_svc_c do_el0_svc+0x20/0x2c el0_svc+0x34/0xdc el0t_64_sync_handler+0x13c/0x158 el0t_64_sync+0x190/0x194 --[end trace 0000000000000000]---
CVE-2024-7775	The Contact Form by Bit Form: Multi Step Form, Calculation Contact Form, Payment Contact Form & Custom Contact Form builder plugin for WordPress is vulnerable uploads due to missing input validation in the addCustomCode function in versions 2.0 to 2.13.9. This makes it possible for authenticated attackers, with Administrator-l upload arbitrary JavaScript files to the affected site's server.
CVE-2024-42316	In the Linux kernel, the following vulnerability has been resolved: mm/mglru: fix div-by-zero in vmpressure_calc_level() evict_folios() uses a second pass to reclaim folio writeback and become clean before it finishes the first pass, since folio_rotate_reclaimable() cannot handle those folios due to the isolation. The second pass tries to av deducting scan_control->nr_scanned. However, this can result in underflow of nr_scanned, under a condition where shrink_folio_list() does not increment nr_scanned, The underflow can cause the divisor, i.e., scale=scanned+reclaimed in vmpressure_calc_level(), to become zero, resulting in the following crash: [exception RIP: vmpre process_one_work at ffffffffa3313f2b Since scan_control->nr_scanned has no established semantics, the potential double counting has minimal risks. Therefore, fix the scan_control->nr_scanned in evict_folios().

CVE Number	Description
CVE-2024-42315	In the Linux kernel, the following vulnerability has been resolved: exfat: fix potential deadlock on __exfat_get_dentry_set When accessing a file with more entries than E array is allocated in __exfat_get_entry_set. The problem is that the bh-array is allocated with GFP_KERNEL. It does not make sense. In the following cases, a deadloc processes may occur. CPU0 CPU1 ---- ---- kswapd balance_pgdat lock(fs_reclaim) exfat_iterate lock(&sbi->s_lock) exfat_readdir exfat_get_uniname_from_ext_entry e __exfat_get_dentry_set kmalloc_array ... lock(fs_reclaim) ... evict exfat_evict_inode lock(&sbi->s_lock) To fix this, let's allocate bh-array with GFP_NOFS.
CVE-2024-34138	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacke to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-42311	In the Linux kernel, the following vulnerability has been resolved: hfs: fix to initialize fields of hfs_inode_info after hfs_alloc_inode() Syzbot reports uninitialized value acc detected capacity change from 0 to 64 == BUG: KMSAN: uninit-value in hfs_revalidate_dentry+0x3(hfs_revalidate_dentry+0x307/0x3f0 fs/hfs/sysdep.c:30 d_revalidate fs/namei.c:862 [inline] lookup_fast+0x89e/0x8e0 fs/namei.c:1649 walk_component fs/namei.c:2001 link_path_walk+0x817/0x1480 fs/namei.c:2332 path_lookupat+0xd9/0x6f0 fs/namei.c:2485 filename_lookup+0x22e/0x740 fs/namei.c:2515 user_path_at_empty+0x8b/ user_path_at include/linux/namei.h:57 [inline] do_mount fs/namespace.c:3689 [inline] __do_sys_mount fs/namespace.c:3898 [inline] __se_sys_mount+0x66b/0x810 fs __x64_sys_mount+0xe4/0x140 fs/namespace.c:3875 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b BUG: KMSAN: uninit-value in hfs_ext_read_extent fs/hfs/extent.c:196 [inline] BUG: KMSAN: uninit-value in hfs_get_blc fs/hfs/extent.c:366 hfs_ext_read_extent fs/hfs/extent.c:196 [inline] hfs_get_block+0x92d/0x1620 fs/hfs/extent.c:366 block_read_full_folio+0x4ff/0x11b0 fs/buffer.c:2271 fs/hfs/inode.c:39 filemap_read_folio+0x148/0x4f0 mm/filemap.c:2426 do_read_cache_folio+0x7c8/0xd90 mm/filemap.c:3553 do_read_cache_page mm/filemap.c:3595 read_cache_page+0xfb/0x2f0 mm/filemap.c:3604 read_mapping_page include/linux/pagemap.h:755 [inline] hfs_btree_open+0x928/0x1ae0 fs/hfs/btree.c:78 hfs_mdb_ fs/hfs/mdb.c:204 hfs_fill_super+0x1fb1/0x2790 fs/hfs/super.c:406 mount_bdev+0x628/0x920 fs/super.c:1359 hfs_mount+0xcd/0xe0 fs/hfs/super.c:456 legacy_get_tree+ vfs_get_tree+0xdc/0x5d0 fs/super.c:1489 do_new_mount+0x7a9/0x16f0 fs/namespace.c:3145 path_mount+0xf98/0x26a0 fs/namespace.c:3475 do_mount fs/namespa __do_sys_mount fs/namespace.c:3697 [inline] __se_sys_mount+0x919/0x9e0 fs/namespace.c:3674 __ia32_sys_mount+0x15b/0x1b0 fs/namespace.c:3674 do_sysca arch/x86/entry/common.c:112 [inline] __do_fast_syscall_32+0xa2/0x100 arch/x86/entry/common.c:178 do_fast_syscall_32+0x37/0x80 arch/x86/entry/common.c:203 d arch/x86/entry/common.c:246 entry_SYSENTER_compat_after_hwframe+0x70/0x82 Uninit was created at: __alloc_pages+0x9a6/0xe00 mm/page_alloc.c:4590 __allo include/linux/gfp.h:238 [inline] alloc_pages_node include/linux/gfp.h:261 [inline] alloc_slab_page mm/slub.c:2190 [inline] allocate_slab mm/slub.c:2354 [inline] new_slab ___slab_alloc+0x16b5/0x3970 mm/slub.c:3540 __slab_alloc mm/slub.c:3625 [inline] __slab_alloc_node mm/slub.c:3678 [inline] slab_alloc_node mm/slub.c:3850 [inline kmem_cache_alloc_lru+0x64d/0xb30 mm/slub.c:3879 alloc_inode_sb include/linux/fs.h:3018 [inline] hfs_alloc_inode+0x5a/0xc0 fs/hfs/super.c:165 alloc_inode+0x83/0 new_inode_pseudo fs/inode.c:1005 [inline] new_inode+0x38/0x4f0 fs/inode.c:1031 hfs_new_inode+0x61/0x1010 fs/hfs/inode.c:186 hfs_mkdir+0x54/0x250 fs/hfs/dir.c: fs/namei.c:4126 do_mkdirat+0x529/0x810 fs/namei.c:4149 __do_sys_mkdirat fs/namei.c:4164 [inline] __se_sys_mkdirat fs/namei.c:4162 [inline] __x64_sys_mkdirat+0 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x63/0x6b It missed .cached_start and .cached_blocks fields in struct hfs_inode_info after hfs_alloc_inode(), fix it.
CVE-2024-42310	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in cdv_intel_lvds_get_modes In cdv_intel_lvds_get_modes() drm_mode_duplicate() is assigned to mode, which will lead to a NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd.
CVE-2024-42309	In the Linux kernel, the following vulnerability has been resolved: drm/gma500: fix null pointer dereference in psb_intel_lvds_get_modes In psb_intel_lvds_get_modes() drm_mode_duplicate() is assigned to mode, which will lead to a possible NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd.
CVE-2024-42307	In the Linux kernel, the following vulnerability has been resolved: cifs: fix potential null pointer use in destroy_workqueue in init_cifs error path Dan Carpenter reported a fs/smb/client/cifsfs.c:1981 init_cifs() error: we previously assumed 'serverclose_wq' could be null (see line 1895) The patch which introduced the serverclose workqueu error paths in init_cifs() for freeing it on errors.
CVE-2023-52889	In the Linux kernel, the following vulnerability has been resolved: apparmor: Fix null pointer deref when receiving skb during sock creation The panic below is observed with secmark set while an ICMP raw socket is being created. SK_CTX(sk)->label is updated in apparmor_socket_post_create(), but the packet is delivered to the socke pointer dereference. Drop the packet if label context is not set. BUG: kernel NULL pointer dereference, address: 000000000000004c #PF: supervisor read access in ke error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 0 PID: 407 Comm: a.out Not tainted 6.4.12-arch1-1 #1 3e6fa2753a2d75925c34ecb78e22e85a65d083df Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 05/28/2020 F 0010:aa_label_next_confined+0xb/0x40 Code: 00 00 48 89 ef e8 d5 25 0c 00 e9 66 ff ff ff 90 90 90 90 90 90 90 90 90 90 90 90 90 90 66 0f 1f 00 0f 1f 44 00 00 8 63 d0 48 8d 14 d7 eb 0b 83 c0 01 48 83 c2 RSP: 0018:ffffa92940003b08 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000000 RCX: 0000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffff8b57471e7800 R08: ffff8b574c642400 R09: 0000000000000002 R10: ffffffffbd820eeb R11: ffffffffbeb7ff00 0000000000000001 R14: 0000000000000001 R15: 0000000000000000 FS: 00007fb092ea7640(0000) GS:ffff8b577bc00000(0000) knlGS:0000000000000000 CS: 00 0000000080050033 CR2: 000000000000004c CR3: 00000001020f2005 CR4: 00000000007706f0 PKRU: 55555554 Call Trace: <IRQ> ? __die+0x23/0x70 ? page_fau exc_page_fault+0x7f/0x180 ? asm_exc_page_fault+0x26/0x30 ? aa_label_next_confined+0xb/0x40 apparmor_secmark_check+0xec/0x330 security_sock_rcv_skb+0x sk_filter_trim_cap+0x47/0x250 sock_queue_rcv_skb_reason+0x20/0x60 raw_rcv+0x13c/0x210 raw_local_deliver+0x1f3/0x250 ip_protocol_deliver_rcu+0x4f/0x2f0 ip_l __netif_receive_skb_one_core+0x89/0xa0 netif_receive_skb+0x119/0x170 ? __netdev_alloc_skb+0x3d/0x140 vmxnet3_rq_rx_complete+0xb23/0x1010 [vmxnet3 56a84f9c97178c57a43a24ec073b45a9d6f01f3a] vmxnet3_poll_rx_only+0x36/0xb0 [vmxnet3 56a84f9c97178c57a43a24ec073b45a9d6f01f3a] __napi_poll+0x28/0x1b0 __do_softirq+0xd1/0x2c8 __irq_exit_rcu+0xbb/0xf0 common_interrupt+0x86/0xa0 </IRQ> <TASK> asm_common_interrupt+0x26/0x40 RIP: 0010:apparmor_socket_po 48 85 ff 75 a1 eb b1 0f 1f 80 00 00 00 00 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f 1e fa 0f 1f 44 00 00 41 54 <55> 48 89 fd 53 45 85 c0 0f 84 b2 00 00 0 0018:ffffa92940ce7e50 EFLAGS: 00000286 RAX: ffffffffbc756440 RBX: 0000000000000000 RCX: 0000000000000001 RDX: 0000000000000003 RSI: 0000000000000 RBP: 0000000000000001 R08: 0000000000000000 R09: 0000000000000000 R10: ffff8b57444cec70 R11: 0000000000000000 R12: 0000000000000003 R13: 00000 ffff8b574eaab740 R15: ffffffffbd8e4748 ? __pfx_apparmor_socket_post_create+0x10/0x10 security_socket_post_create+0x4b/0x80 __sock_create+0x176/0x1f0 __sys __x64_sys_socket+0x17/0x20 do_syscall_64+0x5d/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 ? do_syscall_64+0x6c/0x90 entry_SYSCALL_64_aft
CVE-2024-42262	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Fix potential memory leak in the performance extension If fetching of userspace memory fail sync objs looked up until that point will be leaked because of the missing drm_syncobj_put. Fix it by exporting and using a common cleanup helper. (cherry picked from 484de39fa5f5b7bd0c5f2e2c5265167250ef7501)
CVE-2024-39387	Bridge versions 13.0.8, 14.1.1 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could levera mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-39395	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (Do vulnerability to crash the application, resulting in a DoS condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.

CVE Number	Description
CVE-2024-42263	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Fix potential memory leak in the timestamp extension If fetching of userspace memory fails d objs looked up until that point will be leaked because of the missing drm_syncobj_put. Fix it by exporting and using a common cleanup helper. (cherry picked from com 753ce4fea62182c77e1691ab4f9022008f25b62e)
CVE-2024-42298	In the Linux kernel, the following vulnerability has been resolved: ASoC: fsl: fsl_qmc_audio: Check devm_kasprintf() returned value devm_kasprintf() can return a NULL returned value is not checked. Fix this lack and check the returned value.
CVE-2024-42297	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to don't dirty inode for readonly filesystem syzbot reports f2fs bug as below: kernel BUG at fs/f 0010:f2fs_evict_inode+0x1576/0x1590 fs/f2fs/inode.c:933 Call Trace: evict+0x2a4/0x620 fs/inode.c:664 dispose_list fs/inode.c:697 [inline] evict_inodes+0x5f8/0x690 fs generic_shutdown_super+0x9d/0x2c0 fs/super.c:675 kill_block_super+0x44/0x90 fs/super.c:1667 kill_f2fs_super+0x303/0x3b0 fs/f2fs/super.c:4894 deactivate_locked_ fs/super.c:484 cleanup_mnt+0x426/0x4c0 fs/namespace.c:1256 task_work_run+0x24a/0x300 kernel/task_work.c:180 ptrace_notify+0x2cd/0x380 kernel/signal.c:2399 p include/linux/ptrace.h:411 [inline] ptrace_report_syscall_exit include/linux/ptrace.h:473 [inline] syscall_exit_work kernel/entry/common.c:251 [inline] syscall_exit_to_use kernel/entry/common.c:278 [inline] __syscall_exit_to_user_mode_work kernel/entry/common.c:283 [inline] syscall_exit_to_user_mode+0x15c/0x280 kernel/entry/comm do_syscall_64+0x50/0x110 arch/x86/entry/common.c:88 entry_SYSCALL_64_after_hwframe+0x63/0x6b The root cause is: - do_sys_open - f2fs_lookup - __f2fs_find_ f2fs_mark_inode_dirty_sync - f2fs_dirty_inode - set_inode_flag(inode, FI_DIRTY_INODE) - umount - kill_f2fs_super - kill_block_super - generic_shutdown_super - syn sync_filesystem() - evict_inodes - iput - f2fs_evict_inode - f2fs_bug_on(sbi, is_inode_flag_set(inode, FI_DIRTY_INODE)) : trigger kernel panic When we try to repair i_c filesystem, let's skip dirty inode to avoid panic in later f2fs_evict_inode().
CVE-2024-42268	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix missing lock on sync reset reload On sync reset reload work, when remote host updates performed on that host, it misses taking devlink lock before calling devlink_remote_reload_actions_performed() which results in triggering lock assert like the following: net/devlink/core.c:261 devl_assert_locked+0x3e/0x50 … CPU: 4 PID: 1164 Comm: kworker/u96:6 Tainted: G S W 6.10.0-rc2+ #116 Hardware name: Supermicro SYS- BIOS 2.0 12/18/2015 Workqueue: mlx5_fw_reset_events mlx5_sync_reset_reload_work [mlx5_core] RIP: 0010:devl_assert_locked+0x3e/0x50 … Call Trace: <TASK> devl_assert_locked+0x3e/0x50 ? report_bug+0x160/0x280 ? handle_bug+0x3f/0x80 ? exc_invalid_op+0x17/0x40 ? asm_exc_invalid_op+0x1a/0x20 ? devl_assert_lock devlink_notify+0x88/0x2b0 ? mlx5_attach_device+0x20c/0x230 [mlx5_core] ? __pfx_devlink_notify+0x10/0x10 ? process_one_work+0x4b6/0xbb0 process_one_work+
CVE-2024-42269	In the Linux kernel, the following vulnerability has been resolved: netfilter: iptables: Fix potential null-ptr-deref in ip6table_nat_table_init(). ip6table_nat_table_init() acce >ptr[ip6table_nat_net_ops.id], but the function is exposed to user space before the entry is allocated via register_pernet_subsys(). Let's call register_pernet_subsys() b
CVE-2024-42294	In the Linux kernel, the following vulnerability has been resolved: block: fix deadlock between sd_remove & sd_release Our test report the following hung task: [2538.4 "kworker/0:0":7 blocked for more than 188 seconds. [2538.459427] Call trace: [2538.459430] __switch_to+0x174/0x338 [2538.459436] __schedule+0x628/0x9c4 [25 [2538.459447] schedule_preempt_disabled+0x24/0x40 [2538.459453] __mutex_lock+0x3ec/0xf04 [2538.459456] __mutex_lock_slowpath+0x14/0x24 [2538.459459 2538.459462] del_gendisk+0xdc/0x350 [2538.459466] sd_remove+0x30/0x60 [2538.459470] device_release_driver_internal+0x1c4/0x2c4 [2538.459474] device_rele 2538.459478] bus_remove_device+0x15c/0x174 [2538.459483] device_del+0x1d0/0x358 [2538.459488] __scsi_remove_device+0xa8/0x198 [2538.459493] scsi_for 2538.459497] scsi_remove_host+0x80/0x180 [2538.459502] usb_stor_disconnect+0x68/0xf4 [2538.459506] usb_unbind_interface+0xd4/0x280 [2538.459510] device_release_driver_internal+0x1c4/0x2c4 [2538.459514] device_release_driver+0x18/0x28 [2538.459518] bus_remove_device+0x15c/0x174 [2538.459523] devic 2538.459528] usb_disable_device+0x84/0x194 [2538.459532] usb_disconnect+0xec/0x300 [2538.459537] hub_event+0xb80/0x1870 [2538.459541] process_schedu 2538.459545] worker_thread+0x244/0x334 [2538.459549] kthread+0x114/0x1bc [2538.461001] INFO: task "fsck.":15415 blocked for more than 188 seconds. [2538.4 2538.461016] __switch_to+0x174/0x338 [2538.461021] __schedule+0x628/0x9c4 [2538.461025] schedule+0x7c/0xe8 [2538.461030] blk_queue_enter+0xc4/0x160 [blk_mq_alloc_request+0x120/0x1d4 [2538.461037] scsi_execute_cmd+0x7c/0x23c [2538.461040] ioctl_internal_command+0x5c/0x164 [2538.461046] scsi_set_med 2538.461051] sd_release+0x50/0x94 [2538.461054] blkdev_put+0x190/0x28c [2538.461058] blkdev_release+0x28/0x40 [2538.461063] __fput+0xf8/0x2a8 [2538.46 2538.461070] __arm64_sys_close+0x84/0xe8 [2538.461073] invoke_syscall+0x58/0x114 [2538.461078] el0_svc_common+0xac/0xe0 [2538.461082] do_el0_svc+0x el0_svc+0x38/0x68 [2538.461090] el0t_64_sync_handler+0x68/0xbc [2538.461093] el0t_64_sync+0x1a8/0x1ac T1: T2: sd_remove del_gendisk __blk_mark_disk_de >mq_freeze_depth bdev_release mutex_lock(&disk->open_mutex) sd_release scsi_execute_cmd blk_queue_enter wait_event(!q->mq_freeze_depth) mutex_lock(&dis set GD_OWNS_QUEUE, so QUEUE_FLAG_DYING is not set in this scenario. This is a classic ABBA deadlock. To fix the deadlock, make sure we don't try to acquire the queue.
CVE-2024-42270	In the Linux kernel, the following vulnerability has been resolved: netfilter: iptables: Fix null-ptr-deref in iptable_nat_table_init(). We had a report that iptables-restore so at boot time. [0] The problem is that iptable_nat_table_init() is exposed to user space before the kernel fully initialises netns. In the small race window, a user could call accesses net_generic(net, iptable_nat_net_id), which is available only after registering iptable_nat_net_ops. Let's call register_pernet_subsys() before xt_register_temp bpfilter_umh pid 11702 Started bpfilter BUG: kernel NULL pointer dereference, address: 0000000000000013 PF: supervisor write access in kernel mode PF: error_cod PGD 0 P4D 0 PREEMPT SMP NOPTI CPU: 2 PID: 11879 Comm: iptables-restor Not tainted 6.1.92-99.174.amzn2023.x86_64 #1 Hardware name: Amazon EC2 c6i.4 RIP: 0010:iptable_nat_table_init (net/ipv4/netfilter/iptable_nat.c:87 net/ipv4/netfilter/iptable_nat.c:121) iptable_nat Code: 10 4c 89 f6 48 89 ef e8 0b 19 bb ff 41 89 c4 85 28 41 83 ff 04 75 dc 48 8b 44 24 08 48 8b 0c 24 <48> 89 08 4c 89 ef e8 a2 3b a2 cf 48 83 c4 10 44 89 e0 5b 5d 41 5c RSP: 0018:ffffbef902843cd0 EFLAGS: 0001024 RBX: ffff9f4b052caa20 RCX: ffff9f4b20988d80 RDX: 0000000000000000 RSI: 0000000000000064 RDI: ffffffffc04201c0 RBP: ffff9f4b29394000 R08: ffff9f4b07f77258 R 0000000000000000 R11: ffff9f4b09635388 R12: 0000000000000000 R13: ffff9f4b1a3c6c00 R14: ffff9f4b20988e20 R15: 0000000000000004 FS: 00007f6284340000((knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000013 CR3: 00000001d10a6005 CR4: 00000000007706e0 DR 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? sh (arch/x86/kernel/dumpstack.c:259) ? show_trace_log_lvl (arch/x86/kernel/dumpstack.c:259) ? xt_find_table_lock (net/netfilter/x_tables.c:1259) ? __die_body.cold (arch arch/x86/kernel/dumpstack.c:420) ? page_fault_oops (arch/x86/mm/fault.c:727) ? exc_page_fault (./arch/x86/include/asm/irqflags.h:40 ./arch/x86/include/asm/irqflags.h arch/x86/mm/fault.c:1518) ? asm_exc_page_fault (./arch/x86/include/asm/idtentry.h:570) ? iptable_nat_table_init (net/ipv4/netfilter/iptable_nat.c:87 net/ipv4/netfilter/ipta xt_find_table_lock (net/netfilter/x_tables.c:1259) xt_request_find_table_lock (net/netfilter/x_tables.c:1287) get_info (net/ipv4/netfilter/ip_tables.c:965) ? security_capable (discriminator 13)) ? ns_capable (kernel/capability.c:376 kernel/capability.c:397) ? do_ipt_get_ctl (net/ipv4/netfilter/ip_tables.c:1656) ? bpfilter_send_req (net/bpfilter/bp nf_getsockopt (net/netfilter/nf_sockopt.c:116) ip_getsockopt (net/ipv4/ip_sockglue.c:1827) __sys_getsockopt (net/socket.c:2327) __x64_sys_getsockopt (net/socket.c:2 net/socket.c:2339) do_syscall_64 (arch/x86/entry/common.c:51 arch/x86/entry/common.c:81) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) RIP 8b 0d 45 28 0f 00 f7 d8 64 89 01 48 83 c8 ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 49 89 ca b8 37 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 0a c3 66 0f 1f 84 00 00 002b:00007ffd1f83d638 EFLAGS: 00000246 ORIG_RAX: 0000000000000037 RAX: ffffffffffffffda RBX: 00007ffd1f83d680 RCX: 00007f62844685ee RDX: 0000000000 RDI: 0000000000000004 RBP: 0000000000000004 R08: 00007ffd1f83d670 R09: 0000558798ffa2a0 R10: 00007ffd1f83d680 R11: 0000000000000246 R12: 00007ffd truncated---

CVE Number	Description
CVE-2024-42272	In the Linux kernel, the following vulnerability has been resolved: sched: act_ct: take care of padding in struct zones_ht_key Blamed commit increased lookup key size because zones_ht_key got a struct net pointer. Make sure rhashtable_lookup() is not using the padding bytes which are not initialized. BUG: KMSAN: uninit-value in rh include/linux/rhashtable.h:376 [inline] BUG: KMSAN: uninit-value in __rhashtable_lookup include/linux/rhashtable.h:607 [inline] BUG: KMSAN: uninit-value in rhashtabl include/linux/rhashtable.h:646 [inline] BUG: KMSAN: uninit-value in rhashtable_lookup_fast include/linux/rhashtable.h:672 [inline] BUG: KMSAN: uninit-value in tcf_ct_f net/sched/act_ct.c:329 rht_ptr_rcu include/linux/rhashtable.h:376 [inline] __rhashtable_lookup include/linux/rhashtable.h:607 [inline] rhashtable_lookup include/linux/rha rhashtable_lookup_fast include/linux/rhashtable.h:672 [inline] tcf_ct_flow_table_get+0x611/0x2260 net/sched/act_ct.c:329 tcf_ct_init+0xa67/0x2890 net/sched/act_ct.c: tcf_action_init_1+0x6cc/0xb30 net/sched/act_api.c:1425 tcf_action_init+0x458/0xf00 net/sched/act_api.c:1488 tcf_action_add net/sched/act_api.c:2061 [inline] tc_ctl_a net/sched/act_api.c:2118 rtnetlink_rcv_msg+0x12fc/0x1410 net/core/rtnetlink.c:6647 netlink_rcv_skb+0x375/0x650 net/netlink/af_netlink.c:2550 rtnetlink_rcv+0x34/0x4 netlink_unicast_kernel net/netlink/af_netlink.c:1331 [inline] netlink_unicast+0xf52/0x1260 net/netlink/af_netlink.c:1357 netlink_sendmsg+0x10da/0x11e0 net/netlink/af_ sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 ____sys_sendmsg+0x877/0xb60 net/socket.c:2597 ___sys_sendmsg+ __sys_sendmsg net/socket.c:2680 [inline] __do_sys_sendmsg net/socket.c:2689 [inline] __se_sys_sendmsg net/socket.c:2687 [inline] __x64_sys_sendmsg+0x307/0x x64_sys_call+0x2dd6/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x entry_SYSCALL_64_after_hwframe+0x77/0x7f Local variable key created at: tcf_ct_flow_table_get+0x4a/0x2260 net/sched/act_ct.c:324 tcf_ct_init+0xa67/0x2890 net/
CVE-2024-42289	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: During vport delete send async logout explicitly During vport delete, it is observed that d because of stale entries in outstanding command array. For all these stale I/O entries, eh_abort was issued and aborted (fast_fail_io = 2009h) but I/Os could not compl process of deleting. BUG: kernel NULL pointer dereference, address: 000000000000001c #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-p Oops: 0000 [#1] PREEMPT SMP NOPTI Workqueue: qla2xxx_wq qla_do_work [qla2xxx] RIP: 0010:dma_direct_unmap_sg+0x51/0x1e0 RSP: 0018:ffffa1e1e150fc68 E 0000000000000000 RBX: 0000000000000021 RCX: 0000000000000001 RDX: 0000000000000021 RSI: 0000000000000000 RDI: ffff8ce208a7a0d0 RBP: ffff8ce208a R09: ffff8ce378aac9c8 R10: ffff8ce378aac8a0 R11: ffffa1e1e150f9d8 R12: 0000000000000000 R13: 0000000000000000 R14: ffff8ce378aac9c8 R15: 0000000000000 0000000000000000(0000) GS:ffff8d217f000000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000001c C 0000000000350ee0 Call Trace: <TASK> qla2xxx_qpair_sp_free_dma+0x417/0x4e0 ? qla2xxx_qpair_sp_compl+0x10d/0x1a0 ? qla2x00_status_entry+0x768/0x2830 ? dequeue_entity+0x100/0x3c0 ? qla24xx_process_response_queue+0x6a1/0x19e0 ? __schedule+0x2d5/0x1140 ? qla_do_work+0x47/0x60 ? process_one_work+0x26 process_one_work+0x440/0x440 ? worker_thread+0x2d/0x3d0 ? process_one_work+0x440/0x440 ? kthread+0x156/0x180 ? set_kthread_struct+0x50/0x50 ? ret_from out async logout explicitly for all the ports during vport delete.
CVE-2024-42288	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Fix for possible memory corruption Init Control Block is dereferenced incorrectly. Correc
CVE-2024-42286	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: validate nvme_local_port correctly The driver load failed with error message, qla2xxx [0 register_localport failed: ret=ffffffef and with a kernel crash, BUG: unable to handle kernel NULL pointer dereference at 0000000000000070 Workqueue: events_unbou [qla2xxx] RIP: 0010:nvme_fc_register_remoteport+0x16/0x430 [nvme_fc] RSP: 0018:ffffaaa040eb3d98 EFLAGS: 00010282 RAX: 0000000000000000 RBX: ffff9dfb46b 0000000000000000 RDX: ffff9dfb46b78da8 RSI: ffffaaa040eb3e08 RDI: 0000000000000000 RBP: ffff9dfb612a0a58 R08: ffffffffaf1d6270 R09: 3a34303a30303030 R1 2078787832616c71 R12: ffff9dfb46b78dd4 R13: ffff9dfb46b78c24 R14: ffff9dfb41525300 R15: ffff9dfb46b78da8 FS: 0000000000000000(0000) GS:ffff9dfc67c00000(0 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000070 CR3: 000000018da10004 CR4: 00000000000206f0 Call Trace: qla_nvme_register_ qla2x00_dfs_create_rport+0x231/0x270 [qla2xxx] qla2x00_update_fcport+0x2a1/0x3c0 [qla2xxx] qla_register_fcport_fn+0x54/0xc0 [qla2xxx] Exit the qla_nvme_registe qla_nvme_register_hba() fails and correctly validate nvme_local_port.
CVE-2024-42277	In the Linux kernel, the following vulnerability has been resolved: iommu: sprd: Avoid NULL deref in sprd_iommu_hw_en In sprd_iommu_cleanup() before calling functi >sdev is equal to NULL, which leads to null dereference. Found by Linux Verification Center (linuxtesting.org) with SVACE.
CVE-2024-42278	In the Linux kernel, the following vulnerability has been resolved: ASoC: TAS2781: Fix tasdev_load_calibrated_data() This function has a reversed if statement so it's e NULL dereference.
CVE-2024-42283	In the Linux kernel, the following vulnerability has been resolved: net: nexthop: Initialize all fields in dumped nexthops struct nexthop_grp contains two reserved fields th nla_put_nh_group(), and carry garbage. This can be observed e.g. with strace (edited for clarity): # ip nexthop add id 1 dev lo # ip nexthop add id 101 group 1 # strace ... recvmsg(... [{nla_len=12, nla_type=NHA_GROUP}, [{id=1, weight=0, resvd1=0x69, resvd2=0x67}]] ...) = 52 The fields are reserved and therefore not currently used. memory, and the fact they are not just zero complicates repurposing of the fields for new ends. Initialize the full structure.
CVE-2024-43818	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd: Adjust error handling in case of absent codec device acpi_get_first_physical_node() can such device, ACPI table error, reference count drop to 0, etc). Existing check just emit error message, but doesn't perform return. Then this NULL pointer is passed to devm_acpi_dev_add_driver_gpios() where it is dereferenced. Adjust this error handling by adding error code return. Found by Linux Verification Center (linuxtesting.org
CVE-2024-42320	In the Linux kernel, the following vulnerability has been resolved: s390/dasd: fix error checks in dasd_copy_pair_store() dasd_add_busid() can return an error via ERR_ However, two callsites in dasd_copy_pair_store() do not check the result, potentially resulting in a NULL pointer dereference. Fix this by checking the result with IS_ER stack.
CVE-2024-43827	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add null check before access structs In enable_phantom_plane, we should better ch accessing various structs.
CVE-2024-34127	InDesign Desktop versions ID19.4, ID18.5.2 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacke vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-43836	In the Linux kernel, the following vulnerability has been resolved: net: ethtool: pse-pd: Fix possible null-deref Fix a possible null dereference when a PSE supports both the netlink attributes is specified. The c33 or PoDL PSE capabilities are already validated in the ethnl_set_pse_validate() call.

CVE Number	Description
CVE-2024-43835	In the Linux kernel, the following vulnerability has been resolved: virtio_net: Fix napi_skb_cache_put warning After the commit bdacf3e34945 ("net: Use nested-BH lock merged, the following warning began to appear: WARNING: CPU: 5 PID: 1 at net/core/skbuff.c:1451 napi_skb_cache_put+0x82/0x4b0 __warn+0x12f/0x340 napi_skb_ napi_skb_cache_put+0x82/0x4b0 report_bug+0x165/0x370 handle_bug+0x3d/0x80 exc_invalid_op+0x1a/0x50 asm_exc_invalid_op+0x1a/0x20 __free_old_xmit+0x1c napi_skb_cache_put+0x82/0x4b0 __free_old_xmit+0x1c8/0x510 __free_old_xmit+0x1c8/0x510 __pfx___free_old_xmit+0x10/0x10 The issue arises because virtio is as context even when it's not, such as in the netpoll case. To resolve this, modify virtnet_poll_tx() to only set NAPI when budget is available. Same for virtnet_poll_cleantx(was in a NAPI context.
CVE-2024-43834	In the Linux kernel, the following vulnerability has been resolved: xdp: fix invalid wait context of page_pool_destroy() If the driver uses a page pool, it creates a page po reference count of page pool is 1 as default. A page pool will be destroyed only when a reference count reaches 0. page_pool_destroy() is used to destroy page pool, it When a page pool is destroyed, ->disconnect() is called, which is mem_allocator_disconnect(). This function internally acquires mutex_lock(). If the driver uses XDP, it xdp_rxq_info_reg_mem_model(). The xdp_rxq_info_reg_mem_model() internally increases a page pool reference count if a memory model is a page pool. Now the ref page pool, the driver should call both page_pool_destroy() and xdp_unreg_mem_model(). The xdp_unreg_mem_model() internally calls page_pool_destroy(). Only pag reference count. If a driver calls page_pool_destroy() then xdp_unreg_mem_model(), we will face an invalid wait context warning. Because xdp_unreg_mem_model() c rcu_read_lock(). The page_pool_destroy() internally acquires mutex_lock(). Splat looks like: ============================== [BUG: Invalid wait context] 6.10.0-r ---------- ethtool/1806 is trying to lock: ffffffff90387b90 (mem_id_lock){+.+.}-{4:4}, at: mem_allocator_disconnect+0x73/0x150 other info that might help us debug this: ethtool/1806: stack backtrace: CPU: 0 PID: 1806 Comm: ethtool Tainted: G W 6.10.0-rc6+ #4 f916f41f172891c800f2fed Hardware name: ASUS System Product Name 11/01/2021 Call Trace: <TASK> dump_stack_lvl+0x7e/0xc0 __lock_acquire+0x1681/0x4de0 ? _printk+0x64/0xe0 ? __pfx_mark_lock.part.0+0x10/0x10 ? __pfx___lock lock_acquire+0x1b3/0x580 ? mem_allocator_disconnect+0x73/0x150 ? __wake_up_klogd.part.0+0x16/0xc0 ? __pfx_lock_acquire+0x10/0x10 ? dump_stack_lvl+0x91/ __mutex_lock+0x15c/0x1690 ? mem_allocator_disconnect+0x73/0x150 ? __pfx_prb_read_valid+0x10/0x10 ? mem_allocator_disconnect+0x73/0x150 ? __pfx_llist_ad console_unlock+0x193/0x1b0 ? lockdep_hardirqs_on+0xbe/0x140 ? __pfx___mutex_lock+0x10/0x10 ? tick_nohz_tick_stopped+0x16/0x90 ? __irq_work_queue_local+ irq_work_queue+0x39/0x50 ? __wake_up_klogd.part.0+0x79/0xc0 ? mem_allocator_disconnect+0x73/0x150 mem_allocator_disconnect+0x73/0x150 ? __pfx_mem_al mark_held_locks+0xa5/0xf0 ? rcu_is_watching+0x11/0xb0 page_pool_release+0x36e/0x6d0 page_pool_destroy+0xd7/0x440 xdp_unreg_mem_model+0x1a7/0x2a0 ? __pfx_xdp_unreg_mem_model+0x10/0x10 ? kfree+0x125/0x370 ? bnxt_free_ring.isra.0+0x2eb/0x500 ? bnxt_free_mem+0x5ac/0x2500 xdp_rxq_info_unreg+0x4a/0xd bnxt_free_mem+0x1356/0x2500 bnxt_close_nic+0xf0/0x3b0 ? __pfx_bnxt_close_nic+0x10/0x10 ? ethnl_parse_bit+0x2c6/0x6d0 ? __pfx___nla_validate_parse+0x10/(__pfx_ethnl_parse_bit+0x10/0x10 bnxt_set_features+0x2a8/0x3e0 __netdev_update_features+0x4dc/0x1370 ? ethnl_parse_bitset+0x4ff/0x750 ? __pfx_ethnl_parse_b __pfx___netdev_update_features+0x10/0x10 ? mark_held_locks+0xa5/0xf0 ? _raw_spin_unlock_irqrestore+0x42/0x70 ? __pm_runtime_resume+0x7d/0x110 ethnl_se this problem, it uses rhashtable_lookup_fast() instead of rhashtable_lookup() with rcu_read_lock(). Using xa without rcu_read_lock() here is safe. xa is freed by __xdp_ this is called by call_rcu() of mem_xa_remove(). The mem_xa_remove() is called by page_pool_destroy() if a reference count reaches 0. The xa is already protected by well in the control plane. So removing rcu_read_lock() for page_pool_destroy() is safe.
CVE-2024-43838	In the Linux kernel, the following vulnerability has been resolved: bpf: fix overflow check in adjust_jmp_off() adjust_jmp_off() incorrectly used the insn->imm field for all as that should only be done or the BPF_JMP32 | BPF_JA case, not the general jump instruction case. Fix it by using insn->off for overflow check in the general case.
CVE-2024-43821	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Fix a possible null pointer dereference In function lpfc_xcvr_data_show, the memory allocati thereby making rdp_context a null pointer. In the following context and functions that use this pointer, there are dereferencing operations, leading to null pointer derefer pointer check should be added. If it is null, use scnprintf to notify the user and return len.
CVE-2024-43833	In the Linux kernel, the following vulnerability has been resolved: media: v4l: async: Fix NULL pointer dereference in adding ancillary links In v4l2_async_create_ancilla created for lens and flash sub-devices. These are sub-device to sub-device links and if the async notifier is related to a V4L2 device, the source sub-device of the ancill NULL pointer dereference. Check the notifier's sd field is non-NULL in v4l2_async_create_ancillary_links(). [Sakari Ailus: Reword the subject and commit messages sli
CVE-2024-34135	Illustrator versions 28.5, 27.9.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could lever mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-43840	In the Linux kernel, the following vulnerability has been resolved: bpf, arm64: Fix trampoline for BPF_TRAMP_F_CALL_ORIG When BPF_TRAMP_F_CALL_ORIG is s __bpf_tramp_enter() and __bpf_tramp_exit() functions, passing them the struct bpf_tramp_image *im pointer as an argument in R0. The trampoline generation code us instructions for moving the bpf_tramp_image address into R0, but emit_addr_mov_i64() assumes the address to be in the vmalloc() space and uses only 48 bits. Becau using kzalloc(), its address can use more than 48-bits, in this case the trampoline will pass an invalid address to __bpf_tramp_enter/exit() causing a kernel crash. Fix th in place of emit_addr_mov_i64() as it can work with addresses that are greater than 48-bits.
CVE-2024-21806	Improper conditions check in Linux kernel mode driver for some Intel(R) Ethernet Network Controllers and Adapters E810 Series before version 28.3 may allow an auth enable denial of service via local access.
CVE-2024-43829	In the Linux kernel, the following vulnerability has been resolved: drm/qxl: Add check for drm_cvt_mode Add check for the return value of drm_cvt_mode() and return th NULL pointer dereference.
CVE-2024-34134	Illustrator versions 28.5, 27.9.4 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could lever mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-43828	In the Linux kernel, the following vulnerability has been resolved: ext4: fix infinite loop when replaying fast_commit When doing fast_commit replay an infinite loop may extent_status struct. ext4_ext_determine_insert_hole() does not detect the replay and calls ext4_es_find_extent_range(), which will return immediately without initializin contains garbage, an integer overflow may happen causing an infinite loop in this function, easily reproducible using fstest generic/039. This commit fixes this issue by structure in function ext4_es_find_extent_range(). Thanks to Zhang Yi, for figuring out the real problem!

CVE Number	Description
CVE-2024-43837	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix null pointer dereference in resolve_prog_type() for BPF_PROG_TYPE_EXT When loading a E `attr->attach_prog_fd`, the `prog->aux->dst_prog` will be null. At this time, calling resolve_prog_type() anywhere will result in a null pointer dereference. Example stack handle kernel NULL pointer dereference at virtual address 0000000000000004 [8.108262] Mem abort info: [8.108384] ESR = 0x0000000096000004 [8.108547] EC = 32 bits [8.108722] SET = 0, FnV = 0 [8.108827] EA = 0, S1PTW = 0 [8.108939] FSC = 0x04: level 0 translation fault [8.109102] Data abort info: [8.109203] ISV = 0, 0x00000000 [8.109399] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [8.109614] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [8.109836] user pgtable: 4k pages, 48-bit V 8.110011] [0000000000000004] pgd=0000000000000000, p4d=0000000000000000 [8.112624] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP [8.112 8.113120] CPU: 0 PID: 99 Comm: may_access_dire Not tainted 6.10.0-rc3-next-20240613-dirty #1 [8.113230] Hardware name: linux,dummy-virt (DT) [8.113390] psta UAO -TCO -DIT -SSBS BTYPE=--) [8.113429] pc : may_access_direct_pkt_data+0x24/0xa0 [8.113746] lr : add_subprog_and_kfunc+0x634/0x8e8 [8.113798] sp : ffff ffff80008283b9f0 x28: ffff800082795048 x27: 0000000000000001 [8.113881] x26: ffff0000c0bb2600 x25: 0000000000000000 x24: 0000000000000000 [8.113897] x2 0000000000001864f x21: ffff0000c1138000 [8.113912] x20: 0000000000000001 x19: ffff0000c12b8000 x18: ffffffffffffffff [8.113929] x17: 0000000000000000 x16: 0000 0720072007200720 [8.113944] x14: 0720072007200720 x13: 0720072007200720 x12: 0720072007200720 [8.113958] x11: 0720072007200720 x10: 0000000000f9 8.113991] x8 : 0101010101010101 x7 : 746f72705f6d656d x6 : 000000001e0e0f5f [8.114006] x5 : 0000000000001864f x4 : ffff0000c12b8000 x3 : 000000000000001c 0000000000000002 x1 : 0000000000000000 x0 : 0000000000000000 [8.114126] Call trace: [8.114159] may_access_direct_pkt_data+0x24/0xa0 [8.114202] bpf_che bpf_prog_load+0x658/0xa58 [8.114227] __sys_bpf+0xc50/0x2250 [8.114240] __arm64_sys_bpf+0x28/0x40 [8.114254] invoke_syscall.constprop.0+0x54/0xf0 [8.114 8.114289] el0_svc+0x3c/0x140 [8.114305] el0t_64_sync_handler+0x134/0x150 [8.114331] el0t_64_sync+0x168/0x170 [8.114477] Code: 7100707f 54000081 f9401c 8.118672] ---[end trace 0000000000000000]--- One way to fix it is by forcing `attach_prog_fd` non-empty when bpf_prog_load(). But this will lead to `libbpf_probe_bpf use verifier log to probe prog type and will log nothing if we reject invalid EXT prog before bpf_check(). Another way is by adding null check in resolve_prog_type(). The 4a9c7bbe2ed4 ("bpf: Resolve to prog->aux->dst_prog->type only for BPF_PROG_TYPE_EXT") which wanted to correct type resolution for BPF_PROG_TYPE_TRACI type resolution of BPF_PROG_TYPE_EXT prog actually follows the logic below: prog->aux->dst_prog ? prog->aux->dst_prog->type : prog->type; It implies that when E to `dst_prog`, the prog type should be EXT itself. This code worked fine in the past. So just keep using it. Fix this by returning `prog->type` for BPF_PROG_TYPE_EXT resolve_prog_type().
CVE-2024-34136	Illustrator versions 28.5, 27.9.4 and earlier are affected by a NULL Pointer Dereference vulnerability that could lead to an application denial-of-service (DoS). An attacke to crash the application, resulting in a denial of service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.
CVE-2024-43844	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: wow: fix GTK offload H2C skbuff issue We mistakenly put skb too large and that may exce skbuff: skb_over_panic: text:ffffffffc09e9a9d len:416 put:204 head:ffff8fba04eca780 data:ffff8fba04eca7e0 tail:0x200 end:0x140 dev:<NULL> ------------[cut here]-------- net/core/skbuff.c:192! invalid opcode: 0000 [#1] PREEMPT SMP PTI CPU: 1 PID: 4747 Comm: kworker/u4:44 Tainted: G O 6.6.30-02659-gc18865c4dfbd #1 86547039b47e46935493f615ee31d0b2d711d35e Hardware name: HP Meep/Meep, BIOS Google_Meep.11297.262.0 03/18/2021 Workqueue: events_unbound async 0010:skb_panic+0x5d/0x60 Code: c6 63 8b 8f bb 4c 0f 45 f6 48 c7 c7 4d 89 8b bb 48 89 ce 44 89 d1 41 56 53 41 53 ff b0 c8 00 00 00 e8 27 5f 23 00 48 83 c4 20 <0f> 90 90 90 90 90 90 90 90 0f 1f 44 RSP: 0018:ffffaa700144bad0 EFLAGS: 00010282 RAX: 0000000000000089 RBX: 0000000000000140 RCX: 14432c5aad26c900 RD 00000000ffffdfff RDI: 0000000000000001 RBP: ffffaa700144bae0 R08: 0000000000000000 R09: ffffaa700144b920 R10: 00000000ffffdfff R11: ffffffffbc28fbc0 R12: ffff8 0000000000000000 R14: ffffffffbb8f8b63 R15: 0000000000000000 FS: 0000000000000000(0000) GS:ffff8fba7bd00000(0000) knlGS:0000000000000000 CS: 0010 DS 0000000080050033 CR2: 00007999c4ad1000 CR3: 000000015503a000 CR4: 0000000000350ee0 Call Trace: <TASK> ? __die_body+0x1f/0x70 ? die+0x3d/0x60 ? d skb_panic+0x5d/0x60 ? do_error_trap+0x6d/0x90 ? skb_panic+0x5d/0x60 ? handle_invalid_op+0x30/0x40 ? skb_panic+0x5d/0x60 ? exc_invalid_op+0x3c/0x50 ? asm skb_panic+0x5d/0x60 skb_put+0x49/0x50 rtw89_fw_h2c_wow_gtk_ofld+0xbd/0x220 [rtw89_core 778b32de31cd1f14df2d6721ae99ba8a83636fa5] rtw89_wow_resume 778b32de31cd1f14df2d6721ae99ba8a83636fa5] rtw89_ops_resume+0x2b/0xa0 [rtw89_core 778b32de31cd1f14df2d6721ae99ba8a83636fa5] ieee80211_reconfig+0x 818a894e3b77da6298269c59ed7cdff065a4ed52] ? __pfx_wiphy_resume+0x10/0x10 [cfg80211 1a793119e2aeb157c4ca4091ff8e1d9ae233b59d] ? dev_printk_emit+0 ? __pfx_wiphy_resume+0x10/0x10 [cfg80211 1a793119e2aeb157c4ca4091ff8e1d9ae233b59d] wiphy_resume+0x89/0x180 [cfg80211 1a793119e2aeb157c4ca4091ff8 __pfx_wiphy_resume+0x10/0x10 [cfg80211 1a793119e2aeb157c4ca4091ff8e1d9ae233b59d] dpm_run_callback+0x3c/0x140 device_resume+0x1f9/0x3c0 ? __pfx_dp async_resume+0x1d/0x30 async_run_entry_fn+0x29/0xd0 process_scheduled_works+0x1d8/0x3d0 worker_thread+0x1fc/0x2f0 kthread+0xed/0x110 ? __pfx_worker_t __pfx_kthread+0x10/0x10 ret_from_fork+0x38/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1b/0x30 </TASK> Modules linked in: ccm 8021q r8153_ecm cd dm_integrity async_xor xor async_tx lz4 lz4_compress zstd zstd_compress zram zsmalloc uinput rfcomm cmac algif_hash rtw89_8922ae(O) algif_skcipher rtw89_8922 rtw89_core(O) btusb(O) snd_soc_sst_bxt_da7219_max98357a btbcm(O) snd_soc_hdac_hdmi btintel(O) snd_soc_intel_hda_dsp_common snd_sof_probes btrtl(O) btn snd_soc_dmic uvcvideo videobuf2_vmalloc uvc videobuf2_memops videobuf2_v4l2 videobuf2_common snd_sof_pci_intel_apl snd_sof_intel_hda_common snd_soc_h soundwire_intel soundwire_generic_allocation snd_sof_intel_hda_mlink soundwire_cadence snd_sof_pci snd_sof_xtensa_dsp mac80211 snd_soc_acpi_intel_match s snd_sof_utils soundwire_bus snd_soc_max98357a snd_soc_avs snd_soc_hda_codec snd_hda_ext_core snd_intel_dspcfg snd_intel_sdw_acpi snd_soc_da7219 snd_ snd_hda_core veth ip6table_nat xt_MASQUERADE xt_cgroup fuse bluetooth ecdh_generic cfg80211 ecc gsmi: Log Shutdown ---truncated---
CVE-2024-43824	In the Linux kernel, the following vulnerability has been resolved: PCI: endpoint: pci-epf-test: Make use of cached 'epc_features' in pci_epf_test_core_init() Instead of g pci_epc_get_features() API, use the cached pci_epf_test::epc_features value to avoid the NULL check. Since the NULL check is already performed in pci_epf_test_bin pci_epf_test_core_init() is redundant and it is not possible to hit the NULL pointer dereference. Also with commit a01e7214bef9 ("PCI: endpoint: Remove "core_init_not dereferenced without the NULL check, leading to the following false positive Smatch warning: drivers/pci/endpoint/functions/pci-epf-test.c:784 pci_epf_test_core_init() e 'epc_features' could be null (see line 747) Thus, remove the redundant NULL check and also use the epc_features:: {msix_capable/msi_capable} flags directly to avoid commit log]
CVE-2024-43823	In the Linux kernel, the following vulnerability has been resolved: PCI: keystone: Fix NULL pointer dereference in case of DT error in ks_pcie_setup_rc_app_regs() If IC provided in Device Tree due to any error, resource_list_first_type() will return NULL and pci_parse_request_of_pci_ranges() will just emit a warning. This will cause a N bug by adding NULL return check. Found by Linux Verification Center (linuxtesting.org) with SVACE.
CVE-2024-43846	In the Linux kernel, the following vulnerability has been resolved: lib: objagg: Fix general protection fault The library supports aggregation of objects into other objects o have a parent itself. That is, nesting is not supported. Aggregation happens in two cases: Without and with hints, where hints are a pre-computed recommendation on h objects. Nesting is not possible in the first case due to a check that prevents it, but in the second case there is no check because the assumption is that nesting cannot based on hints. The violation of this assumption leads to various warnings and eventually to a general protection fault [1]. Before fixing the root cause, error out when n general protection fault, probably for non-canonical address 0xdead000000000d90: 0000 [#1] PREEMPT SMP PTI CPU: 1 PID: 1083 Comm: kworker/1:9 Tainted: G W gd9b4f1cca7fb #7 Hardware name: Mellanox Technologies Ltd. MSN3700/VMOD0005, BIOS 5.11 01/06/2019 Workqueue: mlxsw_core mlxsw_sp_acl_tcam_vregion_r 0010:mlxsw_sp_acl_erp_bf_insert+0x25/0x80 [...] Call Trace: <TASK> mlxsw_sp_acl_atcam_entry_add+0x256/0x3c0 mlxsw_sp_acl_tcam_entry_create+0x5e/0xa0 mlxsw_sp_acl_tcam_vchunk_migrate_one+0x16b/0x270 mlxsw_sp_acl_tcam_vregion_rehash_work+0xbe/0x510 process_one_work+0x151/0x370 worker_thread+0x2 ret_from_fork+0x34/0x50 ret_from_fork_asm+0x1a/0x30 </TASK>
CVE-2024-43848	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix TTLM teardown work The worker calculates the wrong sdata pointer, so if it ever ru

CVE Number	Description
CVE-2024-43822	In the Linux kernel, the following vulnerability has been resolved: ASoc: PCM6240: Return directly after a failed devm_kzalloc() in pcmdevice_i2c_probe() The value “-E local variable “ret” in one if branch after a devm_kzalloc() call failed at the beginning. This error code will trigger then a pcmdevice_remove() call with a passed null poin dereference will be performed. Thus return the appropriate error code directly.
CVE-2024-43849	In the Linux kernel, the following vulnerability has been resolved: soc: qcom: pdr: protect locator_addr with the main mutex If the service locator server is restarted fast locator_addr fields concurrently. Protect them by placing modification of those fields under the main pdr->lock.
CVE-2024-43266	Authorization Bypass Through User-Controlled Key vulnerability in WP Job Portal.This issue affects WP Job Portal: from n/a through 2.1.6.
CVE-2024-42486	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. In versions on the 1.15.x branch prior to 1.15.8 and the 1.16.x branch prior to changes are not correctly propagated in Cilium's GatewayAPI controller, which could lead to Gateway resources being able to access secrets for longer than intended, forward traffic to backends in other namespaces for longer than intended. This issue has been patched in Cilium v1.15.8 and v1.16.1. As a workaround, any modificatio Gateway/HTTPRoute/GRPCRoute/TCPRoute CRD (for example, adding any label to any of these resources) will trigger a reconciliation of ReferenceGrants on an affe
CVE-2024-5941	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to unauthorized access and deletion of data due to a missing capability ch function in all versions up to, and including, 3.14.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to read attachment path
CVE-2024-43322	Authorization Bypass Through User-Controlled Key vulnerability in Dylan James Zephyr Project Manager.This issue affects Zephyr Project Manager: from n/a through 3
CVE-2024-43275	Cross-Site Request Forgery (CSRF) vulnerability in xyzscripts.Com Insert PHP Code Snippet.This issue affects Insert PHP Code Snippet: from n/a through 1.3.6.
CVE-2024-43396	Khoj is an application that creates personal AI agents. The Automation feature allows a user to insert arbitrary HTML inside the task instructions, resulting in a Stored X /api/automation endpoint does not get correctly sanitized when rendered on the page, resulting in the ability of users to inject arbitrary HTML/JS. This vulnerability is fix
CVE-2024-42335	7Twenty - CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
CVE-2024-25582	Module savepoints could be abused to inject references to malicious code delivered through the same domain. Attackers could perform malicious API requests or extra account. Exploiting this vulnerability requires temporary access to an account or successful social engineering to make a user follow a prepared link to a malicious acco updates and patch releases. The savepoint module path has been restricted to modules that provide the feature, excluding any arbitrary or non-existing modules. No pu known.
CVE-2024-43326	Missing Authorization vulnerability in Jamie Bergen Plugin Notes Plus allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Plugin Notes
CVE-2023-3409	The Bricks theme for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.8.1. This is due to missing or incorrect nonce validation This makes it possible for unauthenticated attackers to reset the theme's settings via a forged request granted they can trick a site administrator into performing an acti
CVE-2024-39094	Friendica 2024.03 is vulnerable to Cross Site Scripting (XSS) in settings/profile via the homepage, xmpp, and matrix parameters.
CVE-2024-43006	A stored cross-site scripting (XSS) vulnerability exists in ZZCMS2023 in the ask/show.php file at line 21. An attacker can exploit this vulnerability by sending a specially /user/ask_edit.php?action=add, which includes malicious JavaScript code in the 'content' parameter. When a user visits the ask/show_{newsid}.html page, the injected of the user's browser, leading to potential theft of cookies, session tokens, or other sensitive information.
CVE-2024-42758	A Cross-site Scripting (XSS) vulnerability exists in version v2024-01-05 of the indexmenu plugin when is used and enabled in Dokuwiki (Open Source Wiki Engine). A r payloads for example when creating or editing existing page, to trigger the XSS on Dokuwiki, which is then stored in .txt file (due to nature of how Dokuwiki is designed)
CVE-2024-43377	Umbraco CMS is an ASP.NET CMS. An authenticated user can access a few unintended endpoints. This issue is fixed in 14.1.2.
CVE-2024-25837	A stored cross-site scripting (XSS) vulnerability in October CMS Bloghub Plugin v1.3.8 and lower allows attackers to execute arbitrary web scripts or HTML via a crafte section.
CVE-2024-39418	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security featur attacker could leverage this vulnerability to bypass security measures to view and edit low-sensitivity information. Exploitation of this issue does not require user interac
CVE-2024-25633	eLabFTW is an open source electronic lab notebook for research labs. In an eLabFTW system, one can configure who is allowed to create new user accounts. A vulne version 4.4.0 and prior to version 5.0.0 that allows regular users to create new, validated accounts in their team. If the system has anonymous access enabled (disable user can create regular users in any team. This vulnerability has been fixed since version 5.0.0, released on February 17th 2024. Some workarounds are available. Dis *administrators* to create users will provide a mitigation. Additionally, disabling anonymous user access will stop anonymous access (including using existing access ke

CVE Number	Description
CVE-2024-43281	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in VOID CODERS Void Elementor Post Grid Addon for Elementor Page builc Inclusion.This issue affects Void Elementor Post Grid Addon for Elementor Page builder: from n/a through 2.3.
CVE-2024-43272	Missing Authentication for Critical Function vulnerability in icegram Icegram allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Icegra
CVE-2024-7753	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been declared as problematic. This vulnerability affects unknown code of tl manipulation leads to direct request. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7929	A vulnerability, which was classified as problematic, was found in SourceCodester Simple Forum Website 1.0. This affects an unknown part of the file /registration.php The manipulation of the argument username leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and m
CVE-2024-7924	A vulnerability was found in ZZCMS 2023. It has been declared as critical. This vulnerability affects unknown code of the file /l/list.php. The manipulation of the argume The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7919	A vulnerability, which was classified as critical, has been found in Anhui Deshun Intelligent Technology Jieshun JieLink+ JSOTC2016 up to 20240805. This issue affect the file /report/ParkChargeRecord/GetDataList. The manipulation leads to improper access controls. The attack may be initiated remotely. The exploit has been disclos used.
CVE-2024-35538	Typecho v1.3.0 was discovered to contain a Client IP Spoofing vulnerability, which allows attackers to falsify their IP addresses by specifying an arbitrary IP as value of headers while performing HTTP requests.
CVE-2024-43380	fugit contains time tools for flor and the floraison group. The fugit "natural" parser, that turns "every wednesday at 5pm" into "0 17 * * 3", accepted any length of input ar not returning promptly, as expected. The parse call could hold the thread with no end in sight. Fugit dependents that do not check (user) input length for plausibility are fugit 1.11.1.
CVE-2024-5939	The GiveWP – Donation Plugin and Fundraising Platform plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the 's versions up to, and including, 3.13.0. This makes it possible for unauthenticated attackers to read the setup wizard administrative pages.
CVE-2024-7411	The Newsletters plugin for WordPress is vulnerable to Full Path Disclosure in all versions up to, and including, 4.9.9. This is due the plugin not preventing direct access /vendor/mobiledetect/mobiledetectlib/export/exportToJSON.php. This makes it possible for unauthenticated attackers to retrieve the full path of the web application, whi attacks. The information displayed is not useful on its own, and requires another vulnerability to be present for damage to an affected website.
CVE-2023-4027	The Radio Player plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the update_settings function in versions makes it possible for unauthenticated attackers to update plugin settings.
CVE-2024-35136	IBM Db2 for Linux, UNIX and Windows (includes DB2 Connect Server) federated server 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted q conditions. IBM X-Force ID: 291307.
CVE-2023-4025	The Radio Player plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the update_player function in versions up makes it possible for unauthenticated attackers to update player instances.
CVE-2023-4024	The Radio Player plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the delete_player function in versions up makes it possible for unauthenticated attackers to delete player instances.
CVE-2024-6098	When performing an online tag generation to devices which communicate using the ControlLogix protocol, a machine-in-the-middle, or a device that is not configured c leading to unrestricted or unregulated resource allocation. This could cause a denial-of-service condition and crash the Kepware application. By default, these functions accessible for users who recognize and require their advantages.
CVE-2024-7630	The Relevanssi – A Better Search plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 4.22.2 via the relevanssi_do_query() the posts that are returned when searching. This makes it possible for unauthenticated attackers to extract potentially sensitive information from password protected po
CVE-2024-7843	A vulnerability, which was classified as problematic, was found in SourceCodester Online Graduate Tracer System 1.0. Affected is an unknown function of the file /trac manipulation leads to information disclosure. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-37028	BIG-IP Next Central Manager may allow an attacker to lock out an account that has never been logged in. Note: Software versions which have reached End of Technic evaluated.

CVE Number	Description
CVE-2024-7842	A vulnerability, which was classified as problematic, has been found in SourceCodester Online Graduate Tracer System 1.0. This issue affects some unknown processi /tracking/admin/export_it.php. The manipulation leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed to the public and r
CVE-2023-50315	IBM WebSphere Application Server 8.5 and 9.0 could allow an attacker with access to the network to conduct spoofing attacks. An attacker could exploit this vulnerabil trusted authority to obtain sensitive information. IBM X-Force ID: 274714.
CVE-2023-50314	IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.8 could allow an attacker with access to the network to conduct spoofing attacks. An attacker could certificate issued by a trusted authority to obtain sensitive information. IBM X-Force ID: 274713.
CVE-2024-35686	Missing Authorization vulnerability in Automattic Sensei LMS, Automattic Sensei Pro (WC Paid Courses).This issue affects Sensei LMS: from n/a through 4.23.1; Sense n/a through 4.23.1.1.23.1.
CVE-2024-31882	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to a denial of service, under specific non default configurations, as th a specially crafted SQL statement by an authenticated user. IBM X-Force ID: 287614.
CVE-2023-4730	The LadiApp plugn for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the init_endpoint() function hooked via 'init' in 4.3. This makes it possible for unauthenticated attackers to modify a variety of settings. An attacker can directly modify the 'ladipage_key' which enables them to create inject malicious web scripts.
CVE-2024-7912	A vulnerability was found in CodeAstro Online Railway Reservation System 1.0. It has been declared as problematic. This vulnerability affects unknown code of the file manipulation leads to exposure of information through directory listing. The attack can be initiated remotely. The exploit has been disclosed to the public and may be us
CVE-2024-43350	Authorization Bypass Through User-Controlled Key vulnerability in Propovoice Propovoice CRM.This issue affects Propovoice CRM: from n/a through 1.7.6.4.
CVE-2024-7809	A vulnerability was found in SourceCodester Online Graduate Tracer System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown func /tracking/nbproject/. The manipulation leads to exposure of information through directory listing. The attack can be launched remotely. The exploit has been disclosed t
CVE-2024-7813	A vulnerability, which was classified as problematic, has been found in SourceCodester Prison Management System 1.0. This issue affects some unknown processing of the component Profile Image Handler. The manipulation leads to insufficiently protected credentials. The attack may be initiated remotely. The exploit has been discl used.
CVE-2024-7799	A vulnerability was found in SourceCodester Simple Online Bidding System 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the system/bidding/admin/users.php. The manipulation leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed to the public
CVE-2024-28050	Improper access control in some Intel(R) Arc(TM) & Iris(R) Xe Graphics software before version 31.0.101.4824 may allow an authenticated user to potentially enable d
CVE-2024-43381	reNgine is an automated reconnaissance framework for web applications. Versions 2.1.2 and prior are susceptible to Stored Cross-Site Scripting (XSS) attacks. This vu a domain, and if the target domain's DNS record contains an XSS payload, it leads to the execution of malicious scripts in the reNgine's dashboard view when any user payload is directly fetched from the DNS record of the remote target domain. Consequently, an attacker can execute the attack without requiring any additional input fro A patch is available and expected to be part of version 2.1.3.
CVE-2024-39824	Sensitive information disclosure in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow a privileged user to conduct an information d
CVE-2024-39823	Sensitive information disclosure in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow a privileged user to conduct an information d
CVE-2024-43011	An arbitrary file deletion vulnerability exists in the admin/del.php file at line 62 in ZZCMS 2023 and earlier. Due to insufficient validation and sanitization of user input for exploit this vulnerability by using directory traversal techniques to delete arbitrary files on the server. This can lead to the deletion of critical files, potentially disrupting th system.
CVE-2024-42434	Sensitive information disclosure in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow a privileged user to conduct an information d
CVE-2024-42435	Sensitive information disclosure in some Zoom Workplace Apps, SDKs, Rooms Clients, and Rooms Controllers may allow a privileged user to conduct an information d
CVE-2024-40704	IBM InfoSphere Information Server 11.7 could allow a privileged user to obtain sensitive information from authentication request headers. IBM X-Force ID: 298277.

CVE Number	Description
CVE-2024-43280	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Salon Booking System Salon booking system.This issue affects Salon booking system: from n/a thr
CVE-2024-7917	A vulnerability, which was classified as critical, has been found in DouPHP 1.7 Release 20220822. Affected by this issue is some unknown functionality of the file /admi Favicon Handler. The manipulation of the argument site_favicon leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to
CVE-2024-43005	A reflected cross-site scripting (XSS) vulnerability in the component dl_liuyan_save.php of ZZCMS v2023 allows attackers to execute arbitrary code in the context of a u crafted payload.
CVE-2024-42287	In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Complete command early within lock A crash was observed while performing NPIV and pointer dereference, address: 000000000000001c #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 RIP: 0010:dma_direct_unmap_sg+0x51/0x1e0 RSP: 0018:ffffc90026f47b88 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 0000000000000021 RCX: 00000000 0000000000000021 RSI: 0000000000000000 RDI: ffff8881041130d0 RBP: ffff8881041130d0 R08: 0000000000000000 R09: 0000000000000034 R10: ffffc90026f47c4 0000000000000000 R13: 0000000000000000 R14: ffff8881565e4a20 R15: 0000000000000000 FS: 00007f4c69ed3d00(0000) GS:ffff889faac80000(0000) knlGS:0000 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000001c CR3: 0000000288a50002 CR4: 00000000007706e0 DR0: 0000000000000000 DR1: 00000000000 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? __die_body+0x1a/0x60 ? pag do_user_addr_fault+0x174/0x7f0 ? exc_page_fault+0x69/0x1a0 ? asm_exc_page_fault+0x22/0x30 ? dma_direct_unmap_sg+0x51/0x1e0 ? preempt_count_sub+0x96/ qla2xxx_qpair_sp_free_dma+0x29f/0x3b0 [qla2xxx] qla2xxx_qpair_sp_compl+0x60/0x80 [qla2xxx] __qla2x00_abort_all_cmds+0xa2/0x450 [qla2xxx] The command co aborting the commands in driver unload path but outside lock to avoid the WARN_ON condition of performing dma_free_attr within the lock. However this caused race completion via multiple paths causing system crash. Hence complete the command early in unload path but within the lock to avoid race condition.
CVE-2024-43236	URL Redirection to Untrusted Site ('Open Redirect') vulnerability in Scott Paterson Easy PayPal Buy Now Button.This issue affects Easy PayPal Buy Now Button: from
CVE-2024-43009	A reflected cross-site scripting (XSS) vulnerability exists in user/login.php at line 24 in ZZCMS 2023 and earlier. The application directly inserts the value of the HTTP_F response without proper sanitization. An attacker can exploit this vulnerability by tricking a user into visiting a specially crafted URL, which includes a malicious Referer execution of arbitrary JavaScript code in the context of the victim's browser, potentially resulting in session hijacking, defacement, or other malicious activities.
CVE-2023-1604	The Short URL plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.6.8. This is due to missing or incorrect nonce valida function. This makes it possible for unauthenticated attackers to add and import redirects, including comments containing cross-site scripting as detailed in CVE-2023-1 administrator into performing an action such as clicking on a link.
CVE-2024-7899	A vulnerability, which was classified as critical, has been found in InnoCMS 0.3.1. This issue affects some unknown processing of the file /panel/pages/1/edit of the com manipulation leads to code injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. NOTE: The vendor was conta but did not respond in any way.
CVE-2024-7910	A vulnerability was found in CodeAstro Online Railway Reservation System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file the component Profile Photo Update Handler. The manipulation leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to t
CVE-2024-7347	NGINX Open Source and NGINX Plus have a vulnerability in the ngx_http_mp4_module, which might allow an attacker to over-read NGINX worker memory resulting ir crafted mp4 file. The issue only affects NGINX if it is built with the ngx_http_mp4_module and the mp4 directive is used in the configuration file. Additionally, the attack trigger the processing of a specially crafted mp4 file with the ngx_http_mp4_module. Note: Software versions which have reached End of Technical Support (EoTS) ar
CVE-2024-31799	Information Disclosure in GNCC's GC2 Indoor Security Camera 1080P allows an attacker with physical access to read the WiFi passphrase via the UART Debugging F
CVE-2024-43807	In JetBrains TeamCity before 2024.07.1 multiple stored XSS was possible on Clouds page
CVE-2024-43810	In JetBrains TeamCity before 2024.07.1 reflected XSS was possible in the AWS Core plugin
CVE-2024-43374	The UNIX editor Vim prior to version 9.1.0678 has a use-after-free error in argument list handling. When adding a new file to the argument list, this triggers `Buf*` autoc autocommand the buffer that was just opened is closed (including the window where it is shown), this causes the window structure to be freed which contains a referen are actually modifying. Once the autocommands are completed, the references to the window and argument list are no longer valid and as such cause an use-after-free must either intentionally add some unusual autocommands that wipe a buffer during creation (either manually or by sourcing a malicious plugin), but it will crash Vim. Th Vim patch v9.1.0678.
CVE-2023-34424	Improper input validation in firmware for some Intel(R) CSME may allow a privileged user to potentially enable denial of service via local access.
CVE-2022-3399	The Cookie Notice & Compliance for GDPR / CCPA plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'cookie_notice_options[refuse_code_head and including, 2.4.17.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrative privileges and al scripts in pages that will execute whenever a user accesses the injected /wp-admin/admin.php?page=cookie-notice page. This only affects multi-site installations and ir has been disabled.

CVE Number	Description
CVE-2024-6322	Access control for plugin data sources protected by the ReqActions json field of the plugin.json is bypassed if the user or service account is granted associated access ReqActions check was not scoped to each specific datasource. The account must have prior query access to the impacted datasource.
CVE-2024-41699	Priority – CWE-552: Files or Directories Accessible to External Parties
CVE-2024-5916	An information exposure vulnerability in Palo Alto Networks PAN-OS software enables a local system administrator to unintentionally disclose secrets, passwords, and read-only administrator who has access to the config log, can read secrets, passwords, and tokens to external systems.
CVE-2024-21844	Integer overflow in firmware for some Intel(R) CSME may allow an unauthenticated user to potentially enable denial of service via adjacent access.
CVE-2024-41723	Undisclosed requests to BIG-IP iControl REST can lead to information leak of user account names. Note: Software versions which have reached End of Technical Sup
CVE-2024-41698	Priority – CWE-200: Exposure of Sensitive Information to an Unauthorized Actor
CVE-2024-38808	In Spring Framework versions 5.3.0 - 5.3.38 and older unsupported versions, it is possible for a user to provide a specially crafted Spring Expression Language (SpEL) denial of service (DoS) condition. Specifically, an application is vulnerable when the following is true: * The application evaluates user-supplied SpEL expressions.
CVE-2024-7063	The ElementsKit Pro plugin for WordPress is vulnerable to Sensitive Information Exposure in all versions up to, and including, 3.6.6 via the 'render_raw' function. This c with Contributor-level permissions and above, to extract sensitive data including private, future, and draft posts.
CVE-2024-7422	The Theme My Login plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 7.1.7. This is due to missing or incorrect no tml_admin_save_ms_settings() function. This makes it possible for unauthenticated attackers to update the theme's settings via a forged request granted they can trick performing an action such as clicking on a link. Please note that this only affects multi-site instances.
CVE-2024-7711	An Incorrect Authorization vulnerability was identified in GitHub Enterprise Server, allowing an attacker to update the title, assignees, and labels of any issue inside a pu exploitable inside a public repository. This vulnerability affected GitHub Enterprise Server versions before 3.14 and was fixed in versions 3.13.3, 3.12.8, and 3.11.14. Ve Server are not affected. This vulnerability was reported via the GitHub Bug Bounty program.
CVE-2023-7049	The Custom Field For WP Job Manager plugin for WordPress is vulnerable to Insecure Direct Object Reference in all versions up to, and including, 1.2 via the the 'cm_ missing validation on the 'job_id' user controlled key. This makes it possible for authenticated attackers, with contributor-level access and above, to expose potentially s
CVE-2024-39410	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an atta and perform minor integrity changes on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a mali issue does not require user interaction.
CVE-2024-43397	Apollo is a configuration management system. A vulnerability exists in the synchronization configuration feature that allows users to craft specific requests to bypass pe enables them to modify a namespace without the necessary permissions. The issue was addressed with an input parameter check which was released in version 2.3.0
CVE-2024-43376	Umbraco is an ASP.NET CMS. Some endpoints in the Management API can return stack trace information, even when Umbraco is not in debug mode. This vulnerabili
CVE-2024-39404	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security featur attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.
CVE-2024-39405	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security featur attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.
CVE-2024-39407	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security featur attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.
CVE-2024-39408	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an atta and perform minor integrity changeson behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a mali issue requires user interaction.
CVE-2024-39409	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by a Cross-Site Request Forgery (CSRF) vulnerability that could allow an atta and perform minor integrity changes on behalf of a user. The vulnerability could be exploited by tricking a victim into clicking a link or loading a page that submits a mali issue requires user interaction.

CVE Number	Description
CVE-2024-39411	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security featur attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.
CVE-2023-35123	Uncaught exception in OpenBMC Firmware for some Intel(R) Server Platforms before versions egs-1.14-0, bhs-0.27 may allow an authenticated user to potentially ena access.
CVE-2024-39412	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security featur attacker could leverage this vulnerability to bypass security measures and perform a minor integrity change. Exploitation of this issue does not require user interaction.
CVE-2023-3408	The Bricks theme for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.8.1. This is due to missing or incorrect nonce validation This makes it possible for unauthenticated attackers to modify the theme's settings, including enabling a setting which allows lower-privileged users such as contributor a forged request granted they can trick a site administrator into performing an action such as clicking on a link.
CVE-2024-39414	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security featur attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.
CVE-2024-39415	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security featur attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.
CVE-2024-39416	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security featur attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.
CVE-2024-39417	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security featur attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.
CVE-2024-39419	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security featur attacker could leverage this vulnerability to bypass security measures and modify minor information. Exploitation of this issue does not require user interaction.
CVE-2024-39413	Adobe Commerce versions 2.4.7-p1, 2.4.6-p6, 2.4.5-p8, 2.4.4-p9 and earlier are affected by an Improper Authorization vulnerability that could result in a Security featur attacker could leverage this vulnerability to bypass security measures and disclose minor information. Exploitation of this issue does not require user interaction.
CVE-2024-7920	A vulnerability, which was classified as problematic, was found in Anhui Deshun Intelligent Technology Jieshun JieLink+ JSOTC2016 up to 20240805. Affected is an ur /Report/ParkCommon/GetParkInThroughDeivces. The manipulation leads to improper access controls. It is possible to launch the attack remotely. The exploit has beer be used.
CVE-2024-7925	A vulnerability was found in ZZCMS 2023. It has been rated as problematic. This issue affects some unknown processing of the file 3/E_bak5.1/upload/eginfo.php. The phome with the input ShowPHPInfo leads to information disclosure. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used
CVE-2024-43288	Authorization Bypass Through User-Controlled Key vulnerability in gVectors Team wpForo Forum.This issue affects wpForo Forum: from n/a through 2.3.4.
CVE-2024-7902	A vulnerability was found in pkp ojs up to 3.4.0-6 and classified as problematic. Affected by this issue is some unknown functionality of the file /login/signOut. The manip with the input .example.com leads to open redirect. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOTE: The v this disclosure but did not respond in any way.
CVE-2024-7928	A vulnerability, which was classified as problematic, has been found in FastAdmin up to 1.3.3.20220121. Affected by this issue is some unknown functionality of the file manipulation of the argument lang leads to path traversal. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgra able to address this issue. It is recommended to upgrade the affected component.
CVE-2024-43239	Authorization Bypass Through User-Controlled Key vulnerability in Masteriyo Masteriyo - LMS.This issue affects Masteriyo - LMS: from n/a through 1.11.4.
CVE-2024-43317	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Metagauss User Registration Team RegistrationMagic allow (XSS).This issue affects RegistrationMagic: from n/a through 6.0.1.0.
CVE-2024-7921	A vulnerability has been found in Anhui Deshun Intelligent Technology Jieshun JieLink+ JSOTC2016 up to 20240805 and classified as problematic. Affected by this vul functionality of the file /report/ParkOutRecord/GetDataList. The manipulation leads to improper access controls. The attack can be launched remotely. The exploit has b may be used.
CVE-2024-7501	The Download Plugins and Themes in ZIP from Dashboard plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.8.7. incorrect nonce validation on the download_theme() function. This makes it possible for unauthenticated attackers to download arbitrary themes from the website via a trick a site administrator into performing an action such as clicking on a link. In versions prior to 1.8.6 it was possible to download the entire sites files.

CVE Number	Description
CVE-2024-41719	When generating QKView of BIG-IP Next instance from the BIG-IP Next Central Manager (CM), F5 iHealth credentials will be logged in the BIG-IP Central Manager log which have reached End of Technical Support (EoTS) are not evaluated.
CVE-2024-6534	Directus v10.13.0 allows an authenticated external attacker to modify presets created by the same user to assign them to another user. This is possible because the ap parameter in the 'POST /presets' request but not in the PATCH request. When chained with CVE-2024-6533, it could result in account takeover.
CVE-2024-6533	Directus v10.13.0 allows an authenticated external attacker to execute arbitrary JavaScript on the client. This is possible because the application injects an attacker-cor stored in the server and used by the client into an unsanitized DOM element. When chained with CVE-2024-6534, it could result in account takeover.
CVE-2024-42369	matrix-js-sdk is a Matrix messaging protocol Client-Server SDK for JavaScript. A malicious homeserver can craft a room or room structure such that the predecessors f getRoomUpgradeHistory function will infinitely recurse in this case, causing the code to hang. This method is public but also called by the 'leaveRoomChain()' method, the bug. This was patched in matrix-js-sdk 34.3.1.
CVE-2024-42487	Cilium is a networking, observability, and security solution with an eBPF-based dataplane. In the 1.15 branch prior to 1.15.8 and the 1.16 branch prior to 1.16.1, Gatewa GRPCRoutes do not follow the match precedence specified in the Gateway API specification. In particular, request headers are matched before request methods, wher the request methods must be respected before headers are matched. This could result in unexpected behaviour with security This issue is fixed in Cilium v1.15.8 and v for this issue.
CVE-2024-43808	In JetBrains TeamCity before 2024.07.1 self XSS was possible in the HashiCorp Vault plugin
CVE-2024-7793	A vulnerability was found in SourceCodester Task Progress Tracker 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown functionality c The manipulation of the argument task_name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may
CVE-2024-43809	In JetBrains TeamCity before 2024.07.1 reflected XSS was possible on the agentPushPreset page
CVE-2024-7844	A vulnerability has been found in SourceCodester Online Graduate Tracer System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functio /tracking/admin/add_acc.php. The manipulation of the argument name/user/position leads to cross site scripting. The attack can be launched remotely. The exploit has may be used.
CVE-2024-7852	A vulnerability was found in SourceCodester Yoga Class Registration System 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/inquiries/view_inquiry.php. The manipulation of the argument message leads to cross site scripting. The attack may be initiated remotely. The exploit has been d be used.
CVE-2024-7901	A vulnerability has been found in Scada-LTS 2.7.8 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /Scada-LTS/app.sh component Message Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and ma planned for the upcoming release at the end of September 2024.
CVE-2024-8003	A vulnerability was found in Go-Tribe gotribe-admin 1.0 and classified as problematic. Affected by this issue is the function InitRoutes of the file internal/app/routes/rout Handler. The manipulation leads to deserialization. The patch is identified as 45ac90d6d1f82716f77dbcdf8e7309c229080e3c. It is recommended to apply a patch to fix
CVE-2024-7942	A vulnerability has been found in SourceCodester Leads Manager Tool 1.0 and classified as problematic. This vulnerability affects unknown code of the file update-lead argument phone_number leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.
CVE-2024-7812	A vulnerability classified as problematic was found in SourceCodester Best House Rental Management System 1.0. This vulnerability affects unknown code of the file /r action=save_tenant of the component POST Parameter Handler. The manipulation of the argument lastname leads to cross site scripting. The attack can be initiated re disclosed to the public and may be used.
CVE-2024-7914	A vulnerability classified as problematic has been found in SourceCodester Yoga Class Registration System 1.0. Affected is an unknown function of the file /php-ycrs/cl manipulation of the argument address leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be
CVE-2024-7945	A vulnerability was found in itsourcecode Laravel Property Management System 1.0. It has been declared as problematic. Affected by this vulnerability is an unknown fu /admin/notes/create of the component Notes Page. The manipulation of the argument Note text leads to cross site scripting. The attack can be launched remotely. The public and may be used.
CVE-2024-7752	A vulnerability was found in SourceCodester Clinics Patient Management System 1.0. It has been classified as problematic. This affects an unknown part of the file /up manipulation of the argument medicine_name leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and
CVE-2024-7948	A vulnerability classified as problematic was found in SourceCodester Accounts Manager App 1.0. This vulnerability affects unknown code of the file update-account.ph Account Page. The manipulation of the argument Account Name/Username/Password/Link leads to cross site scripting. The attack can be initiated remotely. The explo public and may be used.
CVE-2024-7916	A vulnerability classified as problematic was found in nafisulbari/itsourcecode Insurance Management System 1.0. Affected by this vulnerability is an unknown functiona of the component Add Nominee Page. The manipulation of the argument Nominee-Client ID leads to cross site scripting. The attack can be launched remotely. The exp public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.

CVE Number	Description
CVE-2024-43379	TruffleHog is a secrets scanning tool. Prior to v3.81.9, this vulnerability allows a malicious actor to craft data in a way that, when scanned by specific detectors, could tri unauthorized request to an endpoint chosen by the attacker. For an exploit to be effective, the target endpoint must be an unauthenticated GET endpoint that produces scan the maliciously crafted data and have such an endpoint targeted for the exploit to succeed. The vulnerability has been resolved in TruffleHog v3.81.9 and later ver
CVE-2024-43841	In the Linux kernel, the following vulnerability has been resolved: wifi: virt_wifi: avoid reporting connection success with wrong SSID When user issues a connection wit virt_wifi has advertised, the __cfg80211_connect_result() will trigger the warning: WARN_ON(bss_not_found). The issue is because the connection code in virt_wifi do space (it only checks the BSSID), and virt_wifi will call cfg80211_connect_result() with WLAN_STATUS_SUCCESS even if the SSID is different from the one virt_wifi h cfg80211 won't be able to find the cfg80211_bss and generate the warning. Fixed it by checking the SSID (from user space) in the connection code.
CVE-2024-43845	In the Linux kernel, the following vulnerability has been resolved: udf: Fix bogus checksum computation in udf_rename() Syzbot reports uninitialized memory access in checksum of '..' directory entry of a moved directory. This is indeed true as we pass on-stack diriter.fi to the udf_update_tag() and because that has only struct fileIdentI impUse or name fields, the checksumming function is going to checksum random stack contents beyond the end of the structure. This is actually harmless because the recompute the checksum from on-disk buffers where everything is properly included. So all that is needed is just removing the bogus calculation.
CVE-2024-7887	A vulnerability was found in LimeSurvey 6.3.0-231016 and classified as problematic. Affected by this issue is some unknown functionality of the file /index.php of the co manipulation of the argument size leads to denial of service. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. NOT early about this disclosure but did not respond in any way.
CVE-2024-7900	A vulnerability, which was classified as problematic, was found in xiaohe4966 TpMeCMS 1.3.3.2. Affected is an unknown function of the file /h.php/general/config?ref=a Configuration Handler. The manipulation of the argument Site Name/Beian/Contact address/copyright/technical support leads to cross site scripting. It is possible to lau exploit has been disclosed to the public and may be used. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.
CVE-2024-7814	A vulnerability, which was classified as problematic, was found in CodeAstro Online Railway Reservation System 1.0. Affected is an unknown function of the file /admin component Add Employee Page. The manipulation of the argument emp_fname /emp_lname /emp_nat_idno/emp_addr leads to cross site scripting. It is possible to lau exploit has been disclosed to the public and may be used.
CVE-2024-7815	A vulnerability has been found in CodeAstro Online Railway Reservation System 1.0 and classified as problematic. Affected by this vulnerability is an unknown function update-employee.php of the component Update Employee Page. The manipulation of the argument emp_fname /emp_lname /emp_nat_idno/emp_addr leads to cross launched remotely. The exploit has been disclosed to the public and may be used.
CVE-2023-48361	Improper initialization in firmware for some Intel(R) CSME may allow a privileged user to potentially enable information disclosure via local access.
CVE-2024-24973	Improper input validation for some Intel(R) Distribution for GDB software before version 2024.0.1 may allow an authenticated user to potentially enable denial of service
CVE-2022-1443	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-1789. Reason: This candidate is a reservation duplicate of CVE-20 should reference CVE-2024-1789 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2024-40619	CVE-2024-40619 IMPACT A denial-of-service vulnerability exists in the affected products. The vulnerability occurs when a malformed CIP packet is sent over the netw major nonrecoverable fault causing a denial-of-service.
CVE-2024-43830	In the Linux kernel, the following vulnerability has been resolved: leds: trigger: Unregister sysfs attributes before calling deactivate() Triggers which have trigger specific related data in trigger-data allocated by the activate() callback and freed by the deactivate() callback. Calling device_remove_groups() after calling deactivate() leaves a attributes show/store functions could be called after deactivation and then operate on the just freed trigger-data. Move the device_remove_groups() call to before deact This also makes the deactivation path properly do things in reverse order of the activation path which calls the activate() callback before calling device_add_groups().
CVE-2024-43831	In the Linux kernel, the following vulnerability has been resolved: media: mediatek: vcodec: Handle invalid decoder vsi Handle an invalid decoder vsi in vpu_dec_init to for future use.
CVE-2023-37228	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this candidate hav accidental usage.
CVE-2024-42675	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that Notes: none.
CVE-2024-43832	In the Linux kernel, the following vulnerability has been resolved: s390/uv: Don't call folio_wait_writeback() without a folio reference folio_wait_writeback() requires that folio reference is held, as documented. After we dropped the PTL, the folio could get freed concurrently. So grab a temporary reference.
CVE-2024-39306	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-39304. Reason: This candidate is a duplicate of CVE-2024-39304. reference CVE-2024-39304 instead of this candidate. This CVE was issued to a vulnerability that is dependent on CVE-2024-39304. According to rule 4.2.15 of the CV assign a different CVE ID to a Vulnerability that is fully interdependent with another Vulnerability. The Vulnerabilities are effectively the same single Vulnerability and MU
CVE-2024-43372	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-43369. Reason: This candidate is a duplicate of CVE-2024-43369. reference CVE-2024-43369 instead of this candidate. This CVE was issued to a vulnerability that is dependent on CVE-2024-43369. According to rule 4.2.15 of the CV assign a different CVE ID to a Vulnerability that is fully interdependent with another Vulnerability. The Vulnerabilities are effectively the same single Vulnerability and MU
CVE-2024-7515	CVE-2024-7515 IMPACT A denial-of-service vulnerability exists in the affected products. A malformed PTP management packet can cause a major nonrecoverable fau

CVE Number	Description
CVE-2024-35214	A tampering vulnerability in the CylanceOPTICS Windows Installer Package of CylanceOPTICS for Windows version 3.2 and 3.3 could allow an attacker to potentially u system thereby leaving it with only the protection of CylancePROTECT.
CVE-2023-1673	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this prevent accidental usage.
CVE-2024-7513	CVE-2024-7513 IMPACT A code execution vulnerability exists in the affected product. The vulnerability occurs due to improper default file permissions allowing any us are executed by account with elevated permissions.
CVE-2024-6456	AVEVA Historian Server has a vulnerability, if exploited, could allow a malicious SQL command to execute under the privileges of an interactive Historian REST Interfa engineered by a miscreant into opening a specially crafted URL.
CVE-2024-7507	CVE-2024-7507 IMPACT A denial-of-service vulnerability exists in the affected products. This vulnerability occurs when a malformed PCCC message is received, caus
CVE-2024-6078	CVE-2024-6078 IMPACT An improper authentication vulnerability exists in the affected product, which could allow a malicious user to generate cookies for any user ID password. If exploited, a malicious user could take over the account of a legitimate user. The malicious user would be able to view and modify data stored in the cloud.
CVE-2022-4425	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this prevent accidental usage.
CVE-2022-4411	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this prevent accidental usage.
CVE-2024-43826	In the Linux kernel, the following vulnerability has been resolved: nfs: pass explicit offset/count to trace events nfs_folio_length is unsafe to use without having the folio >f_mapping that protects against truncations and can lead to kernel crashes. E.g. when running xfstests generic/065 with all nfs trace points enabled. Follow the model in an explicit offset and length. This has the additional benefit that these values can be more accurate as some of the users touch partial folio ranges.
CVE-2022-4404	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this prevent accidental usage.
CVE-2024-40620	CVE-2024-40620 IMPACT A vulnerability exists in the affected product due to lack of encryption of sensitive information. The vulnerability results in data being sent bet Dashboard without encryption, which can be seen in the logs of proxy servers, potentially impacting the data's confidentiality.
CVE-2024-42265	In the Linux kernel, the following vulnerability has been resolved: protect the fetch of ->fd[fd] in do_dup2() from mispredictions both callers have verified that fd is not gr misprediction might end up with tofree = fdt->fd[fd]; being speculatively executed. That's wrong for the same reasons why it's wrong in close_fd()/file_close_fd_locked() array_index_nospec(fd, fdt->max_fds) could differ from fd only in case of speculative execution on mispredicted path.
CVE-2024-42321	In the Linux kernel, the following vulnerability has been resolved: net: flow_dissector: use DEBUG_NET_WARN_ON_ONCE The following splat is easy to reproduce up kernels. Florian Westphal provided the following commit: d1dab4f71d37 ("net: add and use __skb_get_hash_symmetric_net") but this complementary fix has been also and it can be easily backported to -stable kernel which consists in using DEBUG_NET_WARN_ON_ONCE instead to silence the following splat given __skb_get_hash infrastructure to to identify packets in traces. [69133.561393] ------------[cut here]------------ [69133.561404] WARNING: CPU: 0 PID: 43576 at net/core/flow_dissector.c: __skb_flow_dissect+0x134f/ [...] [69133.561944] CPU: 0 PID: 43576 Comm: socat Not tainted 6.10.0-rc7+ #379 [69133.561959] RIP: 0010:__skb_flow_dissect+0x134f 83 f9 04 0f 84 b3 00 00 00 45 85 c9 0f 84 aa 00 00 00 41 83 f9 02 0f 84 81 fc ff ff 44 0f b7 b4 24 80 00 00 00 e9 8b f9 ff ff <0f> 0b e9 20 f3 ff ff 41 f6 c6 20 0f 84 e4 ef ff [69133.561979] RSP: 0018:ffffc90000006fc0 EFLAGS: 00010246 [69133.561988] RAX: 0000000000000000 RBX: ffffffff82f33e20 RCX: ffffffff81ab7e19 [69133.561994 ffffc90000007388 RDI: ffff888103a1b418 [69133.562001] RBP: ffffc90000007310 R08: 0000000000000000 R09: 0000000000000000 [69133.562007] R10: ffffc900000 ffff888103a1b400 [69133.562013] R13: 0000000000000000 R14: ffffffff82f33e2a R15: ffffffff82f33e28 [69133.562020] FS: 00007f40f7131740(0000) GS:ffff888390800(knlGS:0000000000000000 [69133.562027] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [69133.562033] CR2: 00007f40f7346ee0 CR3: 000000015d20000 [69133.562040] Call Trace: [69133.562044] <IRQ> [69133.562049] ? __warn+0x9f/0x1a0 [1211.841384] ? __skb_flow_dissect+0x107e/0x2860 [...] [1211.841496] ? b 1211.841753] __skb_get_hash+0x97/0x280 [1211.841765] ? __skb_get_hash_symmetric+0x230/0x230 [1211.841776] ? mod_find+0xbf/0xe0 [1211.841786] ? get_s 1211.841798] ? bpf_ksym_find+0x56/0xe0 [1211.841807] ? __rcu_read_unlock+0x2a/0x70 [1211.841819] nft_trace_init+0x1b9/0x1c0 [nf_tables] [1211.841895] ? nft [nf_tables] [1211.841964] ? get_stack_info+0x2b/0x80 [1211.841975] ? nft_do_chain_arp+0x80/0x80 [nf_tables] [1211.842044] nft_do_chain+0x79c/0x850 [nf_tables
CVE-2024-43820	In the Linux kernel, the following vulnerability has been resolved: dm-raid: Fix WARN_ON_ONCE check for sync_thread in raid_resume rm-raid devices will occasional when being resumed after a table load because DM_RECOVERY_RUNNING is set: WARNING: CPU: 7 PID: 5660 at drivers/md/dm-raid.c:4105 raid_resume+0xee/0x is: WARN_ON_ONCE(test_bit(MD_RECOVERY_RUNNING, &mddev->recovery)); This check is designed to make sure that the sync thread isn't registered, but md_ch MD_RECOVERY_RUNNING without the sync_thread ever getting registered. Instead of checking if MD_RECOVERY_RUNNING is set, check if sync_thread is non-NU
CVE-2024-43816	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Revise lpfc_prep_embed_io routine with proper endian macro usages On big endian archite memory out of bounds pointer dereference when FCP targets are zoned. In lpfc_prep_embed_io, the memcpy(ptr, fcp_cmnd, sgl->sge_len) is referencing a little endian So, the memcpy can cause big endian systems to crash. Redefine the *sgl ptr as a struct sli4_sge_le to make it clear that we are referring to a little endian formatted da routine with proper le32_to_cpu macro usages.

CVE Number	Description
CVE-2023-2920	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-1503. Reason: This candidate is a reservation duplicate of CVE-2(should reference CVE-2024-1503 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2024-42334	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2022-4405	Rejected reason: **REJECT** This is not considered a valid security vulnerability.
CVE-2024-42290	In the Linux kernel, the following vulnerability has been resolved: irqchip/imx-irqsteer: Handle runtime power management correctly The power domain is automatically However, on certain platforms like i.MX8QM and i.MX8QXP, the power-on handling invokes sleeping functions, which triggers the 'scheduling while atomic' bug in the c probing: BUG: scheduling while atomic: kworker/u13:1/48/0x00000002 Call trace: __schedule_bug+0x54/0x6c __schedule+0x7f0/0xa94 schedule+0x5c/0xc4 schedule __mutex_lock.constprop.0+0x2c0/0x540 __mutex_lock_slowpath+0x14/0x20 mutex_lock+0x48/0x54 clk_prepare_lock+0x44/0xa0 clk_prepare+0x20/0x44 imx_irqsteer pm_generic_runtime_resume+0x2c/0x44 __genpd_runtime_resume+0x30/0x80 genpd_runtime_resume+0xc8/0x2c0 __rpm_callback+0x48/0x1d8 rpm_callback+0x6c/ __pm_runtime_resume+0x50/0x94 irq_chip_pm_get+0x2c/0xa0 __irq_do_set_handler+0x178/0x24c irq_set_chained_handler_and_data+0x60/0xa4 mxc_gpio_probe+ implementing the irq_bus_lock/sync_unlock() interrupt chip callbacks and handle power management in them as they are invoked from non-atomic context. [tglx: Rewr]
CVE-2023-5888	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-7246. Reason: This candidate is a reservation duplicate of CVE-2(should reference CVE-2023-7246 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2023-3207	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2024-31237. Reason: This candidate is a reservation duplicate of CVE-2 users should reference CVE-2024-31237 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2023-4717	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. Reason: This candidate was issued in error. Notes: All references and descriptions in this prevent accidental usage.
CVE-2024-42281	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix a segment issue when downgrading gso_size Linearize the skb when downgrading gso_size l BUG_ON() later when the skb is segmented as described in [1,2].
CVE-2024-42279	In the Linux kernel, the following vulnerability has been resolved: spi: microchip-core: ensure TX and RX FIFOs are empty at start of a transfer While transmitting with r going to be emptied in the interrupt handler. A subsequent transfer could then read crap from the previous transfer out of the RX FIFO into the start RX buffer. The core empty the RX and TX FIFOs, so do that before each transfer.
CVE-2024-42276	In the Linux kernel, the following vulnerability has been resolved: nvme-pci: add missing condition check for existence of mapped data nvme_map_data() is called wher hence the nvme_unmap_data() should have same condition to avoid dereference.
CVE-2024-42275	In the Linux kernel, the following vulnerability has been resolved: drm/client: Fix error code in drm_client_buffer_vmap_local() This function accidentally returns zero/su to locking issues and an uninitialized *map_copy in the caller.
CVE-2024-42274	In the Linux kernel, the following vulnerability has been resolved: Revert "ALSA: firewire-lib: operate for period elapse event in process context" Commit 7ba5ca32fe6e period elapse event in process context") removed the process context workqueue from amdtp_domain_stream_pcm_pointer() and update_pcm_pointers() to remove its 800, this lead to a regression since Kernels 5.14.0, causing an AB/BA deadlock competition for the substream lock with eventual system freeze under ALSA operation: substream lock by snd_pcm_stream_lock_irq() in snd_pcm_status64() * (lock B) wait for tasklet to finish by calling tasklet_unlock_spin_wait() in tasklet_disable_in_ator ohci_flush_iso_completions() of ohci.c thread 1: * (lock B) enter tasklet * (lock A) attempt to acquire substream lock, waiting for it to be released: snd_pcm_stream_lock snd_pcm_period_elapsed() in update_pcm_pointers() in process_ctx_payloads() in process_rx_packets() of amdtp-stream.c ? tasklet_unlock_spin_wait </NMI> <TASK firewire_ohci amdtp_domain_stream_pcm_pointer snd_firewire_lib snd_pcm_update_hw_ptr0 snd_pcm snd_pcm_status64 snd_pcm ? native_queued_spin_lock_slow _raw_spin_lock_irqsave snd_pcm_period_elapsed snd_pcm process_rx_packets snd_firewire_lib irq_target_callback snd_firewire_lib handle_it_packet firewire_ohci co Restore the process context work queue to prevent deadlock AB/BA deadlock competition for ALSA substream lock of snd_pcm_stream_lock_irq() in snd_pcm_status6 snd_pcm_stream_lock_irqsave() in snd_pcm_period_elapsed(). revert commit 7ba5ca32fe6e ("ALSA: firewire-lib: operate for period elapse event in process context") F prevent future deadlock.
CVE-2024-42273	In the Linux kernel, the following vulnerability has been resolved: f2fs: assign CURSEG_ALL_DATA_ATGC if blkaddr is valid mkdir /mnt/test/comp f2fs_io setflags com if=/dev/zero of=/mnt/test/comp/testfile bs=16k count=1 truncate --size 13 /mnt/test/comp/testfile In the above scenario, we can get a BUG_ON. kernel BUG at fs/f2fs/se do_write_page+0x78/0x390 [f2fs] f2fs_outplace_write_data+0x62/0xb0 [f2fs] f2fs_do_write_data_page+0x275/0x740 [f2fs] f2fs_write_single_data_page+0x1dc/0x8f0 [f f2fs_write_multi_pages+0x1e5/0xae0 [f2fs] f2fs_write_cache_pages+0xab1/0xc60 [f2fs] f2fs_write_data_pages+0x2d8/0x330 [f2fs] do_writepages+0xcf/0x270 __writeb writeback_sb_inodes+0x242/0x530 __writeback_inodes_wb+0x54/0xf0 wb_writeback+0x192/0x310 wb_workfn+0x30d/0x400 The reason is we gave CURSEG_ALL_D where the page was set the gcing flag by set_cluster_dirty().
CVE-2024-42267	In the Linux kernel, the following vulnerability has been resolved: riscv/mm: Add handling for VM_FAULT_SIGSEGV in mm_fault_error() Handle VM_FAULT_SIGSEGV correctly kill the process and we don't BUG() the kernel.

CVE Number	Description
CVE-2024-42266	In the Linux kernel, the following vulnerability has been resolved: btrfs: make cow_file_range_inline() honor locked_page on error The btrfs buffered write path runs thro has some tricky return value handling for writepage_delalloc(). Specifically, when that returns 1, we exit, but for other return values we continue and end up calling btrfs folio has been unlocked (note that we check the PageLocked bit at the start of __extent_writepage()), this results in an assert panic like this one from syzbot: BTRFS: e free_log_tree:3267: errno=-5 IO failure BTRFS warning (device loop0 state EAL): Skipping commit of aborted transaction. BTRFS: error (device loop0 state EAL) in cle IO failure assertion failed: folio_test_locked(folio), in fs/btrfs/subpage.c:871 ----------[cut here]---------- kernel BUG at fs/btrfs/subpage.c:871! Oops: invalid opcode: 0 PTI CPU: 1 PID: 5090 Comm: syz-executor225 Not tainted 6.10.0-syzkaller-05505-gb1bc554e009e #0 Hardware name: Google Google Compute Engine/Google Comp 06/27/2024 RIP: 0010:btrfs_folio_end_all_writers+0x55b/0x610 fs/btrfs/subpage.c:871 Code: e9 d3 fb ff ff e8 25 22 c2 fd 48 c7 c7 c0 3c 0e 8c 48 c7 c6 80 3d 0e 8c 48 00 e8 66 47 ad 07 90 <0f> 0b e8 6e 45 b0 07 4c 89 ff be 08 00 00 00 e8 21 12 25 fe 4c 89 RSP: 0018:ffffc900033d72e0 EFLAGS: 00010246 RAX: 000000000000004 663b7a08c50a0a00 RDX: 0000000000000000 RSI: 0000000080000000 RDI: 0000000000000000 RBP: ffffc900033d73b0 R08: ffffffff8176b98c R09: 1ffff9200067adfc fffff5200067adfd R12: 0000000000000001 R13: dffffc0000000000 R14: 0000000000000000 R15: ffffea0001cbee80 FS: 0000000000000000(0000) GS:ffff8880b95000 knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f5f076012f8 CR3: 000000000e134000 CR4: 00000000003506f0 DR0: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __extent_writepage fs/ extent_write_cache_pages fs/btrfs/extent_io.c:2251 [inline] btrfs_writepages+0x14d7/0x2760 fs/btrfs/extent_io.c:2373 do_writepages+0x359/0x870 mm/page-writeback filemap_fdatawrite_wbc+0x125/0x180 mm/filemap.c:397 __filemap_fdatawrite_range mm/filemap.c:430 [inline] __filemap_fdatawrite mm/filemap.c:436 [inline] filemap_ mm/filemap.c:463 btrfs_release_file+0x117/0x130 fs/btrfs/file.c:1547 __fput+0x24a/0x8a0 fs/file_table.c:422 task_work_run+0x24f/0x310 kernel/task_work.c:222 exit_ta include/linux/task_work.h:40 [inline] do_exit+0xa2f/0x27f0 kernel/exit.c:877 do_group_exit+0x207/0x2c0 kernel/exit.c:1026 __do_sys_exit_group kernel/exit.c:1037 [inli kernel/exit.c:1035 [inline] __x64_sys_exit_group+0x3f/0x40 kernel/exit.c:1035 x64_sys_call+0x2634/0x2640 arch/x86/include/generated/asm/syscalls_64.h:232 do_sys arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f5f075b70c9 bytes at 0x7f5f075b709f. I was hitting the same issue by doing hundreds of accelerated runs of generic/475, which also hits IO errors by design. I instrumented that rep that the undesirable folio_unlock was coming from the following callstack: folio_unlock+5 __process_pages_contig+475 cow_file_range_inline.constprop.0+230 cow_fil btrfs_run_delalloc_range+566 writepage_delalloc+332 __extent_writepage # inlined in my stacktrace, but I added it here extent_write_cache_pages+622 Looking at the
CVE-2024-42260	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Validate passed in drm syncobj handles in the performance extension If userspace provides anywhere in the handle array the rest of the driver will not handle that well. Fix it by checking handle was looked up successfully or otherwise fail the extension by jump (cherry picked from commit a546b7e4d73c23838d7e4d2c92882b3ca902d213)
CVE-2024-42261	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Validate passed in drm syncobj handles in the timestamp extension If userspace provides ar anywhere in the handle array the rest of the driver will not handle that well. Fix it by checking handle was looked up successfully or otherwise fail the extension by jump (cherry picked from commit 8d1276d1b8f738c3afe1457d4dff5cc66fc848a3)
CVE-2024-42291	In the Linux kernel, the following vulnerability has been resolved: ice: Add a per-VF limit on number of FDIR filters While the iavf driver adds a s/w limit (128) on the nur can request, a malicious VF driver can request more than that and exhaust the resources for other VFs. Add a similar limit in ice.
CVE-2024-42292	In the Linux kernel, the following vulnerability has been resolved: kobject_uevent: Fix OOB access within zap_modalias_env() zap_modalias_env() wrongly calculates s will cause OOB memory access issue if variable MODALIAS is not the last one within its @env parameter, fixed by correcting size to memmove.
CVE-2024-42293	In the Linux kernel, the following vulnerability has been resolved: arm64: mm: Fix lockless walks with static and dynamic page-table folding Lina reports random oopser code when 16K pages are used with 4-level page-tables, the fourth level being folded at runtime due to lack of LPA2. In this configuration, the generic implementation c a 'p4d_t *' corresponding to the 'pgd_t' allocated on the stack of the caller, gup_fast_pgd_range(). This is normally fine, but when the fourth level of page-table is folded will offset from the address of the 'p4d_t' to calculate the address of the PUD in the same page-table page. This results in a stray stack read when the 'p4d_t' has been send the walker into the weeds. Fix the problem by providing our own definition of p4d_offset_lockless() when CONFIG_PGTABLE_LEVELS <= 4 which returns the rea the address of the local stack variable.
CVE-2024-42308	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2024-43815	In the Linux kernel, the following vulnerability has been resolved: crypto: mxs-dcp - Ensure payload is zero when using key slot We could leak stack memory through th AES with a key from one of the hardware's key slots. Fix this by ensuring the payload field is set to 0 in such cases. This does not affect the common use case when th memory via the descriptor payload.
CVE-2024-42322	In the Linux kernel, the following vulnerability has been resolved: ipvs: properly dereference pe in ip_vs_add_service Use pe directly to resolve sparse warning: net/netf warning: dereference of noderef expression
CVE-2024-42264	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Prevent out of bounds access in performance query extensions Check that the number of pe the copy and reset extensions is not greater than the internal kernel storage where the ids will be copied into. (cherry picked from commit f32b5128d2c440368b5bf3a7a
CVE-2024-42319	In the Linux kernel, the following vulnerability has been resolved: mailbox: mtk-cmdq: Move devm_mbox_controller_register() after devm_pm_runtime_enable() When r message with condition pm_runtime_get_sync() < 0 occurs. According to the call tracei below: cmdq_mbox_shutdown mbox_free_channel mbox_controller_unregister __devm_mbox_controller_unregister ... The root cause can be deduced to be calling pm_runtime_get_sync() after calling pm_runtime_disable() as observed below: 1. devm_mbox_controller_register() in cmdq_probe() to bind the cmdq device to the mbox_controller, so devm_mbox_controller_unregister() will automatically unregister controller when the device-managed resource is removed. That means devm_mbox_controller_unregister() and cmdq_mbox_shoutdown() will be called after cmdq_rer uses devm_pm_runtime_enable() in cmdq_probe() after devm_mbox_controller_register(), so that devm_pm_runtime_disable() will be called after cmdq_remove(), but devm_mbox_controller_unregister(). To fix this problem, cmdq_probe() needs to move devm_mbox_controller_register() after devm_pm_runtime_enable() to make dev called after devm_mbox_controller_unregister().
CVE-2024-42318	In the Linux kernel, the following vulnerability has been resolved: landlock: Don't lose track of restrictions on cred_transfer When a process' cred struct is replaced, this cred_prepare LSM hook; but in one special case (when KEYCTL_SESSION_TO_PARENT updates the parent's credentials), the cred_transfer LSM hook is used instea cred_prepare hook, not cred_transfer, so KEYCTL_SESSION_TO_PARENT causes all information on Landlock restrictions to be lost. This basically means that a proc fork() and keyctl() syscalls can get rid of all Landlock restrictions on itself. Fix it by adding a cred_transfer hook that does the same thing as the existing cred_prepare h hook_cred_prepare() call hook_cred_transfer() so that the two functions are less likely to accidentally diverge in the future.)

CVE Number	Description
CVE-2024-42317	In the Linux kernel, the following vulnerability has been resolved: mm/huge_memory: avoid PMD-size page cache if needed xarray can't support arbitrary page cache s page cache size is defined as MAX_PAGECACHE_ORDER by commit 099d90642a71 ("mm/filemap: make MAX_PAGECACHE_ORDER acceptable to xarray"). Howe page cache in the huge memory's collapsing path on ARM64 system whose base page size is 64KB. 512MB page cache is breaking the limitation and a warning is rais as shown in the following example. [root@dhcp-10-26-1-207 ~]# cat /proc/1/smaps | grep KernelPageSize KernelPageSize: 64 kB [root@dhcp-10-26-1-207 ~]# cat /tm **argv) { const char *filename = TEST_XFS_FILENAME; int fd = 0; void *buf = (void *)-1, *p; int pgsize = getpagesize(); int ret = 0; if (pgsize != 0x10000) { fprintf(stdout, size is required!\n"); return -EPERM; } system("echo 0 > /sys/devices/virtual/bdi/253:0/read_ahead_kb"); system("echo 1 > /proc/sys/vm/drop_caches"); /* Open the xfs O_RDONLY); assert(fd > 0); /* Create VMA */ buf = mmap(NULL, TEST_MEM_SIZE, PROT_READ, MAP_SHARED, fd, 0); assert(buf != (void *)-1); fprintf(stdout, "ma Populate VMA */ ret = madvise(buf, TEST_MEM_SIZE, MADV_NOHUGEPAGE); assert(ret == 0); ret = madvise(buf, TEST_MEM_SIZE, MADV_POPULATE_READ); */ ret = madvise(buf, TEST_MEM_SIZE, MADV_HUGEPAGE); assert(ret == 0); ret = madvise(buf, TEST_MEM_SIZE, MADV_COLLAPSE); if (ret) { fprintf(stdout, "Erro madvise(MADV_COLLAPSE)\n", errno); goto out; } /* Split xarray entry. Write permission is needed */ munmap(buf, TEST_MEM_SIZE); buf = (void *)-1; close(fd); fd = assert(fd > 0); fallocate(fd, FALLOC_FL_KEEP_SIZE | FALLOC_FL_PUNCH_HOLE, TEST_MEM_SIZE - pgsize, pgsize); out: if (buf != (void *)-1) munmap(buf, TEST_ return ret; } [root@dhcp-10-26-1-207 ~]# gcc /tmp/test.c -o /tmp/test [root@dhcp-10-26-1-207 ~]# /tmp/test ------------[cut here]------------ WARNING: CPU: 25 PID: 756 xas_split_alloc+0xf8/0x128 Modules linked in: nft_fib_inet nft_fib_ipv4 nft_fib_ipv6 nft_fib \ nft_reject_inet nf_reject_ipv4 nf_reject_ipv6 nft_reject nft_ct \ nft_chain_nat nf_defrag_ipv6 nf_defrag_ipv4 \ ip_set rfkill nf_tables nfnetlink vfat fat virtio_balloon drm fuse \ xfs libcrc32c crct10dif_ce ghash_ce sha2_ce sha256_arm64 virtio_net \ virtio_console failover dimlib virtio_mmio CPU: 25 PID: 7560 Comm: test Kdump: loaded Not tainted 6.10.0-rc7-gavin+ #9 Hardware name: QEMU KVM Virtual Machin 05/24/2024 pstate: 83400005 (Nzcv daif +PAN -UAO +TCO +DIT -SSBS BTYPE=--) pc : xas_split_alloc+0xf8/0x128 lr : split_huge_page_to_list_to_order+0x1c4/0x78 ffff8000ac32f660 x28: ffff0000e0969eb0 x27: ffff8000ac32f6c0 x26: 0000000000000c40 x25: ffff0000e0969eb0 x24: 000000000000000d x23: ffff8000ac32f6c0 x22: ffff 0000000000000000 x20: 0000000000000000 x19: ffffffdfc0700000 x18: 0000000000000000 x17: 0000000000000000 x16: ffffd5f3708ffc70 x15: 0000000000000000 x 0000000000000000 x12: 0000000000000000 x11: ffffffffffffffc0 x10: 0000000000000040 x9 : ffffd5f3708e692c x8 : 0000000000000003 x7 : 0000000000000000 x6 : fff ffffd5f37289e378 x4 : 0000000000000000 x3 : 0000000000000c40 x2 : 000000000000000d x1 : 000000000000000c x0 : 0000000000000000 Call trace: xas_split_allo split_huge_page_to_list_to_order+0x1c4/0x780 truncate_inode_partial_folio+0xdc/0x160 truncate_inode_pages_range+0x1b4/0x4a8 truncate_pagecache_range+0x8
CVE-2024-42312	In the Linux kernel, the following vulnerability has been resolved: sysctl: always initialize i_uid/i_gid Always initialize i_uid/i_gid inside the sysfs core so set_ownership() Commit 5ec27ec735ba ("fs/proc/proc_sysctl.c: fix the default values of i_uid/i_gid on /proc/sys inodes.") added defaults for i_uid/i_gid when set_ownership() was not im adjusting net_ctl_set_ownership() to use the same default values in case the computation of a better value failed.
CVE-2024-7958	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority.
CVE-2024-42295	In the Linux kernel, the following vulnerability has been resolved: nilfs2: handle inconsistent state in nilfs_btnode_create_block() Syzbot reported that a buffer state inco nilfs_btnode_create_block(), triggering a kernel bug. It is not appropriate to treat this inconsistency as a bug; it can occur if the argument block address (the buffer inde virtual block number and has been reallocated due to corruption of the bitmap used to manage its allocation state. So, modify nilfs_btnode_create_block() and its caller filesystem error, rather than triggering a kernel bug.
CVE-2024-42306	In the Linux kernel, the following vulnerability has been resolved: udf: Avoid using corrupted block bitmap buffer When the filesystem block bitmap is corrupted, we dete the bitmap and fail the allocation with error. However the next allocation from the same bitmap will notice the bitmap buffer is already loaded and tries to allocate from t (depending on the exact nature of the bitmap corruption). Fix the problem by using BH_verified bit to indicate whether the bitmap is valid or not.
CVE-2024-42305	In the Linux kernel, the following vulnerability has been resolved: ext4: check dot and dotdot of dx_root before making dir indexed Syzbot reports a issue as follows: == BUG: unable to handle page fault for address: ffffed11022e24fe PGD 23ffee067 P4D 23ffee067 PUD 0 Oop SMP KASAN PTI CPU: 0 PID: 5079 Comm: syz-executor306 Not tainted 6.10.0-rc5-g55027e689933 #0 Call Trace: <TASK> make_indexed_dir+0xdaf/0x13c0 fs/ext4/ ext4_add_entry+0x222a/0x25d0 fs/ext4/namei.c:2451 ext4_rename fs/ext4/namei.c:3936 [inline] ext4_rename2+0x26e5/0x4370 fs/ext4/namei.c:4214 [...] == The immediate cause of this problem is that there is only one valid dentry for the block to be split during do_ bounds accesses to the map triggering the issue. do_split unsigned split dx_make_map count = 1 split = count/2 = 0; continued = hash2 == map[split - 1].hash; ---> ma length of a filename is 255 and the minimum block size is 1024, so it is always guaranteed that the number of entries is greater than or equal to 2 when do_split() is call has no dot and dotdot in dir, and the dentry distribution in dirblock is as follows: bus dentry1 hole dentry2 free |xx--|xx----------|.....|xx----------|.....| 0 12 (8 (8+256)=264 788 236 1024 So when renaming dentry1 increases its name_len length by 1, neither hole nor free is sufficient to hold the new dentry, and make_indexed make_indexed_dir() it is assumed that the first two entries of the dirblock must be dot and dotdot, so bus and dentry1 are left in dx_root because they are treated as do moved to the new leaf block. That's why count is equal to 1. Therefore add the ext4_check_dx_root() helper function to add more sanity checks to dot and dotdot before the above issue.
CVE-2024-42304	In the Linux kernel, the following vulnerability has been resolved: ext4: make sure the first directory block is not a hole The syzbot constructs a directory that has no dirt directory block is a hole. And no errors are reported when creating files in this directory in the following flow. ext4_mknod ... ext4_add_entry // Read block 0 ext4_read_ ext4_bread(NULL, inode, block, 0) if (!bh && (type == INDEX || type == DIRENT_HTREE)) // The first directory block is a hole // But type == DIRENT, so no error is rep directory block without '.' and '..' but with a valid dentry. This may cause some code that relies on dot or dotdot (such as make_indexed_dir()) to crash. Therefore when the first directory block is a hole report that the filesystem is corrupted and return an error to avoid loading corrupted data from disk causing something bad.
CVE-2024-42303	In the Linux kernel, the following vulnerability has been resolved: media: imx-pxp: Fix ERR_PTR dereference in pxp_probe() devm_regmap_init_mmio() can fail, add a error.
CVE-2024-42300	In the Linux kernel, the following vulnerability has been resolved: erofs: fix race in z_erofs_get_gbuf() In z_erofs_get_gbuf(), the current task may be migrated to anothe `z_erofs_gbuf_id()` and `spin_lock(&gbuf->lock)`. Therefore, z_erofs_put_gbuf() will trigger the following issue which was found by stress test: <2>[772156.434168] ker <4>[772156.435007] <4>[772156.439237] CPU: 0 PID: 3078 Comm: stress Kdump: loaded Tainted: G E 6.10.0-rc7+ #2 <4>[772156.439239] Hardware name: Alibaba 1.0.0 01/01/2017 <4>[772156.439241] pstate: 83400005 (Nzcv daif +PAN -UAO +TCO +DIT -SSBS BTYPE=--) <4>[772156.439243] pc : z_erofs_put_gbuf+0x64/0x70 z_erofs_lz4_decompress+0x600/0x6a0 [erofs] .. <6>[772156.445958] stress (3127): drop_caches: 1 <4>[772156.446120] Call trace: <4>[772156.446121] z_erofs_put_ [772156.446761] z_erofs_lz4_decompress+0x600/0x6a0 [erofs] <4>[772156.446897] z_erofs_decompress_queue+0x740/0xa10 [erofs] <4>[772156.447036] z_erofs_r <4>[772156.447160] z_erofs_readahead+0x224/0x390 [erofs] ..
CVE-2024-42299	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: Update log->page_{mask,bits} if log->page_size changed If an NTFS file system is mounted t PAGE_SIZE from the original system, log->page_size will change in log_replay(), but log->page_{mask,bits} don't change correspondingly. This will cause a panic beca - page_off" will get a negative value in the later read_log_page().

CVE Number	Description
CVE-2024-42296	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix return value of f2fs_convert_inline_inode() If device is readonly, make f2fs_convert_inline_ino zero, otherwise it may trigger panic during writeback of inline inode's dirty page as below: f2fs_write_single_data_page+0xbb6/0x1e90 fs/f2fs/data.c:2888 f2fs_write_ca [inline] __f2fs_write_data_pages fs/f2fs/data.c:3342 [inline] f2fs_write_data_pages+0x1efe/0x3a90 fs/f2fs/data.c:3369 do_writepages+0x359/0x870 mm/page-writeback filemap_fdatawrite_wbc+0x125/0x180 mm/filemap.c:397 __filemap_fdatawrite_range mm/filemap.c:430 [inline] file_write_and_wait_range+0x1aa/0x290 mm/filemap.c:7 f2fs_do_sync_file+0x68a/0x1ae0 fs/f2fs/file.c:276 generic_write_sync include/linux/fs.h:2806 [inline] f2fs_file_write_iter+0x7bd/0x24e0 fs/f2fs/file.c:4977 call_write_iter i new_sync_write fs/read_write.c:497 [inline] vfs_write+0xa72/0xc90 fs/read_write.c:590 ksys_write+0x1a0/0x2c0 fs/read_write.c:643 do_syscall_x64 arch/x86/entry/com do_syscall_64+0xf5/0x240 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f
CVE-2024-21689	This High severity RCE (Remote Code Execution) vulnerability CVE-2024-21689 was introduced in versions 9.1.0, 9.2.0, 9.3.0, 9.4.0, 9.5.0, and 9.6.0 of Bamboo Data (Remote Code Execution) vulnerability, with a CVSS Score of 7.6, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, h impact to availability, and requires user interaction. Atlassian recommends that Bamboo Data Center and Server customers upgrade to latest version, if you are unable to one of the specified supported fixed versions: Bamboo Data Center and Server 9.2: Upgrade to a release greater than or equal to 9.2.17 Bamboo Data Center and S greater than or equal to 9.6.5 See the release notes ([https://confluence.atlassian.com/bamboreleases/bamboo-release-notes-1189793869.html]). You can download Data Center and Server from the download center ([https://www.atlassian.com/software/bamboo/download-archives]). This vulnerability was reported via our Bug Boun