SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 25 September 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-2024-8887	CIRCUTOR Q-SMT in its firmware version 1.0.4, could be affected by a denial of service (DoS) attack if an attacker with access to the web service bypasses the authentication mechanisms on the login page, allowing the attacker to use all the functionalities implemented at web level that allow interacting with the device.	10.0	More Details
CVE-2024-0002	A condition exists in FlashArray Purity whereby an attacker can employ a privileged account allowing remote access to the array.	10.0	More Details
CVE-2024-0001	A condition exists in FlashArray Purity whereby a local account intended for initial array configuration remains active potentially allowing a malicious actor to gain elevated privileges.	10.0	More Details
CVE-2024-8888	An attacker with access to the network where CIRCUTOR Q-SMT is located in its firmware version 1.0.4, could steal the tokens used on the web, since these have no expiration date to access the web application without restrictions. Token theft can originate from different methods such as network captures, locally stored web information, etc.	10.0	More Details
CVE-2024-8624	The MDTF – Meta Data and Taxonomies Filter plugin for WordPress is vulnerable to SQL Injection via the 'meta_key' attribute of the 'mdf_select_title' shortcode in all versions up to, and including, 1.3.3.3 due to insufficient escaping on the user supplied parameter and lack of sufficient preparation on the existing SQL query. This makes it possible for authenticated attackers, with Contributor-level access and above, to append additional SQL queries into already existing queries that can be used to extract sensitive information from the database.	9.9	More Details
CVE-2024-9014	pgAdmin versions 8.11 and earlier are vulnerable to a security flaw in OAuth2 authentication. This vulnerability allows an attacker to potentially obtain the client ID and secret, leading to unauthorized access to user data.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46986	Camaleon CMS is a dynamic and advanced content management system based on Ruby on Rails. An arbitrary file write vulnerability accessible via the upload method of the MediaController allows authenticated users to write arbitrary files to any location on the web server Camaleon CMS is running on (depending on the permissions of the underlying filesystem). E.g. This can lead to a delayed remote code execution in case an attacker is able to write a Ruby file into the config/initializers/ subfolder of the Ruby on Rails application. This issue has been addressed in release version 2.8.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.9	More Details
CVE-2024-33109	Directory Traversal in the web interface of the Tiptel IP 286 with firmware version 2.61.13.10 allows attackers to overwrite arbitrary files on the phone via the Ringtone upload function.	9.9	More Details
CVE-2024-47222	New Cloud MyOffice SDK Collaborative Editing Server 2.2.2 through 2.8 allows SSRF via manipulation of requests from external document storage via the MS-WOPI protocol.	9.8	More Details
CVE-2024-46997	DataEase is an open source data visualization analysis tool. Prior to version 2.10.1, an attacker can achieve remote command execution by adding a carefully constructed h2 data source connection string. The vulnerability has been fixed in v2.10.1.	9.8	More Details
CVE-2024-34331	A lack of code signature verification in Parallels Desktop for Mac v19.3.0 and below allows attackers to escalate privileges via a crafted macOS installer, because Parallels Service is setuid root.	9.8	More Details
CVE-2024-45410	Traefik is a golang, Cloud Native Application Proxy. When a HTTP request is processed by Traefik, certain HTTP headers such as X-Forwarded-Host or X-Forwarded-Port are added by Traefik before the request is routed to the application. For a HTTP client, it should not be possible to remove or modify these headers. Since the application trusts the value of these headers, security implications might arise, if they can be modified. For HTTP/1.1, however, it was found that some of theses custom headers can indeed be removed and in certain cases manipulated. The attack relies on the HTTP/1.1 behavior, that headers can be defined as hop-by-hop via the HTTP Connection header. This issue has been addressed in release versions 2.11.9 and 3.1.3. Users are advised to upgrade. There are no known workarounds for this vulnerability.	9.8	More Details
CVE-2024-46640	SeaCMS 13.2 has a remote code execution vulnerability located in the file sql.class.chp. Although the system has a check function, the check function is not executed during execution, allowing remote code execution by writing to the file through the MySQL slow query method.	9.8	More Details
CVE-2024-46103	SEMCMS 4.8 is vulnerable to SQL Injection via SEMCMS_Main.php.	9.8	More Details
CVE-2024-46101	GDidees CMS <= v3.9.1 has a file upload vulnerability.	9.8	More Details
CVE-2024-45489	Arc before 2024-08-26 allows remote code execution in JavaScript boosts. Boosts that run JavaScript cannot be shared by default; however (because of misconfigured Firebase ACLs), it is possible to create or update a boost using another user's ID. This installs the boost in the victim's browser and runs arbitrary Javascript on that browser in a privileged context. NOTE: this is a no-action cloud vulnerability with zero affected users.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46652	Tenda AC8v4 V16.03.34.06 has a stack overflow vulnerability in the fromAdvSetMacMtuWan function.	9.8	More Details
CVE-2024-9043	Secure Email Gateway from Cellopoint has Buffer Overflow Vulnerability in authentication process. Remote unauthenticated attackers can send crafted packets to crash the process, thereby bypassing authentication and obtaining system administrator privileges.	9.8	More Details
CVE-2024-8853	The Webo-facto plugin for WordPress is vulnerable to privilege escalation in versions up to, and including, 1.40 due to insufficient restriction on the 'doSsoAuthentification' function. This makes it possible for unauthenticated attackers to make themselves administrators by registering with a username that contains '-wfuser'.	9.8	More Details
CVE-2024-47218	An issue was discovered in vesoft NebulaGraph through 3.8.0. It allows bypassing authentication.	9.8	More Details
CVE-2024-46983	sofa-hessian is an internal improved version of Hessian3/4 powered by Ant Group CO., Ltd. The SOFA Hessian protocol uses a blacklist mechanism to restrict deserialization of potentially dangerous classes for security protection. But there is a gadget chain that can bypass the SOFA Hessian blacklist protection mechanism, and this gadget chain only relies on JDK and does not rely on any third-party components. This issue is fixed by an update to the blacklist, users can upgrade to sofahessian version 3.5.5 to avoid this issue. Users unable to upgrade may maintain a blacklist themselves in the directory `external/serialize.blacklist`.	9.8	More Details
CVE-2023-27584	Dragonfly is an open source P2P-based file distribution and image acceleration system. It is hosted by the Cloud Native Computing Foundation (CNCF) as an Incubating Level Project. Dragonfly uses JWT to verify user. However, the secret key for JWT, "Secret Key", is hard coded, which leads to authentication bypass. An attacker can perform any action as a user with admin privileges. This issue has been addressed in release version 2.0.9. All users are advised to upgrade. There are no known workarounds for this vulnerability.	9.8	More Details
CVE-2024-46375	Best House Rental Management System 1.0 contains an arbitrary file upload vulnerability in the signup() function of the file rental/admin_class.php.	9.8	More Details
CVE-2024-35515	Insecure deserialization in sqlitedict up to v2.1.0 allows attackers to execute arbitrary code.	9.8	More Details
CVE-2024-44542	SQL Injection vulnerability in todesk v.1.1 allows a remote attacker to execute arbitrary code via the /todesk.com/news.html parameter.	9.8	More Details
CVE-2024-34399	**UNSUPPORTED WHEN ASSIGNED** An issue was discovered in BMC Remedy Mid Tier 7.6.04. An unauthenticated remote attacker is able to access any user account without using any password. NOTE: This vulnerability only affects products that are no longer supported by the maintainer and the impacted version for this vulnerability is 7.6.04 only.	9.8	More Details
CVE-2024-40125	An arbitrary file upload vulnerability in the Media Manager function of Closed-Loop Technology CLESS Server v4.5.2 allows attackers to execute arbitrary code via uploading a crafted PHP file to the upload endpoint.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40568	Buffer Overflow vulnerability in btstack mesh commit before v.864e2f2b6b7878c8fab3cf5ee84ae566e3380c58 allows a remote attacker to execute arbitrary code via the pb_adv_handle_tranaction_cont function in the src/mesh/pb_adv.c component	9.8	More Details
CVE-2024-46374	Best House Rental Management System 1.0 contains a SQL injection vulnerability in the delete_category() function of the file rental/admin_class.php.	9.8	More Details
CVE-2024-8791	The Donation Forms by Charitable – Donations Plugin & Fundraising Platform for WordPress plugin for WordPress is vulnerable to privilege escalation in all versions up to, and including, 1.8.1.14. This is due to the plugin not properly verifying a user's identity when the ID parameter is supplied through the update_core_user() function. This makes it possible for unauthenticated attackers to update the email address and password of arbitrary user accounts, including administrators, which can then be used to log in to those user accounts.	9.8	More Details
CVE-2024-46376	Best House Rental Management System 1.0 contains an arbitrary file upload vulnerability in the update_account() function of the file rental/admin_class.php.	9.8	More Details
CVE-2024-46377	Best House Rental Management System 1.0 contains an arbitrary file upload vulnerability in the save_settings() function of the file rental/admin_class.php.	9.8	More Details
CVE-2024-46946	langchain_experimental (aka LangChain Experimental) 0.1.17 through 0.3.0 for LangChain allows attackers to execute arbitrary code through sympy.sympify (which uses eval) in LLMSymbolicMathChain. LLMSymbolicMathChain was introduced in fcccde406dd9e9b05fc9babcbeb9ff527b0ec0c6 (2023-10-05).	9.8	More Details
CVE-2024-47088	This vulnerability exists in Apex Softcell LD Geo due to missing restrictions for excessive failed authentication attempts on its API based login. A remote attacker could exploit this vulnerability by conducting a brute force attack on login OTP, which could lead to gain unauthorized access to other user accounts.	9.8	More Details
CVE-2024-31570	libfreeimage in FreeImage 3.4.0 through 3.18.0 has a stack-based buffer overflow in the PluginXPM.cpp Load function via an XPM file.	9.8	More Details
CVE-2024-7024	Inappropriate implementation in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	9.6	More Details
CVE-2024-8963	Path Traversal in the Ivanti CSA before 4.6 Patch 519 allows a remote unauthenticated attacker to access restricted functionality.	9.4	More Details
CVE-2024-8889	Vulnerability in CIRCUTOR TCP2RS+ firmware version 1.3b, which could allow an attacker to modify any configuration value, even if the device has the user/password authentication option enabled, without authentication by sending packets through the UDP protocol and port 2000, deconfiguring the device and thus disabling its use. This equipment is at the end of its useful life cycle.	9.3	More Details
CVE-2024-45523	An issue was discovered in Bravura Security Fabric versions 12.3.x before 12.3.5.32784, 12.4.x before 12.4.3.35110, 12.5.x before 12.5.2.35950, 12.6.x before 12.6.2.37183, and 12.7.x before 12.7.1.38241. An unauthenticated attacker can cause a resource leak by issuing multiple failed login attempts through API SOAP.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-0003	A condition exists in FlashArray Purity whereby a malicious user could use a remote administrative service to create an account on the array allowing privileged access.	9.1	More Details
CVE-2024-0004	A condition exists in FlashArray Purity whereby an user with array admin role can execute arbitrary commands remotely to escalate privilege on the array.	9.1	More Details
CVE-2024-0005	A condition exists in FlashArray and FlashBlade Purity whereby a malicious user could execute arbitrary commands remotely through a specifically crafted SNMP configuration.	9.1	More Details
CVE-2024-8671	The WooEvents - Calendar and Event Booking plugin for WordPress is vulnerable to arbitrary file overwrite due to insufficient file path validation in the inc/barcode.php file in all versions up to, and including, 4.1.2. This makes it possible for unauthenticated attackers to overwrite arbitrary files on the server, which can easily lead to remote code execution when the right file is deleted (such as wp-config.php).	9.1	More Details
CVE-2024-34026	A stack-based buffer overflow vulnerability exists in the OpenPLC Runtime EtherNet/IP parser functionality of OpenPLC _v3 b4702061dc14d1024856f71b4543298d77007b88. A specially crafted EtherNet/IP request can lead to remote code execution. An attacker can send a series of EtherNet/IP requests to trigger this vulnerability.	9.0	More Details
CVE-2024-47066	Lobe Chat is an open-source artificial intelligence chat framework. Prior to version 1.19.13, server-side request forgery protection implemented in `src/app/api/proxy/route.ts` does not consider redirect and could be bypassed when attacker provides an external malicious URL which redirects to internal resources like a private network or loopback address. Version 1.19.13 contains an improved fix for the issue.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2024-46086	FrogCMS V0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) vulnerability via /admin/?/plugin/file_manager/delete/123	8.8	More Details
CVE-2024-47210	Gladys Assistant before 4.45.1 allows Privilege Escalation (a user changing their own role) because req.body.role can be used in updateMySelf in server/api/controllers/user.controller.js.	8.8	More Details
CVE-2024-23934	Sony XAV-AX5500 WMV/ASF Parsing Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sony XAV-AX5500 devices. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of WMV/ASF files. A crafted Extended Content Description Object in a WMV media file can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. . Was ZDI-CAN-22994.	8.8	More Details
CVE-2023-41610	Victure PC420 1.1.39 was discovered to contain a hardcoded root password which is stored in plaintext.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41612	Victure PC420 1.1.39 was discovered to use a weak encryption key for the file enabled_telnet.dat on the Micro SD card.	8.8	More Details
CVE-2024-47001	Hidden functionality issue in multiple digital video recorders provided by TAKENAKA ENGINEERING CO., LTD. allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings.	8.8	More Details
CVE-2024-8606	Bypass of two factor authentication in RestAPI in Checkmk < 2.3.0p16 and < 2.2.0p34 allows authenticated users to bypass two factor authentication	8.8	More Details
CVE-2024-8795	The BA Book Everything plugin for WordPress is vulnerable to Cross-Site Request Forgery in all versions up to, and including, 1.6.20. This is due to missing or incorrect nonce validation on the my_account_update() function. This makes it possible for unauthenticated attackers to update a user's account details via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This can be leveraged to reset a user's password and gain access to their account.	8.8	More Details
CVE-2021-38023	Use after free in Extensions in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2024-5958	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Eliz Software Panel allows Command Line Execution through SQL Injection.This issue affects Panel: before v2.3.24.	8.8	More Details
CVE-2024-43778	OS command injection vulnerability in multiple digital video recorders provided by TAKENAKA ENGINEERING CO., LTD. allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings.	8.8	More Details
CVE-2024-41929	Improper authentication vulnerability in multiple digital video recorders provided by TAKENAKA ENGINEERING CO., LTD. allows a remote authenticated attacker to execute an arbitrary OS command on the device or alter the device settings.	8.8	More Details
CVE-2024-7023	Insufficient data validation in Updater in Google Chrome prior to 128.0.6537.0 allowed a remote attacker to perform privilege escalation via a malicious file. (Chromium security severity: Medium)	8.8	More Details
CVE-2024-46394	FrogCMS v0.9.5 was discovered to contain a Cross-Site Request Forgery (CSRF) via /admin/?/user/add	8.8	More Details
CVE-2024-46373	Dedecms V5.7.115 contains an arbitrary code execution via file upload vulnerability in the backend.	8.8	More Details
CVE-2024-42404	SQL injection vulnerability in Welcart e-Commerce prior to 2.11.2 allows an attacker who can login to the product to obtain or alter the information stored in the database.	8.8	More Details
CVE-2024-43201	The Planet Fitness Workouts iOS and Android mobile apps prior to version 9.8.12 (released on 2024-07-25) fail to properly validate TLS certificates, allowing an attacker with appropriate network access to obtain session tokens and sensitive information.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-37779	WoodWing Elvis DAM v6.98.1 was discovered to contain an authenticated remote command execution (RCE) vulnerability via the Apache Ant script functionality.	8.8	More Details
CVE-2024-42323	SnakeYaml Deser Load Malicious xml rce vulnerability in Apache HertzBeat (incubating). This vulnerability can only be exploited by authorized attackers. This issue affects Apache HertzBeat (incubating): before 1.6.0. Users are recommended to upgrade to version 1.6.0, which fixes the issue.	8.8	More Details
CVE-2024-44589	Stack overflow vulnerability in the Login function in the HNAP service in D-Link DCS-960L with firmware 1.09 allows attackers to execute of arbitrary code.	8.8	More Details
CVE-2024-7736	A reflected Cross-site Scripting (XSS) vulnerability affecting ENOVIA Collaborative Industry Innovator from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2024-7737	A stored Cross-site Scripting (XSS) vulnerability affecting 3DSwym in 3DSwymer from Release 3DEXPERIENCE R2022x through Release 3DEXPERIENCE R2024x allows an attacker to execute arbitrary script code in user's browser session.	8.7	More Details
CVE-2024-46984	The reference validator is a tool to perform advanced validation of FHIR resources for TI applications and interoperability standards. The profile location routine in the referencevalidator commons package is vulnerable to `XML External Entities` attack due to insecure defaults of the used Woodstox WstxInputFactory. A malicious XML resource can lead to network requests issued by referencevalidator and thus to a `Server Side Request Forgery` attack. The vulnerability impacts applications which use referencevalidator to process XML resources from untrusted sources. The problem has been patched with the 2.5.1 version of the referencevalidator. Users are strongly recommended to update to this version or a more recent one. A pre-processing or manual analysis of input XML resources on existence of DTD definitions or external entities can mitigate the problem.	8.6	More Details
CVE-2023-47105	exec.CommandContext in Chaosblade 0.3 through 1.7.3, when server mode is used, allows OS command execution via the cmd parameter without authentication.	8.6	More Details
CVE-2024-45752	logiops through 0.3.4, in its default configuration, allows any unprivileged user to configure its logid daemon via an unrestricted D-Bus service, including setting malicious keyboard macros. This allows for privilege escalation with minimal user interaction.	8.5	More Details
CVE-2023-47480	An issue in Pure Data 0.54-0 and fixed in 0.54-1 allows a local attacker to escalate privileges via the set*id () function.	8.4	More Details
CVE-2024-45679	Heap-based buffer overflow vulnerability in Assimp versions prior to 5.4.3 allows a local attacker to execute arbitrary code by importing a specially crafted file into the product.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47061	Plate is a javascript toolkit that makes it easier for you to develop with Slate, a popular framework for building text editors. One longstanding feature of Plate is the ability to add custom DOM attributes to any element or leaf using the `attributes` property. These attributes are passed to the node component using the `nodeProps` prop. It has come to our attention that this feature can be used for malicious purposes, including cross-site scripting (XSS) and information exposure (specifically, users' IP addresses and whether or not they have opened a malicious document). Note that the risk of information exposure via attributes is only relevant to applications in which web requests to arbitrary URLs are not ordinarily allowed. Plate editors that allow users to embed images from arbitrary URLs, for example, already carry the risk of leaking users' IP addresses to third parties. All Plate editors using an affected version of @udecode/plate-core are vulnerable to these information exposure attacks via the style attribute and other attributes that can cause web requests to be sent. In addition, whether or not a Plate editor is vulnerable to cross-site scripting attacks using attributes depends on a number of factors. The most likely DOM attributes to be vulnerable are href and src on links and iframes respectively. Any component that spreads {...nodeProps} onto an <a> or <iframe> element and does not later override href or src will be vulnerable to XSS. In patched versions of Plate, we have disabled element.attributes and leaf.attributes for most attribute names by default, with some exceptions including target, alt, width, height, colspan and rowspan on the link, image, video, table cell and table header cell plugins. If this is a breaking change for you, you can selectively re-enable attributes for certain plugins as follows. Please carefully research and assess the security implications of any attribute you allow, as even seemingly innocuous attributes such as style can be used maliciously. If you are unable to upgrade to any of the patched versions, you should use a tool like patch-package or yarn patch to remove the logic from @udecode/plate-core that adds attributes to nodeProps.	8.3	More Details
CVE-2022-25776	Prior to the patched version, logged in users of Mautic are able to access areas of the application that they should be prevented from accessing. Users could potentially access sensitive data such as names and surnames, company names and stage names.	8.3	More Details
CVE-2024-47000	Zitadel is an open source identity management platform. ZITADEL's user account deactivation mechanism did not work correctly with service accounts. Deactivated service accounts retained the ability to request tokens, which could lead to unauthorized access to applications and resources. Versions 2.62.1, 2.61.1, 2.60.2, 2.59.3, 2.58.5, 2.57.5, 2.56.6, 2.55.8, and 2.54.10 have been released which address this issue. Users are advised t upgrade. Users unable to upgrade may instead of deactivating the service account, consider creating new credentials and replacing the old ones wherever they are used. This effectively prevents the deactivated service account from being utilized. Be sure to revoke all existing authentication keys associated with the service account and to rotate the service account's password.	8.1	More Details
CVE-2024-41721	An insufficient boundary validation in the USB code could lead to an out-of-bounds read on the heap, which could potentially lead to an arbitrary write and remote code execution.	8.1	More Details
CVE-2024-8890	An attacker with access to the network where the CIRCUTOR Q-SMT is located in its firmware version 1.0.4, could obtain legitimate credentials or steal sessions due to the fact that the device only implements the HTTP protocol. This fact prevents a secure communication channel from being established.	8.0	More Details
CVE-2018-20072	Insufficient data validation in PDF in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform out of bounds memory access via a crafted PDF file. (Chromium security severity: Low)	7.8	More Details
CVE-2022-25770	Mautic allows you to update the application via an upgrade script. The upgrade logic isn't shielded off correctly, which may lead to vulnerable situation. This vulnerability is mitigated by the fact that Mautic needs to be installed in a certain way to be vulnerable.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46741	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: Fix double free of 'buf' in error path smatch warning: drivers/misc/fastrpc.c:1926 fastrpc_req_mmap() error: double free of 'buf' In fastrpc_req_mmap() error path, the fastrpc buffer is freed in fastrpc_req_munmap_impl() if unmap is successful. But in the end, there is an unconditional call to fastrpc_buf_free(). So the above case triggers the double free of fastrpc buf.	7.8	More Details
CVE-2024-46740	In the Linux kernel, the following vulnerability has been resolved: binder: fix UAF caused by offsets overwrite Binder objects are processed and copied individually into the target buffer during transactions. Any raw data in-between these objects is copied as well. However, this raw data copy lacks an out-of-bounds check. If the raw data exceeds the data section size then the copy overwrites the offsets section. This eventually triggers an error that attempts to unwind the processed objects. However, at this point the offsets used to index these objects are now corrupted. Unwinding with corrupted offsets can result in decrements of arbitrary nodes and lead to their premature release. Other users of such nodes are left with a dangling pointer triggering a use-after-free. This issue is made evident by the following KASAN report (trimmed): == BUG: KASAN: slab-use-after-free in _raw_spin_lock+0xe4/0x19c Write of size 4 at addr ffff47fc91598f04 by task binder-util/743 CPU: 9 UID: 0 PID: 743 Comm: binder-util Not tainted 6.11.0-rc4 #1 Hardware name: linux,dummy-virt (DT) Call trace: _raw_spin_lock+0xe4/0x19c binder_free_buf+0x128/0x434 binder_thread_write+0x8a4/0x3260 binder_ioctl+0x18f0/0x258c [...] Allocated by task 743: __kmalloc_cache_noprof+0x110/0x270 binder_new_node+0x50/0x700 binder_transaction+0x413c/0x6da8 binder_thread_write+0x978/0x3260 binder_ioctl+0x18f0/0x258c [...] Freed by task 745: kfree+0xbc/0x208 binder_thread_read+0x1c5c/0x37d4 binder_ioctl+0x16d8/0x258c [...] == To avoid this issue, let's check that the raw data copy is within the boundaries of the data section.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46746	In the Linux kernel, the following vulnerability has been resolved: HID: amd_sfh: free driver_data after destroying hid device HID driver callbacks aren't called anymore once hid_destroy_device() has been called. Hence, hid driver_data should be freed only after the hid_destroy_device() function returned as driver_data is used in several callbacks. I observed a crash with kernel 6.10.0 on my T14s Gen 3, after enabling KASAN to debug memory allocation, I got this output: [13.050438] == [13.054060] BUG: KASAN: slab-use-after-free in amd_sfh_get_report+0x3ec/0x530 [amd_sfh] [13.054809] psmouse serio1: trackpoint: Synaptics TrackPoint firmware: 0x02, buttons: 3/3 [13.056432] Read of size 8 at addr ffff88813152f408 by task (udev-worker)/479 [13.060970] CPU: 5 PID: 479 Comm: (udev-worker) Not tainted 6.10.0-arch1-2 #1 893bb55d7f0073f25c46adbb49eb3785fefd74b0 [13.063978] Hardware name: LENOVO 21CQCTO1WW/21CQCTO1WW, BIOS R22ET70W (1.40) 03/21/2024 [13.067860] Call Trace: [13.069383] input: TPPS/2 Synaptics TrackPoint as /devices/platform/i8042/serio1/input/input8 [13.071486] <TASK> [13.071492] dump_stack_lvl+0x5d/0x80 [13.074870] snd_hda_intel 0000:33:00.6: enabling device (0000 -> 0002) [13.078296] ? amd_sfh_get_report+0x3ec/0x530 [amd_sfh 05f43221435b5205f734cd9da29399130f398a38] [13.082199] print_report+0x174/0x505 [13.085776] ? __pfx__raw_spin_lock_irqsave+0x10/0x10 [13.089367] ? srso_alias_return_thunk+0x5/0xfbef5 [13.093255] ? amd_sfh_get_report+0x3ec/0x530 [amd_sfh 05f43221435b5205f734cd9da29399130f398a38] [13.097464] kasan_report+0xc8/0x150 [13.101461] ? amd_sfh_get_report+0x3ec/0x530 [amd_sfh 05f43221435b5205f734cd9da29399130f398a38] [13.105802] amd_sfh_get_report+0x3ec/0x530 [amd_sfh 05f43221435b5205f734cd9da29399130f398a38] [13.110303] amdtp_hid_request+0xb8/0x110 [amd_sfh 05f43221435b5205f734cd9da29399130f398a38] [13.114879] ? srso_alias_return_thunk+0x5/0xfbef5 [13.119450] sensor_hub_get_feature+0x1d3/0x540 [hid_sensor_hub 3f13be3016ff415bea03008d45d99da837ee3082] [13.124097] hid_sensor_parse_common_attributes+0x4d0/0xad0 [hid_sensor_iio_common c3a5cbe93969c28b122609768bbe23efe52eb8f5] [13.127404] ? srso_alias_return_thunk+0x5/0xfbef5 [13.131925] ? __pfx_hid_sensor_parse_common_attributes+0x10/0x10 [hid_sensor_iio_common c3a5cbe93969c28b122609768bbe23efe52eb8f5] [13.136455] ? _raw_spin_lock_irqsave+0x96/0xf0 [13.140197] ? __pfx__raw_spin_lock_irqsave+0x10/0x10 [13.143602] ? devm_iio_device_alloc+0x34/0x50 [industrialio 3d261d5e5765625d2b052be40e526d62b1d2123b] [13.147234] ? srso_alias_return_thunk+0x5/0xfbef5 [13.150446] ? __devm_add_action+0x167/0x1d0 [13.155061] hid_gyro_3d_probe+0x120/0x7f0 [hid_sensor_gyro_3d 63da36a143b775846ab2dbb86c343b401b5e3172] [13.158581] ? srso_alias_return_thunk+0x5/0xfbef5 [13.161814] platform_probe+0xa2/0x150 [13.165029] really_probe+0x1e3/0x8a0 [13.168243] __driver_probe_device+0x18c/0x370 [13.171500] driver_probe_device+0x4a/0x120 [13.175000] __driver_attach+0x190/0x4a0 [13.178521] ? __pfx___driver_attach+0x10/0x10 [13.181771] bus_for_each_dev+0x106/0x180 [13.185033] ? __pfx__raw_spin_lock+0x10/0x10 [13.188229] ? __pfx_bus_for_each_dev+0x10/0x10 [13.191446] ? srso_alias_return_thunk+0x5/0xfbef5 [13.194382] bus_add_driver+0x29e/0x4d0 [13.197328] driver_register+0x1a5/0x360 [13.200283] ? __pfx_hid_gyro_3d_platform_driver_init+0x10/0x10 [hid_sensor_gyro_3d 63da36a143b775846ab2dbb86c343b401b5e3172] [13.203362] do_one_initcall+0xa7/0x380 [13.206432] ? __pfx_do_one_initcall+0x10/0x10 [13.210175] ? srso_alias_return_thunk+0x5/0xfbef5 [13.213211] ? kasan_unpoison+0x44/0x70 [13.216688] do_init_module+0x238/0x750 [13.2196 ---truncated---	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46756	In the Linux kernel, the following vulnerability has been resolved: hwmon: (w83627ehf) Fix underflows seen when writing limit attributes DIV_ROUND_CLOSEST() after kstrtol() results in an underflow if a large negative number such as -9223372036854775808 is provided by the user. Fix it by reordering clamp_val() and DIV_ROUND_CLOSEST() operations.	7.8	More Details
CVE-2024-46738	In the Linux kernel, the following vulnerability has been resolved: VMCI: Fix use-after-free when removing resource in vmci_resource_remove() When removing a resource from vmci_resource_table in vmci_resource_remove(), the search is performed using the resource handle by comparing context and resource fields. It is possible though to create two resources with different types but same handle (same context and resource fields). When trying to remove one of the resources, vmci_resource_remove() may not remove the intended one, but the object will still be freed as in the case of the datagram type in vmci_datagram_destroy_handle(). vmci_resource_table will still hold a pointer to this freed resource leading to a use-after-free vulnerability. BUG: KASAN: use-after-free in vmci_handle_is_equal include/linux/vmw_vmci_defs.h:142 [inline] BUG: KASAN: use-after-free in vmci_resource_remove+0x3a1/0x410 drivers/misc/vmw_vmci/vmci_resource.c:147 Read of size 4 at addr ffff88801c16d800 by task syz-executor197/1592 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x82/0xa9 lib/dump_stack.c:106 print_address_description.constprop.0+0x21/0x366 mm/kasan/report.c:239 __kasan_report.cold+0x7f/0x132 mm/kasan/report.c:425 kasan_report+0x38/0x51 mm/kasan/report.c:442 vmci_handle_is_equal include/linux/vmw_vmci_defs.h:142 [inline] vmci_resource_remove+0x3a1/0x410 drivers/misc/vmw_vmci/vmci_resource.c:147 vmci_qp_broker_detach+0x89a/0x11b9 drivers/misc/vmw_vmci/vmci_queue_pair.c:2182 ctx_free_ctx+0x473/0xbe1 drivers/misc/vmw_vmci/vmci_context.c:444 kref_put include/linux/kref.h:65 [inline] vmci_ctx_put drivers/misc/vmw_vmci/vmci_context.c:497 [inline] vmci_ctx_destroy+0x170/0x1d6 drivers/misc/vmw_vmci/vmci_context.c:195 vmci_host_close+0x125/0x1ac drivers/misc/vmw_vmci/vmci_host.c:143 __fput+0x261/0xa34 fs/file_table.c:282 task_work_run+0xf0/0x194 kernel/task_work.c:164 tracehook_notify_resume include/linux/tracehook.h:189 [inline] exit_to_user_mode_loop+0x184/0x189 kernel/entry/common.c:187 exit_to_user_mode_prepare+0x11b/0x123 kernel/entry/common.c:220 __syscall_exit_to_user_mode_work kernel/entry/common.c:302 [inline] syscall_exit_to_user_mode+0x18/0x42 kernel/entry/common.c:313 do_syscall_64+0x41/0x85 arch/x86/entry/common.c:86 entry_SYSCALL_64_after_hwframe+0x6e/0x0 This change ensures the type is also checked when removing the resource from vmci_resource_table in vmci_resource_remove().	7.8	More Details
CVE-2024-46758	In the Linux kernel, the following vulnerability has been resolved: hwmon: (lm95234) Fix underflows seen when writing limit attributes DIV_ROUND_CLOSEST() after kstrtol() results in an underflow if a large negative number such as -9223372036854775808 is provided by the user. Fix it by reordering clamp_val() and DIV_ROUND_CLOSEST() operations.	7.8	More Details
CVE-2024-46757	In the Linux kernel, the following vulnerability has been resolved: hwmon: (nct6775-core) Fix underflows seen when writing limit attributes DIV_ROUND_CLOSEST() after kstrtol() results in an underflow if a large negative number such as -9223372036854775808 is provided by the user. Fix it by reordering clamp_val() and DIV_ROUND_CLOSEST() operations.	7.8	More Details
CVE-2024-46725	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix out-of-bounds write warning Check the ring type value to fix the out-of-bounds write warning	7.8	More Details
CVE-2024-46759	In the Linux kernel, the following vulnerability has been resolved: hwmon: (adc128d818) Fix underflows seen when writing limit attributes DIV_ROUND_CLOSEST() after kstrtol() results in an underflow if a large negative number such as -9223372036854775808 is provided by the user. Fix it by reordering clamp_val() and DIV_ROUND_CLOSEST() operations.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-38016	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2024-46744	In the Linux kernel, the following vulnerability has been resolved: Squashfs: sanity check symbolic link size Syzkiller reports a "KMSAN: uninit-value in pick_link" bug. This is caused by an uninitialised page, which is ultimately caused by a corrupted symbolic link size read from disk. The reason why the corrupted symlink size causes an uninitialised page is due to the following sequence of events: 1. squashfs_read_inode() is called to read the symbolic link from disk. This assigns the corrupted value 3875536935 to inode->i_size. 2. Later squashfs_symlink_read_folio() is called, which assigns this corrupted value to the length variable, which being a signed int, overflows producing a negative number. 3. The following loop that fills in the page contents checks that the copied bytes is less than length, which being negative means the loop is skipped, producing an uninitialised page. This patch adds a sanity check which checks that the symbolic link size is not larger than expected. -- V2: fix spelling mistake.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46766	In the Linux kernel, the following vulnerability has been resolved: ice: move netif_queue_set_napi to rtnl-protected sections Currently, netif_queue_set_napi() is called from ice_vsi_rebuild() that is not rtnl-locked when called from the reset. This creates the need to take the rtnl_lock just for a single function and complicates the synchronization with .ndo_bpf. At the same time, there no actual need to fill napi-to-queue information at this exact point. Fill napi-to-queue information when opening the VSI and clear it when the VSI is being closed. Those routines are already rtnl-locked. Also, rewrite napi-to-queue assignment in a way that prevents inclusion of XDP queues, as this leads to out-of-bounds writes, such as one below. [+0.000004] BUG: KASAN: slab-out-of-bounds in netif_queue_set_napi+0x1c2/0x1e0 [+0.000012] Write of size 8 at addr ffff889881727c80 by task bash/7047 [+0.000006] CPU: 24 PID: 7047 Comm: bash Not tainted 6.10.0-rc2+ #2 [+0.000004] Hardware name: Intel Corporation S2600WFT/S2600WFT, BIOS SE5C620.86B.02.01.0014.082620210524 08/26/2021 [+0.000003] Call Trace: [+0.000003] <TASK> [+0.000002] dump_stack_lvl+0x60/0x80 [+0.000007] print_report+0xce/0x630 [+0.000007] ? __pfx__raw_spin_lock_irqsave+0x10/0x10 [+0.000007] ? __virt_addr_valid+0x1c9/0x2c0 [+0.000005] ? netif_queue_set_napi+0x1c2/0x1e0 [+0.000003] kasan_report+0xe9/0x120 [+0.000004] ? netif_queue_set_napi+0x1c2/0x1e0 [+0.000004] netif_queue_set_napi+0x1c2/0x1e0 [+0.000005] ice_vsi_close+0x161/0x670 [ice] [+0.000114] ice_dis_vsi+0x22f/0x270 [ice] [+0.000095] ice_pf_dis_all_vsi.constprop.0+0xae/0x1c0 [ice] [+0.000086] ice_prepare_for_reset+0x299/0x750 [ice] [+0.000087] pci_dev_save_and_disable+0x82/0xd0 [+0.000006] pci_reset_function+0x12d/0x230 [+0.000004] reset_store+0xa0/0x100 [+0.000006] ? __pfx_reset_store+0x10/0x10 [+0.000002] ? __pfx_mutex_lock+0x10/0x10 [+0.000004] ? __check_object_size+0x4c1/0x640 [+0.000007] kernfs_fop_write_iter+0x30b/0x4a0 [+0.000006] vfs_write+0x5d6/0xdf0 [+0.000005] ? fd_install+0x180/0x350 [+0.000005] ? __pfx_vfs_write+0x10/0xA10 [+0.000004] ? do_fcntl+0x52c/0xcd0 [+0.000004] ? kasan_save_track+0x13/0x60 [+0.000003] ? kasan_save_free_info+0x37/0x60 [+0.000006] ksys_write+0xfa/0x1d0 [+0.000003] ? __pfx_ksys_write+0x10/0x10 [+0.000002] ? __x64_sys_fcntl+0x121/0x180 [+0.000004] ? _raw_spin_lock+0x87/0xe0 [+0.000005] do_syscall_64+0x80/0x170 [+0.000007] ? _raw_spin_lock+0x87/0xe0 [+0.000004] ? __pfx__raw_spin_lock+0x10/0x10 [+0.000003] ? file_close_fd_locked+0x167/0x230 [+0.000005] ? syscall_exit_to_user_mode+0x7d/0x220 [+0.000005] ? do_syscall_64+0x8c/0x170 [+0.000004] ? do_syscall_64+0x8c/0x170 [+0.000003] ? do_syscall_64+0x8c/0x170 [+0.000003] ? fput+0x1a/0x2c0 [+0.000004] ? filp_close+0x19/0x30 [+0.000004] ? do_dup2+0x25a/0x4c0 [+0.000004] ? __x64_sys_dup2+0x6e/0x2e0 [+0.000002] ? syscall_exit_to_user_mode+0x7d/0x220 [+0.000004] ? do_syscall_64+0x8c/0x170 [+0.000003] ? __count_memcg_events+0x113/0x380 [+0.000005] ? handle_mm_fault+0x136/0x820 [+0.000005] ? do_user_addr_fault+0x444/0xa80 [+0.000004] ? clear_bhb_loop+0x25/0x80 [+0.000004] ? clear_bhb_loop+0x25/0x80 [+0.000002] entry_SYSCALL_64_after_hwframe+0x76/0x7e [+0.000005] RIP: 0033:0x7f2033593154	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46782	In the Linux kernel, the following vulnerability has been resolved: ila: call nf_unregister_net_hooks() sooner syzbot found an use-after-free Read in ila_nf_input [1] Issue here is that ila_xlat_exit_net() frees the rhashtable, then call nf_unregister_net_hooks(). It should be done in the reverse way, with a synchronize_rcu(). This is a good match for a pre_exit() method. [1] BUG: KASAN: use-after-free in rht_key_hashfn include/linux/rhashtable.h:159 [inline] BUG: KASAN: use-after-free in __rhashtable_lookup include/linux/rhashtable.h:604 [inline] BUG: KASAN: use-after-free in rhashtable_lookup include/linux/rhashtable.h:646 [inline] BUG: KASAN: use-after-free in rhashtable_lookup_fast+0x77a/0x9b0 include/linux/rhashtable.h:672 Read of size 4 at addr ffff888064620008 by task ksoftirqd/0/16 CPU: 0 UID: 0 PID: 16 Comm: ksoftirqd/0 Not tainted 6.11.0-rc4-syzkaller-00238-g2ad6d23f465a #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 rht_key_hashfn include/linux/rhashtable.h:159 [inline] __rhashtable_lookup include/linux/rhashtable.h:604 [inline] rhashtable_lookup include/linux/rhashtable.h:646 [inline] rhashtable_lookup_fast+0x77a/0x9b0 include/linux/rhashtable.h:672 ila_lookup_wildcards net/ipv6/ila/ila_xlat.c:132 [inline] ila_xlat_addr net/ipv6/ila/ila_xlat.c:652 [inline] ila_nf_input+0x1fe/0x3c0 net/ipv6/ila/ila_xlat.c:190 nf_hook_entry_hookfn include/linux/netfilter.h:154 [inline] nf_hook_slow+0xc3/0x220 net/netfilter/core.c:626 nf_hook include/linux/netfilter.h:269 [inline] NF_HOOK+0x29e/0x450 include/linux/netfilter.h:312 __netif_receive_skb_one_core net/core/dev.c:5661 [inline] __netif_receive_skb+0x1ea/0x650 net/core/dev.c:5775 process_backlog+0x662/0x15b0 net/core/dev.c:6108 __napi_poll+0xcb/0x490 net/core/dev.c:6772 napi_poll net/core/dev.c:6841 [inline] net_rx_action+0x89b/0x1240 net/core/dev.c:6963 handle_softirqs+0x2c4/0x970 kernel/softirq.c:554 run_ksoftirqd+0xca/0x130 kernel/softirq.c:928 smpboot_thread_fn+0x544/0xa30 kernel/smpboot.c:164 kthread+0x2f0/0x390 kernel/kthread.c:389 ret_from_fork+0x4b/0x80 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:244 </TASK> The buggy address belongs to the physical page: page: refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x64620 flags: 0xfff00000000000(node=0|zone=1|lastcpupid=0x7ff) page_type: 0xbfffffff(buddy) raw: 00fff00000000000 ffffea0000959608 ffffea00019d9408 0000000000000000 raw: 0000000000000000 0000000000000003 00000000bfffffff 0000000000000000 page dumped because: kasan: bad access detected page_owner tracks the page as freed page last allocated via order 3, migratetype Unmovable, gfp_mask 0x52dc0(GFP_KERNEL|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_ZERO), pid 5242, tgid 5242 (syz-executor), ts 73611328570, free_ts 618981657187 set_page_owner include/linux/page_owner.h:32 [inline] post_alloc_hook+0x1f3/0x230 mm/page_alloc.c:1493 prep_new_page mm/page_alloc.c:1501 [inline] get_page_from_freelist+0x2e4c/0x2f10 mm/page_alloc.c:3439 __alloc_pages_noprof+0x256/0x6c0 mm/page_alloc.c:4695 __alloc_pages_node_noprof include/linux/gfp.h:269 [inline] alloc_pages_node_noprof include/linux/gfp.h:296 [inline] ___kmalloc_large_node+0x8b/0x1d0 mm/slub.c:4103 __kmalloc_large_node_noprof+0x1a/0x80 mm/slub.c:4130 __do_kmalloc_node mm/slub.c:4146 [inline] __kmalloc_node_noprof+0x2d2/0x440 mm/slub.c:4164 __kvmalloc_node_noprof+0x72/0x190 mm/util.c:650 bucket_table_alloc lib/rhashtable.c:186 [inline] rhashtable_init_noprof+0x534/0xa60 lib/rhashtable.c:1071 ila_xlat_init_net+0xa0/0x110 net/ipv6/ila/ila_xlat.c:613 ops_ini ---truncated---	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46786	In the Linux kernel, the following vulnerability has been resolved: fscache: delete fscache_cookie_lru_timer when fscache exits to avoid UAF The fscache_cookie_lru_timer is initialized when the fscache module is inserted, but is not deleted when the fscache module is removed. If timer_reduce() is called before removing the fscache module, the fscache_cookie_lru_timer will be added to the timer list of the current cpu. Afterwards, a use-after-free will be triggered in the softIRQ after removing the fscache module, as follows: == BUG: unable to handle page fault for address: fffffbfff803c9e9 PF: supervisor read access in kernel mode PF: error_code(0x0000) - not-present page PGD 21ffea067 P4D 21ffea067 PUD 21ffe6067 PMD 110a7c067 PTE 0 Oops: Oops: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 1 UID: 0 PID: 0 Comm: swapper/1 Tainted: G W 6.11.0-rc3 #855 Tainted: [W]=WARN RIP: 0010:__run_timer_base.part.0+0x254/0x8a0 Call Trace: <IRQ> tmigr_handle_remote_up+0x627/0x810 __walk_groups.isra.0+0x47/0x140 tmigr_handle_remote+0x1fa/0x2f0 handle_softirqs+0x180/0x590 irq_exit_rcu+0x84/0xb0 sysvec_apic_timer_interrupt+0x6e/0x90 </IRQ> <TASK> asm_sysvec_apic_timer_interrupt+0x1a/0x20 RIP: 0010:default_idle+0xf/0x20 default_idle_call+0x38/0x60 do_idle+0x2b5/0x300 cpu_startup_entry+0x54/0x60 start_secondary+0x20d/0x280 common_startup_64+0x13e/0x148 </TASK> Modules linked in: [last unloaded: netfs] == Therefore delete fscache_cookie_lru_timer when removing the fscahe module.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46796	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix double put of @cfile in smb2_set_path_size() If smb2_compound_op() is called with a valid @cfile and returned -EINVAL, we need to call cifs_get_writable_path() before retrying it as the reference of @cfile was already dropped by previous call. This fixes the following KASAN splat when running fstests generic/013 against Windows Server 2022: CIFS: Attempting to mount //w22-fs0/scratch run fstests generic/013 at 2024-09-02 19:48:59 == BUG: KASAN: slab-use-after-free in detach_if_pending+0xab/0x200 Write of size 8 at addr ffff88811f1a3730 by task kworker/3:2/176 CPU: 3 UID: 0 PID: 176 Comm: kworker/3:2 Not tainted 6.11.0-rc6 #2 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 Workqueue: cifsoplockd cifs_oplock_break [cifs] Call Trace: <TASK> dump_stack_lvl+0x5d/0x80 ? detach_if_pending+0xab/0x200 print_report+0x156/0x4d9 ? detach_if_pending+0xab/0x200 ? __virt_addr_valid+0x145/0x300 ? __phys_addr+0x46/0x90 ? detach_if_pending+0xab/0x200 kasan_report+0xda/0x110 ? detach_if_pending+0xab/0x200 detach_if_pending+0xab/0x200 timer_delete+0x96/0xe0 ? __pfx_timer_delete+0x10/0x10 ? rcu_is_watching+0x20/0x50 try_to_grab_pending+0x46/0x3b0 __cancel_work+0x89/0x1b0 ? __pfx___cancel_work+0x10/0x10 ? kasan_save_track+0x14/0x30 cifs_close_deferred_file+0x110/0x2c0 [cifs] ? __pfx_cifs_close_deferred_file+0x10/0x10 [cifs] ? __pfx_down_read+0x10/0x10 cifs_oplock_break+0x4c1/0xa50 [cifs] ? __pfx_cifs_oplock_break+0x10/0x10 [cifs] ? lock_is_held_type+0x85/0xf0 ? mark_held_locks+0x1a/0x90 process_one_work+0x4c6/0x9f0 ? find_held_lock+0x8a/0xa0 ? __pfx_process_one_work+0x10/0x10 ? lock_acquired+0x220/0x550 ? __list_add_valid_or_report+0x37/0x100 worker_thread+0x2e4/0x570 ? __kthread_parkme+0xd1/0xf0 ? __pfx_worker_thread+0x10/0x10 kthread+0x17f/0x1c0 ? kthread+0xda/0x1c0 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x31/0x60 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> Allocated by task 1118: kasan_save_stack+0x30/0x50 kasan_save_track+0x14/0x30 __kasan_kmalloc+0xaa/0xb0 cifs_new_fileinfo+0xc8/0x9d0 [cifs] cifs_atomic_open+0x467/0x770 [cifs] lookup_open.isra.0+0x665/0x8b0 path_openat+0x4c3/0x1380 do_filp_open+0x167/0x270 do_sys_openat2+0x129/0x160 __x64_sys_creat+0xad/0xe0 do_syscall_64+0xbb/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 83: kasan_save_stack+0x30/0x50 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3b/0x70 poison_slab_object+0xe9/0x160 __kasan_slab_free+0x32/0x50 kfree+0xf2/0x300 process_one_work+0x4c6/0x9f0 worker_thread+0x2e4/0x570 kthread+0x17f/0x1c0 ret_from_fork+0x31/0x60 ret_from_fork_asm+0x1a/0x30 Last potentially related work creation: kasan_save_stack+0x30/0x50 __kasan_record_aux_stack+0xad/0xc0 insert_work+0x29/0xe0 __queue_work+0x5ea/0x760 queue_work_on+0x6d/0x90 _cifsFileInfo_put+0x3f6/0x770 [cifs] smb2_compound_op+0x911/0x3940 [cifs] smb2_set_path_size+0x228/0x270 [cifs] cifs_set_file_size+0x197/0x460 [cifs] cifs_setattr+0xd9c/0x14b0 [cifs] notify_change+0x4e3/0x740 do_truncate+0xfa/0x180 vfs_truncate+0x195/0x200 __x64_sys_truncate+0x109/0x150 do_syscall_64+0xbb/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46798	In the Linux kernel, the following vulnerability has been resolved: ASoC: dapm: Fix UAF for snd_soc_pcm_runtime object When using kernel with the following extra config, - CONFIG_KASAN=y - CONFIG_KASAN_GENERIC=y - CONFIG_KASAN_INLINE=y - CONFIG_KASAN_VMALLOC=y - CONFIG_FRAME_WARN=4096 kernel detects that snd_pcm_suspend_all() access a freed 'snd_soc_pcm_runtime' object when the system is suspended, which leads to a use-after-free bug: [52.047746] BUG: KASAN: use-after-free in snd_pcm_suspend_all+0x1a8/0x270 [52.047765] Read of size 1 at addr ffff0000b9434d50 by task systemd-sleep/2330 [52.047785] Call trace: [52.047787] dump_backtrace+0x0/0x3c0 [52.047794] show_stack+0x34/0x50 [52.047797] dump_stack_lvl+0x68/0x8c [52.047802] print_address_description.constprop.0+0x74/0x2c0 [52.047809] kasan_report+0x210/0x230 [52.047815] __asan_report_load1_noabort+0x3c/0x50 [52.047820] snd_pcm_suspend_all+0x1a8/0x270 [52.047824] snd_soc_suspend+0x19c/0x4e0 The snd_pcm_sync_stop() has a NULL check on 'substream->runtime' before making any access. So we need to always set 'substream->runtime' to NULL everytime we kfree() it.	7.8	More Details
CVE-2024-46800	In the Linux kernel, the following vulnerability has been resolved: sch/netem: fix use after free in netem_dequeue If netem_dequeue() enqueues packet to inner qdisc and that qdisc returns __NET_XMIT_STOLEN. The packet is dropped but qdisc_tree_reduce_backlog() is not called to update the parent's q.qlen, leading to the similar use-after-free as Commit e04991a48dbaf382 ("netem: fix return value if duplicate enqueue fails") Commands to trigger KASAN UaF: ip link add type dummy ip link set lo up ip link set dummy0 up tc qdisc add dev lo parent root handle 1: drr tc filter add dev lo parent 1: basic classid 1:1 tc class add dev lo classid 1:1 drr tc qdisc add dev lo parent 1:1 handle 2: netem tc qdisc add dev lo parent 2: handle 3: drr tc filter add dev lo parent 3: basic classid 3:1 action mirred egress redirect dev dummy0 tc class add dev lo classid 3:1 drr ping -c1 -W0.01 localhost # Trigger bug tc class del dev lo classid 1:1 tc class add dev lo classid 1:1 drr ping -c1 -W0.01 localhost # UaF	7.8	More Details
CVE-2024-45858	An arbitrary code execution vulnerability exists in versions 0.2.9 up to 0.5.10 of the Guardrails AI Guardrails framework because of the way it validates XML files. If a victim user loads a maliciously crafted XML file containing Python code, the code will be passed to an eval function, causing it to execute on the user's machine.	7.8	More Details
CVE-2024-7018	Heap buffer overflow in PDF in Google Chrome prior to 124.0.6367.78 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium)	7.8	More Details
CVE-2024-8698	A flaw exists in the SAML signature validation method within the Keycloak XMLSignatureUtil class. The method incorrectly determines whether a SAML signature is for the full document or only for specific assertions based on the position of the signature in the XML document, rather than the Reference element used to specify the signed element. This flaw allows attackers to create crafted responses that can bypass the validation, potentially leading to privilege escalation or impersonation attacks.	7.7	More Details
CVE-2024-46987	Camaleon CMS is a dynamic and advanced content management system based on Ruby on Rails. A path traversal vulnerability accessible via MediaController's download_private_file method allows authenticated users to download any file on the web server Camaleon CMS is running on (depending on the file permissions). This issue may lead to Information Disclosure. This issue has been addressed in release version 2.8.2. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.7	More Details
CVE-2024-46639	A cross-site scripting (XSS) vulnerability in HelpDeskZ v2.0.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name text field of Custom Fields message box.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-41228	A symlink following vulnerability in the pouch cp function of AliyunContainerService pouch v1.3.1 allows attackers to escalate privileges and write arbitrary files.	7.6	More Details
CVE-2024-42346	Galaxy is a free, open-source system for analyzing data, authoring workflows, training and education, publishing tools, managing infrastructure, and more. The editor visualization, /visualizations endpoint, can be used to store HTML tags and trigger javascript execution upon edit operation. All supported branches of Galaxy (and more back to release_20.05) were amended with the supplied patches. Users are advised to upgrade. There are no known workarounds for this vulnerability.	7.6	More Details
CVE-2024-39339	A vulnerability has been discovered in all versions of Smartplay headunits, which are widely used in Suzuki and Toyota cars. This misconfiguration can lead to information disclosure, leaking sensitive details such as diagnostic log traces, system logs, headunit passwords, and personally identifiable information (PII). The exposure of such information may have serious implications for user privacy and system integrity.	7.5	More Details
CVE-2024-46565	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sSrvName parameter at service.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46557	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sProfileName parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46558	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the newProname parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46559	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sBPA_UsrNme parameter at inet15.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46560	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the pub_key parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46648	eNMS 4.4.0 to 4.7.1 is vulnerable to Directory Traversal via scan_folder.	7.5	More Details
CVE-2024-46561	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the queryret parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46564	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sProfileName parameter at fextobj.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46649	eNMS up to 4.7.1 is vulnerable to Directory Traversal via download/folder.	7.5	More Details
CVE-2024-46555	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the pb parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46566	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sAppName parameter at sslapp.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46567	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the iProfileIdx parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46568	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sPeerId parameter at vpn.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46571	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sPPPSrvNm parameter at fwuser.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2023-30464	CoreDNS through 1.10.1 enables attackers to achieve DNS cache poisoning and inject fake responses via a birthday attack.	7.5	More Details
CVE-2024-46580	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the fid parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46556	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sInRCSecret0 parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46554	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the profname parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46582	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sSrvAddr parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46553	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the ipaddrmsk%d parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46645	eNMS 4.0.0 is vulnerable to Directory Traversal via get_tree_files.	7.5	More Details
CVE-2023-28451	An issue was discovered in Technitium 11.0.2. There is a vulnerability (called BadDNS) in DNS resolving software, which triggers a resolver to ignore valid responses, thus causing DoS (denial of service) for normal resolution. The effects of an exploit would be widespread and highly impactful, because the attacker could just forge a response targeting the source port of a vulnerable resolver without the need to guess the correct TXID.	7.5	More Details
CVE-2023-28452	An issue was discovered in CoreDNS through 1.10.1. There is a vulnerability in DNS resolving software, which triggers a resolver to ignore valid responses, thus causing denial of service for normal resolution. In an exploit, the attacker could just forge a response targeting the source port of a vulnerable resolver without the need to guess the correct TXID.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28455	An issue was discovered in Technitium through 11.0.2. The forwarding mode enables attackers to create a query loop using Technitium resolvers, launching amplification attacks and causing potential DoS.	7.5	More Details
CVE-2023-28456	An issue was discovered in Technitium through 11.0.2. It enables attackers to launch amplification attacks (3 times more than other "golden model" software like BIND) and cause potential DoS.	7.5	More Details
CVE-2024-46985	DataEase is an open source data visualization analysis tool. Prior to version 2.10.1, there is an XML external entity injection vulnerability in the static resource upload interface of DataEase. An attacker can construct a payload to implement intranet detection and file reading. The vulnerability has been fixed in v2.10.1.	7.5	More Details
CVE-2023-28457	An issue was discovered in Technitium through 11.0.3. It enables attackers to conduct a DNS cache poisoning attack and inject fake responses within 1 second, which is impactful.	7.5	More Details
CVE-2023-49203	Technitium 11.5.3 allows remote attackers to cause a denial of service (bandwidth amplification) because the DNSBomb manipulation causes accumulation of low-rate DNS queries such that there is a large-sized response in a burst of traffic.	7.5	More Details
CVE-2024-36980	An out-of-bounds read vulnerability exists in the OpenPLC Runtime EtherNet/IP PCCC parser functionality of OpenPLC_v3 b4702061dc14d1024856f71b4543298d77007b88. A specially crafted network request can lead to denial of service. An attacker can send a series of EtherNet/IP requests to trigger this vulnerability.This is the first instance of the incorrect comparison.	7.5	More Details
CVE-2024-36981	An out-of-bounds read vulnerability exists in the OpenPLC Runtime EtherNet/IP PCCC parser functionality of OpenPLC_v3 b4702061dc14d1024856f71b4543298d77007b88. A specially crafted network request can lead to denial of service. An attacker can send a series of EtherNet/IP requests to trigger this vulnerability.This is the final instance of the incorrect comparison.	7.5	More Details
CVE-2024-39589	Multiple invalid pointer dereference vulnerabilities exist in the OpenPLC Runtime EtherNet/IP parser functionality of OpenPLC_v3 16bf8bac1a36d95b73e7b8722d0edb8b9c5bb56a. A specially crafted EtherNet/IP request can lead to denial of service. An attacker can send a series of EtherNet/IP requests to trigger these vulnerabilities.This instance of the vulnerability occurs within the `Protected_Logical_Read_Reply` function	7.5	More Details
CVE-2024-39590	Multiple invalid pointer dereference vulnerabilities exist in the OpenPLC Runtime EtherNet/IP parser functionality of OpenPLC_v3 16bf8bac1a36d95b73e7b8722d0edb8b9c5bb56a. A specially crafted EtherNet/IP request can lead to denial of service. An attacker can send a series of EtherNet/IP requests to trigger these vulnerabilities.This instance of the vulnerability occurs within the `Protected_Logical_Write_Reply` function	7.5	More Details
CVE-2024-46550	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the CGIbyFieldName parameter at chglog.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46551	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sBPA_Pwd parameter at inet15.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46552	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sStRtMskShow parameter at ipstrt.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46581	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sProfName parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-45807	Envoy is a cloud-native high-performance edge/middle/service proxy. Envoy's 1.31 is using `oghttp` as the default HTTP/2 codec, and there are potential bugs around stream management in the codec. To resolve this Envoy will switch off the `oghttp2` by default. The impact of this issue is that envoy will crash. This issue has been addressed in release version 1.31.2. All users are advised to upgrade. There are no known workarounds for this issue.	7.5	More Details
CVE-2024-47220	An issue was discovered in the WEBrick toolkit through 1.8.1 for Ruby. It allows HTTP request smuggling by providing both a Content-Length header and a Transfer-Encoding header, e.g., "GET /admin HTTP/1.1\r\n" inside of a "POST /user HTTP/1.1\r\n" request. NOTE: the supplier's position is "Webrick should not be used in production."	7.5	More Details
CVE-2024-46596	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sAct parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-8287	Anbox Management Service, in versions 1.17.0 through 1.23.0, does not validate the TLS certificate provided to it by the Anbox Stream Agent. An attacker must be able to machine-in-the-middle the Anbox Stream Agent from within an internal network before they can attempt to take advantage of this.	7.5	More Details
CVE-2024-34057	Triangle Microworks TMW IEC 61850 Client source code libraries before 12.2.0 lack a buffer size check when processing received messages. The resulting buffer overflow can cause a crash, resulting in a denial of service.	7.5	More Details
CVE-2024-45601	Mesop is a Python-based UI framework designed for rapid web apps development. A vulnerability has been discovered and fixed in Mesop that could potentially allow unauthorized access to files on the server hosting the Mesop application. The vulnerability was related to insufficient input validation in a specific endpoint. This could have allowed an attacker to access files not intended to be served. Users are strongly advised to update to the latest version of Mesop immediately. The latest version includes a fix for this vulnerability. At time of publication 0.12.4 is the most recently available version of Mesop.	7.5	More Details
CVE-2024-37406	In Brave Android prior to v1.67.116, domains in the Brave Shields popup are elided from the right instead of the left, which may lead to domain confusion.	7.5	More Details
CVE-2024-43989	Server-Side Request Forgery (SSRF) vulnerability in Firsh Justified Image Grid allows Server Side Request Forgery.This issue affects Justified Image Grid: from n/a through 4.6.1.	7.5	More Details
CVE-2024-42861	An issue in IEEE 802.1AS linuxptp v.4.2 and before allowing a remote attacker to cause a denial of service via a crafted Pdelay_Req message to the time synchronization function	7.5	More Details
CVE-2024-46382	A SQL injection vulnerability in linlinjava litemall 1.8.0 allows a remote attacker to obtain sensitive information via the goodsId, goodsSn, and name parameters in AdminGoodscontroller.java.	7.5	More Details
CVE-2024-45861	Kastle Systems firmware prior to May 1, 2024, contained a hard-coded credential, which if accessed may allow an attacker to access sensitive information.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45862	Kastle Systems firmware prior to May 1, 2024, stored machine credentials in cleartext, which may allow an attacker to access sensitive information.	7.5	More Details
CVE-2024-46583	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the extRadSrv2 parameter at cgiapp.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46598	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the iprofileidx parameter at dialin.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46597	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sPubKey parameter at dialin.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-47221	CheckUser in ScadaServerEngine/MainLogic.cs in Rapid SCADA through 5.8.4 allows an empty password.	7.5	More Details
CVE-2024-46592	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the ssidencrypt_5g%d parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46595	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the saveitem parameter at lan2lan.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46584	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the AControlIp1 parameter at acontrol.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46594	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the saveVPNProfile parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46593	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the trapcomm parameter at cgiswm.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46585	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sProfileName parameter at usergrp.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46586	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sCloudPass parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46588	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sProfileName parameter at wizfw.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46589	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sIpv6AiccuUser parameter at inetipv6.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46590	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the ssidencrypt%d parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-46591	Draytek Vigor 3910 v4.3.2.6 was discovered to contain a buffer overflow in the sDnsPro parameter at v2x00.cgi. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2024-9034	A vulnerability was found in code-projects Patient Record Management System 1.0 and classified as critical. Affected by this issue is some unknown functionality of the file login.php. The manipulation of the argument username leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-9091	A vulnerability was found in code-projects Student Record System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file /index.php. The manipulation of the argument regno leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-46999	Zitadel is an open source identity management platform. ZITADEL's user grants deactivation mechanism did not work correctly. Deactivated user grants were still provided in token, which could lead to unauthorized access to applications and resources. Additionally, the management and auth API always returned the state as active or did not provide any information about the state. Versions 2.62.1, 2.61.1, 2.60.2, 2.59.3, 2.58.5, 2.57.5, 2.56.6, 2.55.8, and 2.54.10 have been released which address this issue. Users are advised to upgrade. Users unable to upgrade may explicitly remove the user grants to make sure the user does not get access anymore.	7.3	More Details
CVE-2021-27917	Prior to this patch, a stored XSS vulnerability existed in the contact tracking and page hits report.	7.3	More Details
CVE-2024-9087	A vulnerability, which was classified as critical, was found in code-projects Vehicle Management 1.0. This affects an unknown part of the file /edit1.php. The manipulation of the argument sno leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-9039	A vulnerability, which was classified as critical, has been found in SourceCodester Best House Rental Management System 1.0. Affected by this issue is some unknown functionality of the file /ajax.php?action=signup. The manipulation of the argument firstname/lastname/email leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-9085	A vulnerability was found in code-projects Restaurant Reservation System 1.0. It has been rated as critical. This issue affects some unknown processing of the file index.php. The manipulation of the argument date leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory mentions sid as affected paramater which is incorrect.	7.3	More Details
CVE-2024-9035	A vulnerability was found in code-projects Blood Bank Management System 1.0. It has been classified as critical. This affects an unknown part of the file /admin/login.php of the component Admin Login. The manipulation of the argument username/password leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9080	A vulnerability was found in code-projects Student Record System 1.0. It has been classified as critical. Affected is an unknown function of the file /pincode-verification.php. The manipulation of the argument pincode leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-9079	A vulnerability was found in code-projects Student Record System 1.0 and classified as critical. This issue affects some unknown processing of the file /marks.php. The manipulation of the argument coursename leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-9078	A vulnerability has been found in code-projects Student Record System 1.0 and classified as critical. This vulnerability affects unknown code of the file /course.php. The manipulation of the argument coursename leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-9037	A vulnerability classified as critical has been found in Codezips Internal Marks Calculation 1.0. Affected is an unknown function of the file index.php. The manipulation of the argument tid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	7.3	More Details
CVE-2024-8623	The The MDTF – Meta Data and Taxonomies Filter plugin for WordPress is vulnerable to arbitrary shortcode execution in all versions up to, and including, 1.3.3.3. This is due to the software allowing users to execute an action that does not properly validate a value before running do_shortcode. This makes it possible for unauthenticated attackers to execute arbitrary shortcodes.	7.3	More Details
CVE-2024-40442	An issue in Doccano Open source annotation tools for machine learning practitioners v.1.8.4 and Doccano Auto Labeling Pipeline module to annotate a document automatically v.0.1.23 allows a remote attacker to escalate privileges via a crafted REST Request.	7.2	More Details
CVE-2022-2439	The Easy Digital Downloads – Simple eCommerce for Selling Digital Files plugin for WordPress is vulnerable to deserialization of untrusted input via the 'upload[file]' parameter in versions up to, and including 3.3.3. This makes it possible for authenticated administrative users to call files using a PHAR wrapper, that will deserialize and call arbitrary PHP Objects that can be used to perform a variety of malicious actions granted a POP chain is also present.	7.2	More Details
CVE-2024-39842	A SQL injection vulnerability in Centreon 24.04.2 allows a remote high-privileged attacker to execute arbitrary SQL command via user massive changes inputs.	7.2	More Details
CVE-2022-25769	ImpactThe default .htaccess file has some restrictions in the access to PHP files to only allow specific PHP files to be executed in the root of the application. This logic isn't correct, as the regex in the second FilesMatch only checks the filename, not the full path.	7.2	More Details
CVE-2024-43971	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Sunshine Sunshine Photo Cart allows Reflected XSS.This issue affects Sunshine Photo Cart: from n/a through 3.2.5.	7.1	More Details
CVE-2024-43970	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in SureCart allows Reflected XSS.This issue affects SureCart: from n/a through 2.29.3.	7.1	More Details
CVE-2024-46724	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix out-of-bounds read of df_v1_7_channel_number Check the fb_channel_number range to avoid the array out-of-bounds read error	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-44003	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in spicethemes Spice Starter Sites allows Reflected XSS.This issue affects Spice Starter Sites: from n/a through 1.2.5.	7.1	More Details
CVE-2024-46731	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: fix the Out-of-bounds read warning using index i - 1U may beyond element index for mc_data[] when i = 0.	7.1	More Details
CVE-2024-46743	In the Linux kernel, the following vulnerability has been resolved: of/irq: Prevent device address out-of-bounds read in interrupt map walk When of_irq_parse_raw() is invoked with a device address smaller than the interrupt parent node (from #address-cells property), KASAN detects the following out-of-bounds read when populating the initial match table (dyndbg="func of_irq_parse_* +p"): OF: of_irq_parse_one: dev=/soc@0/picasso/watchdog, index=0 OF: parent=/soc@0/pci@878000000000/gpio0@17,0, intsize=2 OF: intspec=4 OF: of_irq_parse_raw: ipar=/soc@0/pci@878000000000/gpio0@17,0, size=2 OF: -> addrsize=3 == BUG: KASAN: slab-out-of-bounds in of_irq_parse_raw+0x2b8/0x8d0 Read of size 4 at addr ffffff81beca5608 by task bash/764 CPU: 1 PID: 764 Comm: bash Tainted: G O 6.1.67-484c613561-nokia_sm_arm64 #1 Hardware name: Unknown Unknown Product/Unknown Product, BIOS 2023.01-12.24.03-dirty 01/01/2023 Call trace: dump_backtrace+0xdc/0x130 show_stack+0x1c/0x30 dump_stack_lvl+0x6c/0x84 print_report+0x150/0x448 kasan_report+0x98/0x140 __asan_load4+0x78/0xa0 of_irq_parse_raw+0x2b8/0x8d0 of_irq_parse_one+0x24c/0x270 parse_interrupts+0xc0/0x120 of_fwnode_add_links+0x100/0x2d0 fw_devlink_parse_fwtree+0x64/0xc0 device_add+0xb38/0xc30 of_device_add+0x64/0x90 of_platform_device_create_pdata+0xd0/0x170 of_platform_bus_create+0x244/0x600 of_platform_notify+0x1b0/0x254 blocking_notifier_call_chain+0x9c/0xd0 __of_changeset_entry_notify+0x1b8/0x230 __of_changeset_apply_notify+0x54/0xe4 of_overlay_fdt_apply+0xc04/0xd94 ... The buggy address belongs to the object at ffffff81beca5600 which belongs to the cache kmalloc-128 of size 128 The buggy address is located 8 bytes inside of 128-byte region [ffffff81beca5600, ffffff81beca5680) The buggy address belongs to the physical page: page:00000000230d3d03 refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x1beca4 head:00000000230d3d03 order:1 compound_mapcount:0 compound_pincount:0 flags: 0x8000000000010200(slablheadlzone=2) raw: 8000000000010200 0000000000000000 dead000000000122 ffffff810000c300 raw: 0000000000000000 0000000000200020 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffffff81beca5500: 04 fc fc fc fc fc fc fc fc fc fc fc fc fc fc ffffff81beca5580: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc >ffffff81beca5600: 00 fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ^ ffffff81beca5680: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ffffff81beca5700: 00 00 00 00 00 00 fc fc fc fc fc fc fc fc fc fc == OF: -> got it ! Prevent the out-of-bounds read by copying the device address into a buffer of sufficient size.	7.1	More Details
CVE-2024-46747	In the Linux kernel, the following vulnerability has been resolved: HID: cougar: fix slab-out-of-bounds Read in cougar_report_fixup report_fixup for the Cougar 500k Gaming Keyboard was not verifying that the report descriptor size was correct before accessing it	7.1	More Details
CVE-2024-44002	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in PickPlugins Team Showcase allows Reflected XSS.This issue affects Team Showcase: from n/a through 1.22.25.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46774	In the Linux kernel, the following vulnerability has been resolved: powerpc/rtas: Prevent Spectre v1 gadget construction in sys_rtas() Smatch warns: arch/powerpc/kernel/rtas.c:1932 __do_sys_rtas() warn: potential spectre issue 'args.args' [r] (local cap) The 'nargs' and 'nret' locals come directly from a user-supplied buffer and are used as indexes into a small stack-based array and as inputs to copy_to_user() after they are subject to bounds checks. Use array_index_nospec() after the bounds checks to clamp these values for speculative execution.	7.1	More Details
CVE-2024-46722	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix mc_data out-of-bounds read warning Clear warning that read mc_data[i-1] may out-of-bounds.	7.1	More Details
CVE-2024-43975	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in highwarden Super Store Finder allows Cross-Site Scripting (XSS).This issue affects Super Store Finder: from n/a through 6.9.7.	7.1	More Details
CVE-2024-46723	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix ucode out-of-bounds read warning Clear warning that read ucode[] may out-of-bounds.	7.1	More Details
CVE-2022-25768	The logic in place to facilitate the update process via the user interface lacks access control to verify if permission exists to perform the tasks. Prior to this patch being applied it might be possible for an attacker to access the Mautic version number or to execute parts of the upgrade process without permission. As upgrading in the user interface is deprecated, this functionality is no longer required.	7.0	More Details
CVE-2024-23972	Sony XAV-AX5500 USB Configuration Descriptor Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Sony XAV-AX5500 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the USB host driver. A crafted USB configuration descriptor can trigger an overflow of a fixed-length buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-23185	6.8	More Details
CVE-2024-23933	Sony XAV-AX5500 CarPlay TLV Stack-based Buffer Overflow Remote Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Sony XAV-AX5500 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the implementation of the Apple CarPlay protocol. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-23238	6.8	More Details
CVE-2024-23922	Sony XAV-AX5500 Insufficient Firmware Update Validation Remote Code Execution Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of Sony XAV-AX5500 devices. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of software updates. The issue results from the lack of proper validation of software update packages. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-22939	6.8	More Details
CVE-2024-39843	A SQL injection vulnerability in Centreon 24.04.2 allows a remote high-privileged attacker to execute arbitrary SQL command via create user form inputs.	6.7	More Details
CVE-2024-40441	An issue in Doccano Open source annotation tools for machine learning practitioners v.1.8.4 and Doccano Auto Labeling Pipeline module to annotate a document automatically v.0.1.23 allows a remote attacker to escalate privileges via the model_attribs parameter.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25775	Prior to the patched version, logged in users of Mautic are vulnerable to an SQL injection vulnerability in the Reports bundle. The user could retrieve and alter data like sensitive data, login, and depending on database permission the attacker can manipulate file systems.	6.6	More Details
CVE-2024-44540	Ubiquiti AirMax firmware version firmware version 8 allows attackers with physical access to gain a privileged command shell via the UART Debugging Port.	6.6	More Details
CVE-2024-39342	Entrust Instant Financial Issuance (formerly known as Cardwizard) 6.10.0, 6.9.0, 6.9.1, 6.9.2, and 6.8.x and earlier uses a DLL library (i.e. DCG.Security.dll) with a custom AES encryption process that relies on static hard-coded key values. These keys are not uniquely generated per installation of the software. Combined with the encrypted password that can be obtained from "WebAPI.cfg.xml" in CVE-2024-39341, the decryption is trivial and can lead to privilege escalation on the Windows host.	6.6	More Details
CVE-2024-8969	OMFLOW from The SYSCOM Group has a vulnerability involving the exposure of sensitive data. This allows remote attackers who have logged into the system to obtain password hashes of all users and administrators.	6.5	More Details
CVE-2024-43996	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in ElementsKit ElementsKit Pro allows PHP Local File Inclusion.This issue affects ElementsKit Pro: from n/a through 3.6.0.	6.5	More Details
CVE-2024-44048	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in wpWax Product Carousel Slider & Grid Ultimate for WooCommerce allows PHP Local File Inclusion.This issue affects Product Carousel Slider & Grid Ultimate for WooCommerce: from n/a through 1.9.10.	6.5	More Details
CVE-2024-47085	This vulnerability exists in Apex Softcell LD DP Back Office due to improper validation of certain parameters (cCdslClicentcode and cLdClientCode) in the API endpoint. An authenticated remote attacker could exploit this vulnerability by manipulating parameters in the API request body leading to exposure of sensitive information belonging to other users.	6.5	More Details
CVE-2024-46978	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible for any user knowing the ID of a notification filter preference of another user, to enable/disable it or even delete it. The impact is that the target user might start loosing notifications on some pages because of this. This vulnerability is present in XWiki since 13.2-rc-1. This vulnerability has been patched in XWiki 14.10.21, 15.5.5, 15.10.1, 16.0-rc-1. The patch consists in checking properly the rights of the user before performing any action on the filters. Users are advised to upgrade. It's possible to fix manually the vulnerability by editing the document `XWiki.Notifications.Code.NotificationPreferenceService` to apply the changes performed in commit e8acc9d8e6af7dfbfe70716ded431642ae4a6dd4.	6.5	More Details
CVE-2024-47086	This vulnerability exists in Apex Softcell LD DP Back Office due to improper implementation of OTP validation mechanism in certain API endpoints. An authenticated remote attacker could exploit this vulnerability by providing arbitrary OTP value for authentication and subsequently changing its API response. Successful exploitation of this vulnerability could allow the attacker to bypass OTP verification for other user accounts.	6.5	More Details
CVE-2024-47087	This vulnerability exists in Apex Softcell LD Geo due to improper validation of the certain parameters (Client ID, DPID or BOID) in the API endpoint. An authenticated remote attacker could exploit this vulnerability by manipulating parameters in the API request body leading to exposure of sensitive information belonging to other users.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46959	runofast Indoor Security Camera for Baby Monitor has a default password of password for the root account. This allows access to the /stream1 URI via the rtsp:// protocol to receive the video and audio stream.	6.5	More Details
CVE-2024-47089	This vulnerability exists in the Apex Softcell LD Geo due to improper validation of the transaction token ID in the API endpoint. An authenticated remote attacker could exploit this vulnerability by manipulating the transaction token ID in the API request leading to unauthorized access and modification of transactions belonging to other users.	6.5	More Details
CVE-2023-41611	Victure PC420 1.1.39 was discovered to use a weak and partially hardcoded key to encrypt data.	6.5	More Details
CVE-2022-25777	Prior to the patched version, an authenticated user of Mautic could read system files and access the internal addresses of the application due to a Server-Side Request Forgery (SSRF) vulnerability.	6.5	More Details
CVE-2024-31184	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MeterStats::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-43489	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	6.5	More Details
CVE-2024-43992	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Latepoint LatePoint allows Stored XSS.This issue affects LatePoint: from n/a through 4.9.91.	6.5	More Details
CVE-2024-46644	eNMS 4.4.0 to 4.7.1 is vulnerable to Directory Traversal via edit_file.	6.5	More Details
CVE-2024-46646	eNMS up to 4.7.1 is vulnerable to Directory Traversal via /download/file.	6.5	More Details
CVE-2024-43983	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Podlove Podlove Podcast Publisher allows Stored XSS.This issue affects Podlove Podcast Publisher: from n/a through 4.1.13.	6.5	More Details
CVE-2024-43987	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in wayneconnor Sliding Door allows Stored XSS.This issue affects Sliding Door: from n/a through 3.6.	6.5	More Details
CVE-2024-46647	eNMS 4.4.0 to 4.7.1 is vulnerable to Directory Traversal via upload_files.	6.5	More Details
CVE-2024-43988	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in digitalnature Mystique allows Stored XSS.This issue affects Mystique: from n/a through 2.5.7.	6.5	More Details
CVE-2024-43991	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in webdzier Hotel Galaxy allows Stored XSS.This issue affects Hotel Galaxy: from n/a through 4.4.24.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43993	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Liquido allows Stored XSS.This issue affects Liquido: from n/a through 1.0.1.2.	6.5	More Details
CVE-2024-44005	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Wpsoul Greenshift – animation and page builder blocks allows Stored XSS.This issue affects Greenshift – animation and page builder blocks: from n/a through 9.3.7.	6.5	More Details
CVE-2024-43994	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in CryoutCreations Kahuna allows Stored XSS.This issue affects Kahuna: from n/a through 1.7.0.	6.5	More Details
CVE-2024-43995	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in sonalsinha21 Posterity allows Stored XSS.This issue affects Posterity: from n/a through 3.6.	6.5	More Details
CVE-2024-6786	The vulnerability allows an attacker to craft MQTT messages that include relative path traversal sequences, enabling them to read arbitrary files on the system. This could lead to the disclosure of sensitive information, such as configuration files and JWT signing secrets.	6.5	More Details
CVE-2024-44001	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in WP Royal Royal Elementor Addons allows Stored XSS.This issue affects Royal Elementor Addons: from n/a through 1.3.982.	6.5	More Details
CVE-2024-45810	Envoy is a cloud-native high-performance edge/middle/service proxy. Envoy will crash when the http async client is handling `sendLocalReply` under some circumstance, e.g., websocket upgrade, and requests mirroring. The http async client will crash during the `sendLocalReply()` in http async client, one reason is http async client is duplicating the status code, another one is the destroy of router is called at the destructor of the async stream, while the stream is deferred deleted at first. There will be problems that the stream decoder is destroyed but its reference is called in `router.onDestroy()`, causing segment fault. This will impact ext_authz if the `upgrade` and `connection` header are allowed, and request mirrorring. This issue has been addressed in versions 1.31.2, 1.30.6, 1.29.9, and 1.28.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2024-45808	Envoy is a cloud-native high-performance edge/middle/service proxy. A vulnerability has been identified in Envoy that allows malicious attackers to inject unexpected content into access logs. This is achieved by exploiting the lack of validation for the `REQUESTED_SERVER_NAME` field for access loggers. This issue has been addressed in versions 1.31.2, 1.30.6, 1.29.9, and 1.28.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2024-45806	Envoy is a cloud-native high-performance edge/middle/service proxy. A security vulnerability in Envoy allows external clients to manipulate Envoy headers, potentially leading to unauthorized access or other malicious actions within the mesh. This issue arises due to Envoy's default configuration of internal trust boundaries, which considers all RFC1918 private address ranges as internal. The default behavior for handling internal addresses in Envoy has been changed. Previously, RFC1918 IP addresses were automatically considered internal, even if the internal_address_config was empty. The default configuration of Envoy will continue to trust internal addresses while in this release and it will not trust them by default in next release. If you have tooling such as probes on your private network which need to be treated as trusted (e.g. changing arbitrary x-envoy headers) please explicitly include those addresses or CIDR ranges into `internal_address_config`. Successful exploitation could allow attackers to bypass security controls, access sensitive data, or disrupt services within the mesh, like Istio. This issue has been addressed in versions 1.31.2, 1.30.6, 1.29.9, and 1.28.7. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43496	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	6.5	More Details
CVE-2024-42351	Galaxy is a free, open-source system for analyzing data, authoring workflows, training and education, publishing tools, managing infrastructure, and more. An attacker can potentially replace the contents of public datasets resulting in data loss or tampering. All supported branches of Galaxy (and more back to release_21.05) were amended with the below patch. Users are advised to upgrade. There are no known workarounds for this vulnerability.	6.5	More Details
CVE-2024-31169	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::QueueGetConfigReply::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31183	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::Hello::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31171	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::StatsReplyPort::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31170	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::StatsReplyQueue::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31168	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::EchoCommon::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31166	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::HelloElemVersionBitmap::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31173	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::StatsReplyFlow::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31174	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::FeaturesReply::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-5682	Improper Restriction of Excessive Authentication Attempts vulnerability in Yordam Information Technology Yordam Library Automation System allows Interface Manipulation.This issue affects Yordam Library Automation System: before 20.1.	6.5	More Details
CVE-2024-31176	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::TableFeaturePropOXM::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31177	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg modules). This vulnerability is associated with program routines fluid_msg::of13::TableFeaturePropActions::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31178	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::TableFeaturePropNextTables::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31179	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::TableFeaturePropInstruction::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31180	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::GroupDesc::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31181	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::GroupStats::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31172	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::StatsReplyTable::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31189	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartRequestTableFeatures::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31186	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::QueueGetConfigReply::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31190	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyMeterConfig::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31188	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyTableFeatures::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31195	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyTable::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31191	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyMeter::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31192	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyGroupDesc::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31187	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyPortDescription::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31194	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyPortStats::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details
CVE-2024-31193	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MultipartReplyGroup::unpack. This issue affects libfluid: 0.1.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45348	Xiaomi Router AX9000 has a post-authorization command injection vulnerability. This vulnerability is caused by the lack of validation of user input, and an attacker can exploit this vulnerability to execute arbitrary code.	6.4	More Details
CVE-2024-8657	The Garden Gnome Package plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's ggpkg shortcode in all versions up to, and including, 2.2.9 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-8364	The WP Custom Fields Search plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's wpcfs-preset shortcode in all versions up to, and including, 1.2.35 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2024-9004	A vulnerability classified as critical has been found in D-Link DAR-7000 up to 20240912. Affected is an unknown function of the file /view/DBManage/Backup_Server_commit.php. The manipulation of the argument host leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	6.3	More Details
CVE-2024-9090	A vulnerability was found in SourceCodester Modern Loan Management System 1.0. It has been classified as critical. Affected is an unknown function of the file search_member.php. The manipulation of the argument searchMember leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9001	A vulnerability was found in TOTOLINK T10 4.1.8cu.5207. It has been declared as critical. This vulnerability affects the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi. The manipulation of the argument command leads to os command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2024-9088	A vulnerability has been found in SourceCodester Telecom Billing Management System 1.0 and classified as critical. This vulnerability affects the function login. The manipulation of the argument uname leads to buffer overflow. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9041	A vulnerability has been found in SourceCodester Best House Rental Management System 1.0 and classified as critical. This vulnerability affects unknown code of the file /ajax.php?action=update_account. The manipulation of the argument firstname/lastname/email leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9081	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file view_category.php. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9086	A vulnerability classified as critical has been found in code-projects Restaurant Reservation System 1.0. Affected is an unknown function of the file /filter.php. The manipulation of the argument from/to leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The initial researcher advisory only mentions the parameter "from" to be affected. But it must be assumed that parameter "to" is affected as well.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-9082	A vulnerability was found in SourceCodester Online Eyewear Shop 1.0. It has been rated as critical. Affected by this issue is some unknown functionality of the file /Users.phpf=save of the component User Creation Handler. The manipulation of the argument type with the input 1 leads to improper authorization. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9032	A vulnerability, which was classified as critical, was found in SourceCodester Simple Forum-Discussion System 1.0. Affected is an unknown function of the file /index.php. The manipulation of the argument page leads to path traversal. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9006	A vulnerability was found in jeanmarc77 123solar 1.8.4.5. It has been rated as critical. Affected by this issue is some unknown functionality of the file config/config_invt1.php. The manipulation of the argument PASSOx leads to code injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The patch is identified as f4a8c748ec436e5a79f91ccb6a6f73752b336aa5. It is recommended to apply a patch to fix this issue.	6.3	More Details
CVE-2024-9011	A vulnerability, which was classified as critical, was found in code-projects Crud Operation System 1.0. Affected is an unknown function of the file updata.php. The manipulation of the argument sid leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9009	A vulnerability, which was classified as critical, has been found in code-projects Online Quiz Site 1.0. This issue affects some unknown processing of the file showtest.php. The manipulation of the argument subid leads to sql injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9008	A vulnerability classified as critical was found in SourceCodester Best Online News Portal 1.0. This vulnerability affects unknown code of the file /news-details.php of the component Comment Section. The manipulation of the argument name leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9093	A vulnerability classified as critical has been found in SourceCodester Profile Registration without Reload Refresh 1.0. This affects an unknown part of the file del.php of the component GET Parameter Handler. The manipulation of the argument list leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9036	A vulnerability was found in itsourcecode Online Bookstore 1.0. It has been rated as critical. This issue affects some unknown processing of the file admin_add.php. The manipulation of the argument image leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-9094	A vulnerability classified as critical was found in code-projects Blood Bank System 1.0. This vulnerability affects unknown code of the file /admin/blood/update/o-.php. The manipulation of the argument bloodname leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	6.3	More Details
CVE-2024-8850	The MC4WP: Mailchimp for WordPress plugin for WordPress is vulnerable to Reflected Cross-Site Scripting via the 'email' parameter when a placeholder such as {email} is used for the field in versions 4.9.9 to 4.9.16 due to insufficient input sanitization and output escaping. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47068	Rollup is a module bundler for JavaScript. Versions prior to 2.79.2, 3.29.5, and 4.22.4 are susceptible to a DOM Clobbering vulnerability when bundling scripts with properties from `import.meta` (e.g., `import.meta.url`) in `cjs`/`umd`/`iife` format. The DOM Clobbering gadget can lead to cross-site scripting (XSS) in web pages where scriptless attacker-controlled HTML elements (e.g., an `img` tag with an unsanitized `name` attribute) are present. Versions 2.79.2, 3.29.5, and 4.22.4 contain a patch for the vulnerability.	6.1	More Details
CVE-2024-42697	Cross Site Scripting vulnerability in Leotheme Leo Product Search Module v.2.1.6 and earlier allows a remote attacker to execute arbitrary code via the q parameter of the product search function.	6.1	More Details
CVE-2024-8716	The XT Ajax Add To Cart for WooCommerce plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.1.2. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-8653	A vulnerability in NetCat CMS allows an attacker to execute JavaScript code in a user's browser when they visit specific paths on the site. This issue affects NetCat CMS v. 6.4.0.24126.2 and possibly others. Apply patch from vendor https://netcat.ru/ https://netcat.ru/] . Versions 6.4.0.24248 and on have the patch.	6.1	More Details
CVE-2024-6877	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Eliz Software Panel allows Reflected XSS.This issue affects Panel: before v2.3.24.	6.1	More Details
CVE-2024-43024	Multiple stored cross-site scripting (XSS) vulnerabilities in RWS MultiTrans v7.0.23324.2 and earlier allow attackers to execute arbitrary web scripts or HTML via a crafted payload.	6.1	More Details
CVE-2024-8662	The Koko Analytics plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.3.12. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-8652	A vulnerability in NetCat CMS allows an attacker to execute JavaScript code in a user's browser when they visit specific path on the site. This issue affects NetCat CMS v. 6.4.0.24126.2 and possibly others. Apply patch from vendor https://netcat.ru/ https://netcat.ru/] . Versions 6.4.0.24248 and on have the patch.	6.1	More Details
CVE-2024-8883	A misconfiguration flaw was found in Keycloak. This issue can allow an attacker to redirect users to an arbitrary URL if a 'Valid Redirect URI' is set to http://localhost or http://127.0.0.1, enabling sensitive information such as authorization codes to be exposed to the attacker, potentially leading to session hijacking.	6.1	More Details
CVE-2024-47069	Oveleon Cookie Bar is a cookie bar is for the Contao Open Source CMS and allows a visitor to define cookie & privacy settings for the website. Prior to versions 1.16.3 and 2.1.3, the `block/locale` endpoint does not properly sanitize the user-controlled `locale` input before including it in the backend's HTTP response, thereby causing reflected cross-site scripting. Versions 1.16.3 and 2.1.3 contain a patch for the vulnerability.	6.1	More Details
CVE-2024-46372	DedeCMS 5.7.115 is vulnerable to Cross Site Scripting (XSS) via the advertisement code box in the advertisement management module.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45366	Welcart e-Commerce prior to 2.11.2 contains a cross-site scripting vulnerability. If this vulnerability is exploited, an arbitrary script may be executed on the user's web browser.	6.1	More Details
CVE-2024-25673	Couchbase Server 7.6.x before 7.6.2, 7.2.x before 7.2.6, and all earlier versions allows HTTP Host header injection.	6.1	More Details
CVE-2024-47227	iRedAdmin before 2.6 allows XSS, e.g., via order_name.	6.1	More Details
CVE-2024-8770	A Cross-Site Scripting (XSS) vulnerability was identified in the repository transfer feature of GitHub Enterprise Server, which allows attackers to steal sensitive user information via social engineering. This vulnerability affected all versions of GitHub Enterprise Server and was fixed in version 3.10.17, 3.11.15, 3.12.9, 3.13.4, and 3.14.1. This vulnerability was reported via the GitHub Bug Bounty program.	6.1	More Details
CVE-2024-8544	The Pixel Cat – Conversion Pixel Manager plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 3.0.5. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-8738	The Seriously Simple Stats plugin for WordPress is vulnerable to Reflected Cross-Site Scripting due to the use of add_query_arg without appropriate escaping on the URL in all versions up to, and including, 1.6.0. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link.	6.1	More Details
CVE-2024-43025	An HTML injection vulnerability in RWS MultiTrans v7.0.23324.2 and earlier allows attackers to alter the HTML-layout and possibly execute a phishing attack via a crafted payload injected into a sent e-mail.	6.1	More Details
CVE-2024-46544	Incorrect Default Permissions vulnerability in Apache Tomcat Connectors allows local users to view and modify shared memory containing mod_jk configuration which may lead to information disclosure and/or denial of service. This issue affects Apache Tomcat Connectors: from 1.2.9-beta through 1.2.49. Only mod_jk on Unix like systems is affected. Neither the ISAPI redirector nor mod_jk on Windows is affected. Users are recommended to upgrade to version 1.2.50, which fixes the issue.	5.9	More Details
CVE-2024-43972	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Pagelayer Team PageLayer allows Stored XSS.This issue affects PageLayer: from n/a through 1.8.7.	5.9	More Details
CVE-2024-46241	PHPGurukul Dairy Farm Shop Management System v1.1 is vulnerable to Cross-Site Scripting (XSS) via the pname parameter in add_product.php and edit_product.php.	5.9	More Details
CVE-2024-39341	Entrust Instant Financial Issuance (On Premise) Software (formerly known as Cardwizard) 6.10.0, 6.9.0, 6.9.1, 6.9.2, and 6.8.x and earlier leaves behind a configuration file (i.e. WebAPI.cfg.xml) after the installation process. This file can be accessed without authentication on HTTP port 80 by guessing the correct IIS webroot path. It includes system configuration parameter names and values with sensitive configuration values encrypted.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-43999	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Saturday Drive Ninja Forms allows Stored XSS.This issue affects Ninja Forms: from n/a through 3.8.11.	5.9	More Details
CVE-2024-46721	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix possible NULL pointer dereference profile->parent->dents[AAFS_PROF_DIR] could be NULL only if its parent is made from __create_missing_ancestors(..) and 'ent->old' is NULL in aa_replace_profiles(..). In that case, it must return an error code and the code, -ENOENT represents its state that the path of its parent is not existed yet. BUG: kernel NULL pointer dereference, address: 0000000000000030 PGD 0 P4D 0 PREEMPT SMP PTI CPU: 4 PID: 3362 Comm: apparmor_parser Not tainted 6.8.0-24-generic #24 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.15.0-1 04/01/2014 RIP: 0010:aafs_create.constprop.0+0x7f/0x130 Code: 4c 63 e0 48 83 c4 18 4c 89 e0 5b 41 5c 41 5d 41 5e 41 5f 5d 31 d2 31 c9 31 f6 31 ff 45 31 c0 45 31 c9 45 31 d2 c3 cc cc cc cc <4d> 8b 55 30 4d 8d ba a0 00 00 00 4c 89 55 c0 4c 89 ff e8 7a 6a ae RSP: 0018:ffffc9000b2c7c98 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 00000000000041ed RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffc9000b2c7cd8 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffffff82baac10 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 00007be9f22cf740(0000) GS:ffff88817bc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000030 CR3: 0000000134b08000 CR4: 00000000000006f0 Call Trace: <TASK> ? show_regs+0x6d/0x80 ? __die+0x24/0x80 ? page_fault_oops+0x99/0x1b0 ? kernelmode_fixup_or_oops+0xb2/0x140 ? __bad_area_nosemaphore+0x1a5/0x2c0 ? find_vma+0x34/0x60 ? bad_area_nosemaphore+0x16/0x30 ? do_user_addr_fault+0x2a2/0x6b0 ? exc_page_fault+0x83/0x1b0 ? asm_exc_page_fault+0x27/0x30 ? aafs_create.constprop.0+0x7f/0x130 ? aafs_create.constprop.0+0x51/0x130 __aafs_profile_mkdir+0x3d6/0x480 aa_replace_profiles+0x83f/0x1270 policy_update+0xe3/0x180 profile_load+0xbc/0x150 ? rw_verify_area+0x47/0x140 vfs_write+0x100/0x480 ? __x64_sys_openat+0x55/0xa0 ? syscall_exit_to_user_mode+0x86/0x260 ksys_write+0x73/0x100 __x64_sys_write+0x19/0x30 x64_sys_call+0x7e/0x25c0 do_syscall_64+0x7f/0x180 entry_SYSCALL_64_after_hwframe+0x78/0x80 RIP: 0033:0x7be9f211c574 Code: c7 00 16 00 00 00 b8 ff ff ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 f3 0f 1e fa 80 3d d5 ea 0e 00 00 74 13 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 54 c3 0f 1f 00 55 48 89 e5 48 83 ec 20 48 89 RSP: 002b:00007ffd26f2b8c8 EFLAGS: 00000202 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 00005d504415e200 RCX: 00007be9f211c574 RDX: 0000000000001fc1 RSI: 00005d504418bc80 RDI: 0000000000000004 RBP: 0000000000001fc1 R08: 0000000000001fc1 R09: 0000000080000000 R10: 0000000000000000 R11: 0000000000000202 R12: 00005d504418bc80 R13: 0000000000000004 R14: 00007ffd26f2b9b0 R15: 00007ffd26f2ba30 </TASK> Modules linked in: snd_seq_dummy snd_hrtimer qrtr snd_hda_codec_generic snd_hda_intel snd_intel_dspcfg snd_intel_sdw_acpi snd_hda_codec snd_hda_core snd_hwdep snd_pcm snd_seq_midi snd_seq_midi_event snd_rawmidi snd_seq snd_seq_device i2c_i801 snd_timer i2c_smbus qxl snd soundcore drm_ttm_helper lpc_ich ttm joydev input_leds serio_raw mac_hid binfmt_misc msr parport_pc ppdev lp parport efi_pstore nfnetlink dmi_sysfs qemu_fw_cfg ip_tables x_tables autofs4 hid_generic usbhid hid ahci libahci psmouse virtio_rng xhci_pci xhci_pci_renesas CR2: 0000000000000030 ---[end trace 0000000000000000]--- RIP: 0010:aafs_create.constprop.0+0x7f/0x130 Code: 4c 63 e0 48 83 c4 18 4c 89 e0 5b 41 5c 41 5d 41 5e 41 5f 5d 31 d2 31 c9 31 f6 31 ff 45 31 c0 45 31 c9 45 31 d2 c3 cc cc cc cc <4d> 8b 55 30 4d 8d ba a0 00 00 00 4c 89 55 c0 4c 89 ff e8 7a 6a ae RSP: 0018:ffffc9000b2c7c98 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 00000000000041ed RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffc9000b2c7cd8 R08: 0000000000000000 R09: 0000000000000000 R10: 0000 ---truncated---	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46720	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix dereference after null check check the pointer hive before use.	5.5	More Details
CVE-2024-6785	The configuration file stores credentials in cleartext. An attacker with local access rights can read or modify the configuration file, potentially resulting in the service being abused due to sensitive information exposure.	5.5	More Details
CVE-2024-46719	In the Linux kernel, the following vulnerability has been resolved: usb: typec: ucsi: Fix null pointer dereference in trace ucsi_register_altmode checks IS_ERR for the alt pointer and treats NULL as valid. When CONFIG_TYPEC_DP_ALTMODE is not enabled, ucsi_register_displayport returns NULL which causes a NULL pointer dereference in trace. Rather than return NULL, call typec_port_register_altmode to register DisplayPort alternate mode as a non-controllable mode when CONFIG_TYPEC_DP_ALTMODE is not enabled.	5.5	More Details
CVE-2024-46714	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Skip wbscl_set_scaler_filter if filter is null Callers can pass null in filter (i.e. from returned from the function wbscl_get_filter_coeffs_16p) and a null check is added to ensure that is not the case. This fixes 4 NULL_RETURNS issues reported by Coverity.	5.5	More Details
CVE-2024-46784	In the Linux kernel, the following vulnerability has been resolved: net: mana: Fix error handling in mana_create_txq/rxq's NAPI cleanup Currently napi_disable() gets called during rxq and txq cleanup, even before napi is enabled and hrtimer is initialized. It causes kernel panic. ? page_fault_oops+0x136/0x2b0 ? page_counter_cancel+0x2e/0x80 ? do_user_addr_fault+0x2f2/0x640 ? refill_obj_stock+0xc4/0x110 ? exc_page_fault+0x71/0x160 ? asm_exc_page_fault+0x27/0x30 ? __mmdrop+0x10/0x180 ? __mmdrop+0xec/0x180 ? hrtimer_active+0xd/0x50 hrtimer_try_to_cancel+0x2c/0xf0 hrtimer_cancel+0x15/0x30 napi_disable+0x65/0x90 mana_destroy_rxq+0x4c/0x2f0 mana_create_rxq.isra.0+0x56c/0x6d0 ? mana_uncfg_vport+0x50/0x50 mana_alloc_queues+0x21b/0x320 ? skb_dequeue+0x5f/0x80	5.5	More Details
CVE-2024-46726	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Ensure index calculation will not overflow [WHY & HOW] Make sure vmid0p72_idx, vnom0p8_idx and vmax0p9_idx calculation will never overflow and exceess array size. This fixes 3 OVERRUN and 1 INTEGER_OVERFLOW issues reported by Coverity.	5.5	More Details
CVE-2024-46727	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add otg_master NULL check within resource_log_pipe_topology_update [Why] Coverity reports NULL_RETURN warning. [How] Add otg_master NULL check.	5.5	More Details
CVE-2024-46761	In the Linux kernel, the following vulnerability has been resolved: pci/hotplug/pnv_php: Fix hotplug driver crash on Powernv The hotplug driver for powerpc (pci/hotplug/pnv_php.c) causes a kernel crash when we try to hot-unplug/disable the PCIe switch/bridge from the PHB. The crash occurs because although the MSI data structure has been released during disable/hot-unplug path and it has been assigned with NULL, still during unregistration the code was again trying to explicitly disable the MSI which causes the NULL pointer dereference and kernel crash. The patch fixes the check during unregistration path to prevent invoking pci_disable_msi/msix() since its data structure is already freed.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46789	In the Linux kernel, the following vulnerability has been resolved: mm/slub: add check for s->flags in the alloc_tagging_slab_free_hook When enable CONFIG_MEMCG & CONFIG_KFENCE & CONFIG_KMEMLEAK, the following warning always occurs,This is because the following call stack occurred: mem_pool_alloc kmem_cache_alloc_noprof slab_alloc_node kfence_alloc Once the kfence allocation is successful,slab->obj_exts will not be empty, because it has already been assigned a value in kfence_init_pool. Since in the prepare_slab_obj_exts_hook function,we perform a check for s->flags & (SLAB_NO_OBJ_EXT | SLAB_NOLEAKTRACE),the alloc_tag_add function will not be called as a result.Therefore,ref->ct remains NULL. However,when we call mem_pool_free,since obj_ext is not empty, it eventually leads to the alloc_tag_sub scenario being invoked. This is where the warning occurs. So we should add corresponding checks in the alloc_tagging_slab_free_hook. For __GFP_NO_OBJ_EXT case,I didn't see the specific case where it's using kfence,so I won't add the corresponding check in alloc_tagging_slab_free_hook for now. [3.734349] ------------[cut here]------------ [3.734807] alloc_tag was not set [3.735129] WARNING: CPU: 4 PID: 40 at ./include/linux/alloc_tag.h:130 kmem_cache_free+0x444/0x574 [3.735866] Modules linked in: autofs4 [3.736211] CPU: 4 UID: 0 PID: 40 Comm: ksoftirqd/4 Tainted: G W 6.11.0-rc3-dirty #1 [3.736969] Tainted: [W]=WARN [3.737258] Hardware name: QEMU KVM Virtual Machine, BIOS unknown 2/2/2022 [3.737875] pstate: 60400005 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [3.738501] pc : kmem_cache_free+0x444/0x574 [3.738951] lr : kmem_cache_free+0x444/0x574 [3.739361] sp : ffff80008357bb60 [3.739693] x29: ffff80008357bb70 x28: 0000000000000000 x27: 0000000000000000 [3.740338] x26: ffff80008207f000 x25: ffff000b2eb2fd60 x24: ffff0000c0005700 [3.740982] x23: ffff8000804229e4 x22: ffff800082080000 x21: ffff800081756000 [3.741630] x20: fffffd7ff8253360 x19: 00000000000000a8 x18: ffffffffffffffff [3.742274] x17: ffff800ab327f000 x16: ffff800083398000 x15: ffff800081756df0 [3.742919] x14: 0000000000000000 x13: 205d344320202020 x12: 5b5d373038343337 [3.743560] x11: ffff80008357b650 x10: 000000000000005d x9 : 00000000ffffffd0 [3.744231] x8 : 7f7f7f7f7f7f7f7f x7 : ffff80008237bad0 x6 : c0000000ffff7fff [3.744907] x5 : ffff80008237ba78 x4 : ffff8000820bbad0 x3 : 0000000000000001 [3.745580] x2 : 68d66547c09f7800 x1 : 68d66547c09f7800 x0 : 0000000000000000 [3.746255] Call trace: [3.746530] kmem_cache_free+0x444/0x574 [3.746931] mem_pool_free+0x44/0xf4 [3.747306] free_object_rcu+0xc8/0xdc [3.747693] rcu_do_batch+0x234/0x8a4 [3.748075] rcu_core+0x230/0x3e4 [3.748424] rcu_core_si+0x14/0x1c [3.748780] handle_softirqs+0x134/0x378 [3.749189] run_ksoftirqd+0x70/0x9c [3.749560] smpboot_thread_fn+0x148/0x22c [3.749978] kthread+0x10c/0x118 [3.750323] ret_from_fork+0x10/0x20 [3.750696] ---[end trace 0000000000000000]---	5.5	More Details
CVE-2024-46762	In the Linux kernel, the following vulnerability has been resolved: xen: privcmd: Fix possible access to a freed kirqfd instance Nothing prevents simultaneous ioctl calls to privcmd_irqfd_assign() and privcmd_irqfd_deassign(). If that happens, it is possible that a kirqfd created and added to the irqfds_list by privcmd_irqfd_assign() may get removed by another thread executing privcmd_irqfd_deassign(), while the former is still using it after dropping the locks. This can lead to a situation where an already freed kirqfd instance may be accessed and cause kernel oops. Use SRCU locking to prevent the same, as is done for the KVM implementation for irqfds.	5.5	More Details
CVE-2024-5960	Plaintext Storage of a Password vulnerability in Eliz Software Panel allows : Use of Known Domain Credentials.This issue affects Panel: before v2.3.24.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46763	In the Linux kernel, the following vulnerability has been resolved: fou: Fix null-ptr-deref in GRO. We observed a null-ptr-deref in fou_gro_receive() while shutting down a host. [0] The NULL pointer is sk->sk_user_data, and the offset 8 is of protocol in struct fou. When fou_release() is called due to netns dismantle or explicit tunnel teardown, udp_tunnel_sock_release() sets NULL to sk->sk_user_data. Then, the tunnel socket is destroyed after a single RCU grace period. So, in-flight udp4_gro_receive() could find the socket and execute the FOU GRO handler, where sk->sk_user_data could be NULL. Let's use rcu_dereference_sk_user_data() in fou_from_sock() and add NULL checks in FOU GRO handlers. [0]: BUG: kernel NULL pointer dereference, address: 0000000000000008 PF: supervisor read access in kernel mode PF: error_code(0x0000) - not-present page PGD 80000001032f4067 P4D 80000001032f4067 PUD 103240067 PMD 0 SMP PTI CPU: 0 PID: 0 Comm: swapper/0 Not tainted 5.10.216-204.855.amzn2.x86_64 #1 Hardware name: Amazon EC2 c5.large/, BIOS 1.0 10/16/2017 RIP: 0010:fou_gro_receive (net/ipv4/fou.c:233) [fou] Code: 41 5f c3 cc cc cc cc e8 e7 2e 69 f4 0f 1f 80 00 00 00 00 0f 1f 44 00 00 49 89 f8 41 54 48 89 f7 48 89 d6 49 8b 80 88 02 00 00 <0f> b6 48 08 0f b7 42 4a 66 25 fd fd 80 cc 02 66 89 42 4a 0f b6 42 RSP: 0018:ffffa330c0003d08 EFLAGS: 00010297 RAX: 0000000000000000 RBX: ffff93d9e3a6b900 RCX: 0000000000000010 RDX: ffff93d9e3a6b900 RSI: ffff93d9e3a6b900 RDI: ffff93dac2e24d08 RBP: ffff93d9e3a6b900 R08: ffff93dacbce6400 R09: 0000000000000002 R10: 0000000000000000 R11: ffffffffb5f369b0 R12: ffff93dacbce6400 R13: ffff93dac2e24d08 R14: 0000000000000000 R15: ffffffffb4edd1c0 FS: 0000000000000000(0000) GS:ffff93daee800000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000008 CR3: 0000000102140001 CR4: 00000000007706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <IRQ> ? show_trace_log_lvl (arch/x86/kernel/dumpstack.c:259) ? __die_body.cold (arch/x86/kernel/dumpstack.c:478 arch/x86/kernel/dumpstack.c:420) ? no_context (arch/x86/mm/fault.c:752) ? exc_page_fault (arch/x86/include/asm/irqflags.h:49 arch/x86/include/asm/irqflags.h:89 arch/x86/mm/fault.c:1435 arch/x86/mm/fault.c:1483) ? asm_exc_page_fault (arch/x86/include/asm/idtentry.h:571) ? fou_gro_receive (net/ipv4/fou.c:233) [fou] udp_gro_receive (include/linux/netdevice.h:2552 net/ipv4/udp_offload.c:559) udp4_gro_receive (net/ipv4/udp_offload.c:604) inet_gro_receive (net/ipv4/af_inet.c:1549 (discriminator 7)) dev_gro_receive (net/core/dev.c:6035 (discriminator 4)) napi_gro_receive (net/core/dev.c:6170) ena_clean_rx_irq (drivers/amazon/net/ena/ena_netdev.c:1558) [ena] ena_io_poll (drivers/amazon/net/ena/ena_netdev.c:1742) [ena] napi_poll (net/core/dev.c:6847) net_rx_action (net/core/dev.c:6917) __do_softirq (arch/x86/include/asm/jump_label.h:25 include/linux/jump_label.h:200 include/trace/events/irq.h:142 kernel/softirq.c:299) asm_call_irq_on_stack (arch/x86/entry/entry_64.S:809) </IRQ> do_softirq_own_stack (arch/x86/include/asm/irq_stack.h:27 arch/x86/include/asm/irq_stack.h:77 arch/x86/kernel/irq_64.c:77) irq_exit_rcu (kernel/softirq.c:393 kernel/softirq.c:423 kernel/softirq.c:435) common_interrupt (arch/x86/kernel/irq.c:239) asm_common_interrupt (arch/x86/include/asm/idtentry.h:626) RIP: 0010:acpi_idle_do_entry (arch/x86/include/asm/irqflags.h:49 arch/x86/include/asm/irqflags.h:89 drivers/acpi/processor_idle.c:114 drivers/acpi/processor_idle.c:575) Code: 8b 15 d1 3c c4 02 ed c3 cc cc cc cc 65 48 8b 04 25 40 ef 01 00 48 8b 00 a8 08 75 eb 0f 1f 44 00 00 0f 00 2d d5 09 55 00 fb f4 <fa> c3 cc cc cc cc e9 be fc ff ff 66 66 2e 0f 1f 84 00 00 00 00 00 RSP: 0018:ffffffffb5603e58 EFLAGS: 00000246 RAX: 0000000000004000 RBX: ffff93dac0929c00 RCX: ffff93daee833900 RDX: ffff93daee800000 RSI: ffff93d ---truncated---	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46765	In the Linux kernel, the following vulnerability has been resolved: ice: protect XDP configuration with a mutex The main threat to data consistency in ice_xdp() is a possible asynchronous PF reset. It can be triggered by a user or by TX timeout handler. XDP setup and PF reset code access the same resources in the following sections: * ice_vsi_close() in ice_prepare_for_reset() - already rtnl-locked * ice_vsi_rebuild() for the PF VSI - not protected * ice_vsi_open() - already rtnl-locked With an unfortunate timing, such accesses can result in a crash such as the one below: [+1.999878] ice 0000:b1:00.0: Registered XDP mem model MEM_TYPE_XSK_BUFF_POOL on Rx ring 14 [+2.002992] ice 0000:b1:00.0: Registered XDP mem model MEM_TYPE_XSK_BUFF_POOL on Rx ring 18 [Mar15 18:17] ice 0000:b1:00.0 ens801f0np0: NETDEV WATCHDOG: CPU: 38: transmit queue 14 timed out 80692736 ms [+0.000093] ice 0000:b1:00.0 ens801f0np0: tx_timeout: VSI_num: 6, Q 14, NTC: 0x0, HW_HEAD: 0x0, NTU: 0x0, INT: 0x4000001 [+0.000012] ice 0000:b1:00.0 ens801f0np0: tx_timeout recovery level 1, txqueue 14 [+0.394718] ice 0000:b1:00.0: PTP reset successful [+0.006184] BUG: kernel NULL pointer dereference, address: 0000000000000098 [+0.000045] #PF: supervisor read access in kernel mode [+0.000023] #PF: error_code(0x0000) - not-present page [+0.000023] PGD 0 P4D 0 [+0.000018] Oops: 0000 [#1] PREEMPT SMP NOPTI [+0.000023] CPU: 38 PID: 7540 Comm: kworker/38:1 Not tainted 6.8.0-rc7 #1 [+0.000031] Hardware name: Intel Corporation S2600WFT/S2600WFT, BIOS SE5C620.86B.02.01.0014.082620210524 08/26/2021 [+0.000036] Workqueue: ice ice_service_task [ice] [+0.000183] RIP: 0010:ice_clean_tx_ring+0xa/0xd0 [ice] [...] [+0.000013] Call Trace: [+0.000016] <TASK> [+0.000014] ? __die+0x1f/0x70 [+0.000029] ? page_fault_oops+0x171/0x4f0 [+0.000029] ? schedule+0x3b/0xd0 [+0.000027] ? exc_page_fault+0x7b/0x180 [+0.000022] ? asm_exc_page_fault+0x22/0x30 [+0.000031] ? ice_clean_tx_ring+0xa/0xd0 [ice] [+0.000194] ice_free_tx_ring+0xe/0x60 [ice] [+0.000186] ice_destroy_xdp_rings+0x157/0x310 [ice] [+0.000151] ice_vsi_decfg+0x53/0xe0 [ice] [+0.000180] ice_vsi_rebuild+0x239/0x540 [ice] [+0.000186] ice_vsi_rebuild_by_type+0x76/0x180 [ice] [+0.000145] ice_rebuild+0x18c/0x840 [ice] [+0.000145] ? delay_tsc+0x4a/0xc0 [+0.000022] ? delay_tsc+0x92/0xc0 [+0.000020] ice_do_reset+0x140/0x180 [ice] [+0.000886] ice_service_task+0x404/0x1030 [ice] [+0.000824] process_one_work+0x171/0x340 [+0.000685] worker_thread+0x277/0x3a0 [+0.000675] ? preempt_count_add+0x6a/0xa0 [+0.000677] ? _raw_spin_lock_irqsave+0x23/0x50 [+0.000679] ? __pfx_worker_thread+0x10/0x10 [+0.000653] kthread+0xf0/0x120 [+0.000635] ? __pfx_kthread+0x10/0x10 [+0.000616] ret_from_fork+0x2d/0x50 [+0.000612] ? __pfx_kthread+0x10/0x10 [+0.000604] ret_from_fork_asm+0x1b/0x30 [+0.000604] </TASK> The previous way of handling this through returning -EBUSY is not viable, particularly when destroying AF_XDP socket, because the kernel proceeds with removal anyway. There is plenty of code between those calls and there is no need to create a large critical section that covers all of them, same as there is no need to protect ice_vsi_rebuild() with rtnl_lock(). Add xdp_state_lock mutex to protect ice_vsi_rebuild() and ice_xdp(). Leaving unprotected sections in between would result in two states that have to be considered: 1. when the VSI is closed, but not yet rebuild 2. when VSI is already rebuild, but not yet open The latter case is actually already handled through !netif_running() case, we just need to adjust flag checking a little. The former one is not as trivial, because between ice_vsi_close() and ice_vsi_rebuild(), a lot of hardware interaction happens, this can make adding/deleting rings exit with an error. Luckily, VSI rebuild is pending and can apply new configuration for us in a managed fashion. Therefore, add an additional VSI state flag ICE_VSI_REBUILD_PENDING to indicate that ice_x ---truncated---	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46788	In the Linux kernel, the following vulnerability has been resolved: tracing/osnoise: Use a cpumask to know what threads are kthreads The start_kthread() and stop_thread() code was not always called with the interface_lock held. This means that the kthread variable could be unexpectedly changed causing the kthread_stop() to be called on it when it should not have been, leading to: while true; do rtla timerlat top -u -q & PID=$!; sleep 5; kill -INT $PID; sleep 0.001; kill -TERM $PID; wait $PID; done Causing the following OOPS: Oops: general protection fault, probably for non-canonical address 0xdffffc0000000002: 0000 [#1] PREEMPT SMP KASAN PTI KASAN: null-ptr-deref in range [0x0000000000000010-0x0000000000000017] CPU: 5 UID: 0 PID: 885 Comm: timerlatu/5 Not tainted 6.11.0-rc4-test-00002-gbc754cc76d1b-dirty #125 a533010b71dab205ad2f507188ce8c82203b0254 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 RIP: 0010:hrtimer_active+0x58/0x300 Code: 48 c1 ee 03 41 54 48 01 d1 48 01 d6 55 53 48 83 ec 20 80 39 00 0f 85 30 02 00 00 49 8b 6f 30 4c 8d 75 10 4c 89 f0 48 c1 e8 03 <0f> b6 3c 10 4c 89 f0 83 e0 07 83 c0 03 40 38 f8 7c 09 40 84 ff 0f RSP: 0018:ffff88811d97f940 EFLAGS: 00010202 RAX: 0000000000000002 RBX: ffff88823c6b5b28 RCX: ffffed10478d6b6b RDX: dfffffc0000000000 RSI: ffffed10478d6b6c RDI: ffff88823c6b5b28 RBP: 0000000000000000 R08: ffff88823c6b5b58 R09: ffff88823c6b5b60 R10: ffff88811d97f957 R11: 0000000000000010 R12: 00000000000a801d R13: ffff88810d8b35d8 R14: 0000000000000010 R15: ffff88823c6b5b28 FS: 0000000000000000(0000) GS:ffff88823c680000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000561858ad7258 CR3: 000000007729e001 CR4: 0000000000170ef0 Call Trace: <TASK> ? die_addr+0x40/0xa0 ? exc_general_protection+0x154/0x230 ? asm_exc_general_protection+0x26/0x30 ? hrtimer_active+0x58/0x300 ? __pfx_mutex_lock+0x10/0x10 ? __pfx_locks_remove_file+0x10/0x10 hrtimer_cancel+0x15/0x40 timerlat_fd_release+0x8e/0x1f0 ? security_file_release+0x43/0x80 __fput+0x372/0xb10 task_work_run+0x11e/0x1f0 ? _raw_spin_lock+0x85/0xe0 ? __pfx_task_work_run+0x10/0x10 ? poison_slab_object+0x109/0x170 ? do_exit+0x7a0/0x24b0 do_exit+0x7bd/0x24b0 ? __pfx_migrate_enable+0x10/0x10 ? __pfx_do_exit+0x10/0x10 ? __pfx_read_tsc+0x10/0x10 ? ktime_get+0x64/0x140 ? _raw_spin_lock_irq+0x86/0xe0 do_group_exit+0xb0/0x220 get_signal+0x17ba/0x1b50 ? vfs_read+0x179/0xa40 ? timerlat_fd_read+0x30b/0x9d0 ? __pfx_get_signal+0x10/0x10 ? __pfx_timerlat_fd_read+0x10/0x10 arch_do_signal_or_restart+0x8c/0x570 ? __pfx_arch_do_signal_or_restart+0x10/0x10 ? vfs_read+0x179/0xa40 ? ksys_read+0xfe/0x1d0 ? __pfx_ksys_read+0x10/0x10 syscall_exit_to_user_mode+0xbc/0x130 do_syscall_64+0x74/0x110 ? __pfx___rseq_handle_notify_resume+0x10/0x10 ? __pfx_ksys_read+0x10/0x10 ? fpregs_restore_userregs+0xdb/0x1e0 ? fpregs_restore_userregs+0xdb/0x1e0 ? syscall_exit_to_user_mode+0x116/0x130 ? do_syscall_64+0x74/0x110 ? do_syscall_64+0x74/0x110 ? do_syscall_64+0x74/0x110 entry_SYSCALL_64_after_hwframe+0x71/0x79 RIP: 0033:0x7ff0070eca9c Code: Unable to access opcode bytes at 0x7ff0070eca72. RSP: 002b:00007ff006dff8c0 EFLAGS: 00000246 ORIG_RAX: 0000000000000000 RAX: 0000000000000000 RBX: 0000000000000005 RCX: 00007ff0070eca9c RDX: 0000000000000400 RSI: 00007ff006dff9a0 RDI: 0000000000000003 RBP: 00007ff006dffde0 R08: 0000000000000000 R09: 00007ff000000ba0 R10: 00007ff007004b08 R11: 0000000000000246 R12: 0000000000000003 R13: 00007ff006dff9a0 R14: 0000000000000007 R15: 0000000000000008 </TASK> Modules linked in: snd_hda_intel snd_intel_dspcfg snd_intel_sdw_acpi snd_hda_codec snd_hwdep snd_hda_core ---[end trace 0000000000000000]--- This is because it would mistakenly call kthread_stop() on a user space thread making it "exit" before it actually exits. Since kthread ---truncated---	5.5	More Details
CVE-2024-46768	In the Linux kernel, the following vulnerability has been resolved: hwmon: (hp-wmi-sensors) Check if WMI event data exists The BIOS can choose to return no event data in response to a WMI event, so the ACPI object passed to the WMI notify handler can be NULL. Check for such a situation and ignore the event in such a case.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46769	In the Linux kernel, the following vulnerability has been resolved: spi: intel: Add check devm_kasprintf() returned value intel_spi_populate_chip() use devm_kasprintf() to set pdata->name. This can return a NULL pointer on failure but this returned value is not checked.	5.5	More Details
CVE-2024-46770	In the Linux kernel, the following vulnerability has been resolved: ice: Add netif_device_attach/detach into PF reset flow Ethtool callbacks can be executed while reset is in progress and try to access deleted resources, e.g. getting coalesce settings can result in a NULL pointer dereference seen below. Reproduction steps: Once the driver is fully initialized, trigger reset: # echo 1 > /sys/class/net/<interface>/device/reset when reset is in progress try to get coalesce settings using ethtool: # ethtool -c <interface> BUG: kernel NULL pointer dereference, address: 0000000000000020 PGD 0 P4D 0 Oops: Oops: 0000 [#1] PREEMPT SMP PTI CPU: 11 PID: 19713 Comm: ethtool Tainted: G S 6.10.0-rc7+ #7 RIP: 0010:ice_get_q_coalesce+0x2e/0xa0 [ice] RSP: 0018:ffffbab1e9bcf6a8 EFLAGS: 00010206 RAX: 000000000000000c RBX: ffff94512305b028 RCX: 0000000000000000 RDX: 0000000000000000 RSI: ffff9451c3f2e588 RDI: ffff9451c3f2e588 RBP: 0000000000000000 R08: 0000000000000000 R09: 0000000000000000 R10: ffff9451c3f2e580 R11: 000000000000001f R12: ffff945121fa9000 R13: ffffbab1e9bcf760 R14: 0000000000000013 R15: ffffffff9e65dd40 FS: 00007faee5fbe740(0000) GS:ffff94546fd80000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000020 CR3: 0000000106c2e005 CR4: 00000000001706f0 Call Trace: <TASK> ice_get_coalesce+0x17/0x30 [ice] coalesce_prepare_data+0x61/0x80 ethnl_default_doit+0xde/0x340 genl_family_rcv_msg_doit+0xf2/0x150 genl_rcv_msg+0x1b3/0x2c0 netlink_rcv_skb+0x5b/0x110 genl_rcv+0x28/0x40 netlink_unicast+0x19c/0x290 netlink_sendmsg+0x222/0x490 __sys_sendto+0x1df/0x1f0 __x64_sys_sendto+0x24/0x30 do_syscall_64+0x82/0x160 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7faee60d8e27 Calling netif_device_detach() before reset makes the net core not call the driver when ethtool command is issued, the attempt to execute an ethtool command during reset will result in the following message: netlink error: No such device instead of NULL pointer dereference. Once reset is done and ice_rebuild() is executing, the netif_device_attach() is called to allow for ethtool operations to occur again in a safe manner.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46771	In the Linux kernel, the following vulnerability has been resolved: can: bcm: Remove proc entry when dev is unregistered. syzkaller reported a warning in bcm_connect() below. [0] The repro calls connect() to vxcan1, removes vxcan1, and calls connect() with ifindex == 0. Calling connect() for a BCM socket allocates a proc entry. Then, bcm_sk(sk)->bound is set to 1 to prevent further connect(). However, removing the bound device resets bcm_sk(sk)->bound to 0 in bcm_notify(). The 2nd connect() tries to allocate a proc entry with the same name and sets NULL to bcm_sk(sk)->bcm_proc_read, leaking the original proc entry. Since the proc entry is available only for connect()ed sockets, let's clean up the entry when the bound netdev is unregistered. [0]: proc_dir_entry 'can-bcm/2456' already registered WARNING: CPU: 1 PID: 394 at fs/proc/generic.c:376 proc_register+0x645/0x8f0 fs/proc/generic.c:375 Modules linked in: CPU: 1 PID: 394 Comm: syz-executor403 Not tainted 6.10.0-rc7-g852e42cc2dd4 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01/2014 RIP: 0010:proc_register+0x645/0x8f0 fs/proc/generic.c:375 Code: 00 00 00 00 00 48 85 ed 0f 85 97 02 00 00 4d 85 f6 0f 85 9f 02 00 00 48 c7 c7 9b cb cf 87 48 89 de 4c 89 fa e8 1c 6f eb fe 90 <0f> 0b 90 90 48 c7 c7 98 37 99 89 e8 cb 7e 22 05 bb 00 00 00 10 48 RSP: 0018:ffa0000000cd7c30 EFLAGS: 00010246 RAX: 9e129be1950f0200 RBX: ff1100011b51582c RCX: ff1100011857cd80 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000002 RBP: 0000000000000000 R08: ffd400000000000f R09: ff1100013e78cac0 R10: ffac800000cd7980 R11: ff1100013e12b1f0 R12: 0000000000000000 R13: 0000000000000000 R14: 0000000000000000 R15: ff1100011a99a2ec FS: 00007fbd7086f740(0000) GS:ff1100013fd00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00000000200071c0 CR3: 0000000118556004 CR4: 0000000000771ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe07f0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> proc_create_net_single+0x144/0x210 fs/proc/proc_net.c:220 bcm_connect+0x472/0x840 net/can/bcm.c:1673 __sys_connect_file net/socket.c:2049 [inline] __sys_connect+0x5d2/0x690 net/socket.c:2066 __do_sys_connect net/socket.c:2076 [inline] __se_sys_connect net/socket.c:2073 [inline] __x64_sys_connect+0x8f/0x100 net/socket.c:2073 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xd9/0x1c0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x4b/0x53 RIP: 0033:0x7fbd708b0e5d Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 73 9f 1b 00 f7 d8 64 89 01 48 RSP: 002b:00007fff8cd33f08 EFLAGS: 00000246 ORIG_RAX: 000000000000002a RAX: ffffffffffffffda RBX: 0000000000000003 RCX: 00007fbd708b0e5d RDX: 0000000000000010 RSI: 0000000020000040 RDI: 0000000000000003 RBP: 0000000000000000 R08: 0000000000000040 R09: 0000000000000040 R10: 0000000000000040 R11: 0000000000000246 R12: 00007fff8cd34098 R13: 0000000000401280 R14: 0000000000406de8 R15: 00007fbd70ab9000 </TASK> remove_proc_entry: removing non-empty directory 'net/can-bcm', leaking at least '2456'	5.5	More Details
CVE-2024-46772	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check denominator crb_pipes before used [WHAT & HOW] A denominator cannot be 0, and is checked before used. This fixes 2 DIVIDE_BY_ZERO issues reported by Coverity.	5.5	More Details
CVE-2024-46773	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check denominator pbn_div before used [WHAT & HOW] A denominator cannot be 0, and is checked before used. This fixes 1 DIVIDE_BY_ZERO issue reported by Coverity.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46785	In the Linux kernel, the following vulnerability has been resolved: eventfs: Use list_del_rcu() for SRCU protected list variable Chi Zhiling reported: We found a null pointer accessing in tracefs[1], the reason is that the variable 'ei_child' is set to LIST_POISON1, that means the list was removed in eventfs_remove_rec. so when access the ei_child->is_freed, the panic triggered. by the way, the following script can reproduce this panic loop1 (){ while true do echo "p:kp submit_bio" > /sys/kernel/debug/tracing/kprobe_events echo "" > /sys/kernel/debug/tracing/kprobe_events done } loop2 (){ while true do tree /sys/kernel/debug/tracing/events/kprobes/ done } loop1 & loop2 [1]: [1147.959632][T17331] Unable to handle kernel paging request at virtual address dead000000000150 [1147.968239] [T17331] Mem abort info: [1147.971739][T17331] ESR = 0x0000000096000004 [1147.976172] [T17331] EC = 0x25: DABT (current EL), IL = 32 bits [1147.982171][T17331] SET = 0, FnV = 0 [1147.985906][T17331] EA = 0, S1PTW = 0 [1147.989734][T17331] FSC = 0x04: level 0 translation fault [1147.995292][T17331] Data abort info: [1147.998858][T17331] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [1148.005023][T17331] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [1148.010759][T17331] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [1148.016752][T17331] [dead000000000150] address between user and kernel address ranges [1148.024571][T17331] Internal error: Oops: 0000000096000004 [#1] SMP [1148.030825] [T17331] Modules linked in: team_mode_loadbalance team nlmon act_gact cls_flower sch_ingress bonding tls macvlan dummy ib_core bridge stp llc veth amdgpu amdxcp mfd_core gpu_sched drm_exec drm_buddy radeon crct10dif_ce video drm_suballoc_helper ghash_ce drm_ttm_helper sha2_ce ttm sha256_arm64 i2c_algo_bit sha1_ce sbsa_gwdt cp210x drm_display_helper cec sr_mod cdrom drm_kms_helper binfmt_misc sg loop fuse drm dm_mod nfnetlink ip_tables autofs4 [last unloaded: tls] [1148.072808][T17331] CPU: 3 PID: 17331 Comm: ls Tainted: G W ------- ---- 6.6.43 #2 [1148.081751][T17331] Source Version: 21b3b386e948bedd29369af66f3e98ab01b1c650 [1148.088783][T17331] Hardware name: Greatwall GW-001M1A-FTF/GW-001M1A-FTF, BIOS KunLun BIOS V4.0 07/16/2020 [1148.098419][T17331] pstate: 20000005 (nzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [1148.106060][T17331] pc : eventfs_iterate+0x2c0/0x398 [1148.111017][T17331] lr : eventfs_iterate+0x2fc/0x398 [1148.115969][T17331] sp : ffff80008d56bbd0 [1148.119964] [T17331] x29: ffff80008d56bbf0 x28: ffff001ff5be2600 x27: 0000000000000000 [1148.127781] [T17331] x26: ffff001ff52ca4e0 x25: 0000000000009977 x24: dead000000000100 [1148.135598][T17331] x23: 0000000000000000 x22: 000000000000000b x21: ffff800082645f10 [1148.143415][T17331] x20: ffff001fddf87c70 x19: ffff80008d56bc90 x18: 0000000000000000 [1148.151231][T17331] x17: 0000000000000000 x16: 0000000000000000 x15: ffff001ff52ca4e0 [1148.159048][T17331] x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 [1148.166864][T17331] x11: 0000000000000000 x10: 0000000000000000 x9 : ffff8000804391d0 [1148.174680][T17331] x8 : 0000000180000000 x7 : 0000000000000018 x6 : 0000aaab04b92862 [1148.182498][T17331] x5 : 0000aaab04b92862 x4 : 0000000080000000 x3 : 0000000000000068 [1148.190314][T17331] x2 : 000000000000000f x1 : 0000000000007ea8 x0 : 0000000000000001 [1148.198131][T17331] Call trace: [1148.201259][T17331] eventfs_iterate+0x2c0/0x398 [1148.205864][T17331] iterate_dir+0x98/0x188 [1148.210036][T17331] __arm64_sys_getdents64+0x78/0x160 [1148.215161][T17331] invoke_syscall+0x78/0x108 [1148.219593][T17331] el0_svc_common.constprop.0+0x48/0xf0 [1148.224977][T17331] do_el0_svc+0x24/0x38 [1148.228974][T17331] el0_svc+0x40/0x168 [1148.232798][T17 ---truncated---	5.5	More Details
CVE-2024-46775	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Validate function returns [WHAT & HOW] Function return values must be checked before data can be used in subsequent functions. This fixes 4 CHECKED_RETURN issues reported by Coverity.	5.5	More Details
CVE-2024-46776	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Run DC_LOG_DC after checking link->link_enc [WHAT] The DC_LOG_DC should be run after link->link_enc is checked, not before. This fixes 1 REVERSE_INULL issue reported by Coverity.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46777	In the Linux kernel, the following vulnerability has been resolved: udf: Avoid excessive partition lengths Avoid mounting filesystems where the partition would overflow the 32-bits used for block number. Also refuse to mount filesystems where the partition length is so large we cannot safely index bits in a block bitmap.	5.5	More Details
CVE-2024-46778	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check UnboundedRequestEnabled's value CalculateSwathAndDETConfiguration_params_st's UnboundedRequestEnabled is a pointer (i.e. dml_bool_t *UnboundedRequestEnabled), and thus if (p->UnboundedRequestEnabled) checks its address, not bool value. This fixes 1 REVERSE_INULL issue reported by Coverity.	5.5	More Details
CVE-2024-46779	In the Linux kernel, the following vulnerability has been resolved: drm/imagination: Free pvr_vm_gpuva after unlink This caused a measurable memory leak. Although the individual allocations are small, the leaks occurs in a high-usage codepath (remapping or unmapping device memory) so they add up quickly.	5.5	More Details
CVE-2024-46780	In the Linux kernel, the following vulnerability has been resolved: nilfs2: protect references to superblock parameters exposed in sysfs The superblock buffers of nilfs2 can not only be overwritten at runtime for modifications/repairs, but they are also regularly swapped, replaced during resizing, and even abandoned when degrading to one side due to backing device issues. So, accessing them requires mutual exclusion using the reader/writer semaphore "nilfs->ns_sem". Some sysfs attribute show methods read this superblock buffer without the necessary mutual exclusion, which can cause problems with pointer dereferencing and memory access, so fix it.	5.5	More Details
CVE-2024-46781	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix missing cleanup on rollforward recovery error In an error injection test of a routine for mount-time recovery, KASAN found a use-after-free bug. It turned out that if data recovery was performed using partial logs created by dsync writes, but an error occurred before starting the log writer to create a recovered checkpoint, the inodes whose data had been recovered were left in the ns_dirty_files list of the nilfs object and were not freed. Fix this issue by cleaning up inodes that have read the recovery data if the recovery routine fails midway before the log writer starts.	5.5	More Details
CVE-2024-46760	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw88: usb: schedule rx work after everything is set up Right now it's possible to hit NULL pointer dereference in rtw_rx_fill_rx_status on hw object and/or its fields because initialization routine can start getting USB replies before rtw_dev is fully setup. The stack trace looks like this: rtw_rx_fill_rx_status rtw8821c_query_rx_desc rtw_usb_rx_handler ... queue_work rtw_usb_read_port_complete ... usb_submit_urb rtw_usb_rx_resubmit rtw_usb_init_rx rtw_usb_probe So while we do the async stuff rtw_usb_probe continues and calls rtw_register_hw, which does all kinds of initialization (e.g. via ieee80211_register_hw) that rtw_rx_fill_rx_status relies on. Fix this by moving the first usb_submit_urb after everything is set up. For me, this bug manifested as: [8.893177] rtw_8821cu 1-1:1.2: band wrong, packet dropped [8.910904] rtw_8821cu 1-1:1.2: hw->conf.chandef.chan NULL in rtw_rx_fill_rx_status because I'm using Larry's backport of rtw88 driver with the NULL checks in rtw_rx_fill_rx_status.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46755	In the Linux kernel, the following vulnerability has been resolved: wifi: mwifiex: Do not return unused priv in mwifiex_get_priv_by_id() mwifiex_get_priv_by_id() returns the priv pointer corresponding to the bss_num and bss_type, but without checking if the priv is actually currently in use. Unused priv pointers do not have a wiphy attached to them which can lead to NULL pointer dereferences further down the callstack. Fix this by returning only used priv pointers which have priv->bss_mode set to something else than NL80211_IFTYPE_UNSPECIFIED. Said NULL pointer dereference happened when an Accesspoint was started with wpa_supplicant -i mlan0 with this config: network={ ssid="somessid" mode=2 frequency=2412 key_mgmt=WPA-PSK WPA-PSK-SHA256 proto=RSN group=CCMP pairwise=CCMP psk="12345678" } When waiting for the AP to be established, interrupting wpa_supplicant with <ctrl-c> and starting it again this happens: l Unable to handle kernel NULL pointer dereference at virtual address 0000000000000140 l Mem abort info: l ESR = 0x0000000096000004 l EC = 0x25: DABT (current EL), IL = 32 bits l SET = 0, FnV = 0 l EA = 0, S1PTW = 0 l FSC = 0x04: level 0 translation fault l Data abort info: l ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 l CM = 0, WnR = 0, TnD = 0, TagAccess = 0 l GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 l user pgtable: 4k pages, 48-bit VAs, pgdp=0000000046d96000 l [0000000000000140] pgd=0000000000000000, p4d=0000000000000000 l Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP l Modules linked in: caam_jr caamhash_desc spidev caamalg_desc crypto_engine authenc libdes mwifiex_sdio +mwifiex crct10dif_ce cdc_acm onboard_usb_hub fsl_imx8_ddr_perf imx8m_ddrc rtc_ds1307 lm75 rtc_snvs +imx_sdma caam imx8mm_thermal spi_imx error imx_cpufreq_dt fuse ip_tables x_tables ipv6 l CPU: 0 PID: 8 Comm: kworker/0:1 Not tainted 6.9.0-00007-g937242013fce-dirty #18 l Hardware name: somemachine (DT) l Workqueue: events sdio_irq_work l pstate: 00000005 (nzcv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) l pc : mwifiex_get_cfp+0xd8/0x15c [mwifiex] l lr : mwifiex_get_cfp+0x34/0x15c [mwifiex] l sp : ffff8000818b3a70 l x29: ffff8000818b3a70 x28: ffff000006bfd8a5 x27: 0000000000000004 l x26: 000000000000002c x25: 0000000000001511 x24: 0000000002e86bc9 l x23: ffff000006bfd996 x22: 0000000000000004 x21: ffff000007bec000 l x20: 000000000000002c x19: 0000000000000000 x18: 0000000000000000 l x17: 000000040044ffff x16: 00500072b5503510 x15: ccc283740681e517 l x14: 0201000101006d15 x13: 0000000002e8ff43 x12: 002c01000000ffb1 l x11: 0100000000000000 x10: 02e8ff43002c0100 x9 : 0000ffb100100157 l x8 : ffff000003d20000 x7 : 00000000000002f1 x6 : 00000000ffffe124 l x5 : 0000000000000001 x4 : 0000000000000003 x3 : 0000000000000000 l x2 : 0000000000000000 x1 : 0001000000011001 x0 : 0000000000000000 l Call trace: l mwifiex_get_cfp+0xd8/0x15c [mwifiex] l mwifiex_parse_single_response_buf+0x1d0/0x504 [mwifiex] l mwifiex_handle_event_ext_scan_report+0x19c/0x2f8 [mwifiex] l mwifiex_process_sta_event+0x298/0xf0c [mwifiex] l mwifiex_process_event+0x110/0x238 [mwifiex] l mwifiex_main_process+0x428/0xa44 [mwifiex] l mwifiex_sdio_interrupt+0x64/0x12c [mwifiex_sdio] l process_sdio_pending_irqs+0x64/0x1b8 l sdio_irq_work+0x4c/0x7c l process_one_work+0x148/0x2a0 l worker_thread+0x2fc/0x40c l kthread+0x110/0x114 l ret_from_fork+0x10/0x20 l Code: a94153f3 a8c37bfd d50323bf d65f03c0 (f940a000) l ---[end trace 0000000000000000]---	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46790	In the Linux kernel, the following vulnerability has been resolved: codetag: debug: mark codetags for poisoned page as empty When PG_hwpoison pages are freed they are treated differently in free_pages_prepare() and instead of being released they are isolated. Page allocation tag counters are decremented at this point since the page is considered not in use. Later on when such pages are released by unpoison_memory(), the allocation tag counters will be decremented again and the following warning gets reported: [113.930443][T3282] ------------[cut here]------------ [113.931105][T3282] alloc_tag was not set [113.931576][T3282] WARNING: CPU: 2 PID: 3282 at ./include/linux/alloc_tag.h:130 pgalloc_tag_sub.part.66+0x154/0x164 [113.932866][T3282] Modules linked in: hwpoison_inject fuse ip6t_rpfilter ip6t_REJECT nf_reject_ipv6 ipt_REJECT nf_reject_ipv4 xt_conntrack ebtable_nat ebtable_broute ip6table_nat ip6table_man4 [113.941638][T3282] CPU: 2 UID: 0 PID: 3282 Comm: madvise11 Kdump: loaded Tainted: G W 6.11.0-rc4-dirty #18 [113.943003][T3282] Tainted: [W]=WARN [113.943453][T3282] Hardware name: QEMU KVM Virtual Machine, BIOS unknown 2/2/2022 [113.944378][T3282] pstate: 40400005 (nZcv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) [113.945319][T3282] pc : pgalloc_tag_sub.part.66+0x154/0x164 [113.946016][T3282] lr : pgalloc_tag_sub.part.66+0x154/0x164 [113.946706][T3282] sp : ffff800087093a10 [113.947197][T3282] x29: ffff800087093a10 x28: ffff0000d7a9d400 x27: ffff80008249f0a0 [113.948165][T3282] x26: 0000000000000000 x25: ffff80008249f2b0 x24: 0000000000000000 [113.949134][T3282] x23: 0000000000000001 x22: 0000000000000001 x21: 0000000000000000 [113.950597][T3282] x20: ffff0000c08fcad8 x19: ffff80008251e000 x18: ffffffffffffffff [113.952207][T3282] x17: 0000000000000000 x16: 0000000000000000 x15: ffff800081746210 [113.953161][T3282] x14: 0000000000000000 x13: 205d323832335420 x12: 5b5d353031313339 [113.954120][T3282] x11: ffff800087093500 x10: 000000000000005d x9 : 00000000ffffffd0 [113.955078][T3282] x8 : 7f7f7f7f7f7f7f7f x7 : ffff80008236ba90 x6 : c0000000ffff7fff [113.956036][T3282] x5 : ffff000b34bf4dc8 x4 : ffff8000820aba90 x3 : 0000000000000001 [113.956994][T3282] x2 : ffff800ab320f000 x1 : 841d1e35ac932e00 x0 : 0000000000000000 [113.957962][T3282] Call trace: [113.958350][T3282] pgalloc_tag_sub.part.66+0x154/0x164 [113.959000][T3282] pgalloc_tag_sub+0x14/0x1c [113.959539][T3282] free_unref_page+0xf4/0x4b8 [113.960096][T3282] __folio_put+0xd4/0x120 [113.960614][T3282] folio_put+0x24/0x50 [113.961103][T3282] unpoison_memory+0x4f0/0x5b0 [113.961678][T3282] hwpoison_unpoison+0x30/0x48 [hwpoison_inject] [113.962436][T3282] simple_attr_write_xsigned.isra.34+0xec/0x1cc [113.963183][T3282] simple_attr_write+0x38/0x48 [113.963750][T3282] debugfs_attr_write+0x54/0x80 [113.964330][T3282] full_proxy_write+0x68/0x98 [113.964880][T3282] vfs_write+0xdc/0x4d0 [113.965372][T3282] ksys_write+0x78/0x100 [113.965875][T3282] __arm64_sys_write+0x24/0x30 [113.966440][T3282] invoke_syscall+0x7c/0x104 [113.966984][T3282] el0_svc_common.constprop.1+0x88/0x104 [113.967652][T3282] do_el0_svc+0x2c/0x38 [113.968893][T3282] el0_svc+0x3c/0x1b8 [113.969379][T3282] el0t_64_sync_handler+0x98/0xbc [113.969980][T3282] el0t_64_sync+0x19c/0x1a0 [113.970511][T3282] ---[end trace 0000000000000000]--- To fix this, clear the page tag reference after the page got isolated and accounted for.	5.5	More Details
CVE-2024-46739	In the Linux kernel, the following vulnerability has been resolved: uio_hv_generic: Fix kernel NULL pointer dereference in hv_uio_rescind For primary VM Bus channels, primary_channel pointer is always NULL. This pointer is valid only for the secondary channels. Also, rescind callback is meant for primary channels only. Fix NULL pointer dereference by retrieving the device_obj from the parent for the primary channel.	5.5	More Details
CVE-2024-46728	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check index for aux_rd_interval before using aux_rd_interval has size of 7 and should be checked. This fixes 3 OVERRUN and 1 INTEGER_OVERFLOW issues reported by Coverity.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-40703	IBM Cognos Analytics 11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 12.0.0, 12.0.1, 12.0.2, 12.0.3, and IBM Cognos Analytics Reports for iOS 11.0.0.7 could allow a local attacker to obtain sensitive information in the form of an API key. An attacker could use this information to launch further attacks against affected applications.	5.5	More Details
CVE-2024-46730	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Ensure array index tg_inst won't be -1 [WHY & HOW] tg_inst will be a negative if timing_generator_count equals 0, which should be checked before used. This fixes 2 OVERRUN issues reported by Coverity.	5.5	More Details
CVE-2024-8354	A flaw was found in QEMU. An assertion failure was present in the usb_ep_get() function in hw/net/core.c when trying to get the USB endpoint from a USB device. This flaw may allow a malicious unprivileged guest user to crash the QEMU process on the host and cause a denial of service condition.	5.5	More Details
CVE-2024-46783	In the Linux kernel, the following vulnerability has been resolved: tcp_bpf: fix return value of tcp_bpf_sendmsg() When we cork messages in psock->cork, the last message triggers the flushing will result in sending a sk_msg larger than the current message size. In this case, in tcp_bpf_send_verdict(), 'copied' becomes negative at least in the following case: 468 case __SK_DROP: 469 default: 470 sk_msg_free_partial(sk, msg, tosend); 471 sk_msg_apply_bytes(psock, tosend); 472 *copied -= (tosend + delta); // <==== HERE 473 return -EACCES; Therefore, it could lead to the following BUG with a proper value of 'copied' (thanks to syzbot). We should not use negative 'copied' as a return value here. ------------[cut here]------------ kernel BUG at net/socket.c:733! Internal error: Oops - BUG: 00000000f2000800 [#1] PREEMPT SMP Modules linked in: CPU: 0 UID: 0 PID: 3265 Comm: syz-executor510 Not tainted 6.11.0-rc3-syzkaller-00060-gd07b43284ab3 #0 Hardware name: linux,dummy-virt (DT) pstate: 61400009 (nZCv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=--) pc : sock_sendmsg_nosec net/socket.c:733 [inline] pc : sock_sendmsg_nosec net/socket.c:728 [inline] pc : __sock_sendmsg+0x5c/0x60 net/socket.c:745 lr : sock_sendmsg_nosec net/socket.c:730 [inline] lr : __sock_sendmsg+0x54/0x60 net/socket.c:745 sp : ffff800088ea3b30 x29: ffff800088ea3b30 x28: fbf00000062bc900 x27: 0000000000000000 x26: ffff800088ea3bc0 x25: ffff800088ea3bc0 x24: 0000000000000000 x23: f9f00000048dc000 x22: 0000000000000000 x21: ffff800088ea3d90 x20: f9f00000048dc000 x19: ffff800088ea3d90 x18: 0000000000000001 x17: 0000000000000000 x16: 0000000000000000 x15: 000000002002ffaf x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000000 x10: ffff8000815849c0 x9 : ffff8000815b49c0 x8 : 0000000000000000 x7 : 000000000000003f x6 : 0000000000000000 x5 : 00000000000007e0 x4 : fff07ffffd239000 x3 : fbf00000062bc900 x2 : 0000000000000000 x1 : 0000000000000000 x0 : 00000000ffffffdef Call trace: sock_sendmsg_nosec net/socket.c:733 [inline] __sock_sendmsg+0x5c/0x60 net/socket.c:745 ____sys_sendmsg+0x274/0x2ac net/socket.c:2597 ___sys_sendmsg+0xac/0x100 net/socket.c:2651 __sys_sendmsg+0x84/0xe0 net/socket.c:2680 __do_sys_sendmsg net/socket.c:2689 [inline] __se_sys_sendmsg net/socket.c:2687 [inline] __arm64_sys_sendmsg+0x24/0x30 net/socket.c:2687 __invoke_syscall arch/arm64/kernel/syscall.c:35 [inline] invoke_syscall+0x48/0x110 arch/arm64/kernel/syscall.c:49 el0_svc_common.constprop.0+0x40/0xe0 arch/arm64/kernel/syscall.c:132 do_el0_svc+0x1c/0x28 arch/arm64/kernel/syscall.c:151 el0_svc+0x34/0xec arch/arm64/kernel/entry-common.c:712 el0t_64_sync_handler+0x100/0x12c arch/arm64/kernel/entry-common.c:730 el0t_64_sync+0x19c/0x1a0 arch/arm64/kernel/entry.S:598 Code: f9404463 d63f0060 3108441f 54fffe81 (d4210000) ---[end trace 0000000000000000]---	5.5	More Details
CVE-2024-45769	A vulnerability was found in Performance Co-Pilot (PCP). This flaw allows an attacker to send specially crafted data to the system, which could cause the program to misbehave or crash.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46732	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Assign linear_pitch_alignment even for VM [Description] Assign linear_pitch_alignment so we don't cause a divide by 0 error in VM environments	5.5	More Details
CVE-2024-46735	In the Linux kernel, the following vulnerability has been resolved: ublk_drv: fix NULL pointer dereference in ublk_ctrl_start_recovery() When two UBLK_CMD_START_USER_RECOVERY commands are submitted, the first one sets 'ubq->ubq_daemon' to NULL, and the second one triggers WARN in ublk_queue_reinit() and subsequently a NULL pointer dereference issue. Fix it by adding the check in ublk_ctrl_start_recovery() and return immediately in case of zero 'ub->nr_queues_ready'. BUG: kernel NULL pointer dereference, address: 0000000000000028 RIP: 0010:ublk_ctrl_start_recovery.constprop.0+0x82/0x180 Call Trace: <TASK> ? __die+0x20/0x70 ? page_fault_oops+0x75/0x170 ? exc_page_fault+0x64/0x140 ? asm_exc_page_fault+0x22/0x30 ? ublk_ctrl_start_recovery.constprop.0+0x82/0x180 ublk_ctrl_uring_cmd+0x4f7/0x6c0 ? pick_next_task_idle+0x26/0x40 io_uring_cmd+0x9a/0x1b0 io_issue_sqe+0x193/0x3f0 io_wq_submit_work+0x9b/0x390 io_worker_handle_work+0x165/0x360 io_wq_worker+0xcb/0x2f0 ? finish_task_switch.isra.0+0x203/0x290 ? finish_task_switch.isra.0+0x203/0x290 ? __pfx_io_wq_worker+0x10/0x10 ret_from_fork+0x2d/0x50 ? __pfx_io_wq_worker+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK>	5.5	More Details
CVE-2024-46737	In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: fix kernel crash if commands allocation fails If the commands allocation fails in nvmet_tcp_alloc_cmds() the kernel crashes in nvmet_tcp_release_queue_work() because of a NULL pointer dereference. nvmet: failed to install queue 0 cntlid 1 ret 6 Unable to handle kernel NULL pointer dereference at virtual address 0000000000000008 Fix the bug by setting queue->nr_cmds to zero in case nvmet_tcp_alloc_cmd() fails.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46749	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btnxpuart: Fix Null pointer dereference in btnxpuart_flush() This adds a check before freeing the rx->skb in flush and close functions to handle the kernel crash seen while removing driver after FW download fails or before FW download completes. dmesg log: [54.634586] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000080 [54.643398] Mem abort info: [54.646204] ESR = 0x0000000096000004 [54.649964] EC = 0x25: DABT (current EL), IL = 32 bits [54.655286] SET = 0, FnV = 0 [54.658348] EA = 0, S1PTW = 0 [54.661498] FSC = 0x04: level 0 translation fault [54.666391] Data abort info: [54.669273] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [54.674768] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [54.674771] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [54.674775] user pgtable: 4k pages, 48-bit VAs, pgdp=0000000048860000 [54.674780] [0000000000000080] pgd=0000000000000000, p4d=0000000000000000 [54.703880] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP [54.710152] Modules linked in: btnxpuart(-) overlay fsl_jr_uio caam_jr caamkeyblob_desc caamhash_desc caamalg_desc crypto_engine authenc libdes crct10dif_ce polyval_ce polyval_generic snd_soc_imx_spdif snd_soc_imx_card snd_soc_ak5558 snd_soc_ak4458 caam secvio error snd_soc_fsl_micfil snd_soc_fsl_spdif snd_soc_fsl_sai snd_soc_fsl_utils imx_pcm_dma gpio_ir_recv rc_core sch_fq_codel fuse [54.744357] CPU: 3 PID: 72 Comm: kworker/u9:0 Not tainted 6.6.3-otbr-g128004619037 #2 [54.744364] Hardware name: FSL i.MX8MM EVK board (DT) [54.744368] Workqueue: hci0 hci_power_on [54.757244] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [54.757249] pc : kfree_skb_reason+0x18/0xb0 [54.772299] lr : btnxpuart_flush+0x40/0x58 [btnxpuart] [54.782921] sp : ffff8000805ebca0 [54.782923] x29: ffff8000805ebca0 x28: ffffa5c6cf1869c0 x27: ffffa5c6cf186000 [54.782931] x26: ffff377b84852400 x25: ffff377b848523c0 x24: ffff377b845e7230 [54.782938] x23: ffffa5c6ce8dbe08 x22: ffffa5c6ceb65410 x21: 00000000ffffff92 [54.782945] x20: ffffa5c6ce8dbe98 x19: ffffffffffffffac x18: ffffffffffffffff [54.807651] x17: 0000000000000000 x16: ffffa5c6ce2824ec x15: ffff8001005eb857 [54.821917] x14: 0000000000000000 x13: ffffa5c6cf1a02e0 x12: 0000000000000642 [54.821924] x11: 0000000000000040 x10: ffffa5c6cf19d690 x9 : ffffa5c6cf19d688 [54.821931] x8 : ffff377b86000028 x7 : 0000000000000000 x6 : 0000000000000000 [54.821938] x5 : ffff377b86000000 x4 : 0000000000000000 x3 : 0000000000000000 [54.843331] x2 : 0000000000000000 x1 : 0000000000000002 x0 : ffffffffffffffac [54.857599] Call trace: [54.857601] kfree_skb_reason+0x18/0xb0 [54.863878] btnxpuart_flush+0x40/0x58 [btnxpuart] [54.863888] hci_dev_open_sync+0x3a8/0xa04 [54.872773] hci_power_on+0x54/0x2e4 [54.881832] process_one_work+0x138/0x260 [54.881842] worker_thread+0x32c/0x438 [54.881847] kthread+0x118/0x11c [54.881853] ret_from_fork+0x10/0x20 [54.896406] Code: a9be7bfd 910003fd f9000bf3 aa0003f3 (b940d400) [54.896410] ---[end trace 0000000000000000]---	5.5	More Details
CVE-2024-46742	In the Linux kernel, the following vulnerability has been resolved: smb/server: fix potential null-ptr-deref of lease_ctx_info in smb2_open() null-ptr-deref will occur when (req_op_level == SMB2_OPLOCK_LEVEL_LEASE) and parse_lease_state() return NULL. Fix this by check if 'lease_ctx_info' is NULL. Additionally, remove the redundant parentheses in parse_durable_handle_context().	5.5	More Details
CVE-2024-46801	In the Linux kernel, the following vulnerability has been resolved: libfs: fix get_stashed_dentry() get_stashed_dentry() tries to optimistically retrieve a stashed dentry from a provided location. It needs to ensure to hold rcu lock before it dereference the stashed location to prevent UAF issues. Use rcu_dereference() instead of READ_ONCE() it's effectively equivalent with some lockdep bells and whistles and it communicates clearly that this expects rcu protection.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46799	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: ti: am65-cpsw: Fix NULL dereference on XDP_TX If number of TX queues are set to 1 we get a NULL pointer dereference during XDP_TX. ~# ethtool -L eth0 tx 1 ~# ./xdp-trafficgen udp -A <ipv6-src> -a <ipv6-dst> eth0 -t 2 Transmitting on eth0 (ifindex 2) [241.135257] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000030 Fix this by using actual TX queues instead of max TX queues when picking the TX channel in am65_cpsw_ndo_xdp_xmit().	5.5	More Details
CVE-2024-46797	In the Linux kernel, the following vulnerability has been resolved: powerpc/qspinlock: Fix deadlock in MCS queue If an interrupt occurs in queued_spin_lock_slowpath() after we increment qnodesp->count and before node->lock is initialized, another CPU might see stale lock values in get_tail_qnode(). If the stale lock value happens to match the lock on that CPU, then we write to the "next" pointer of the wrong qnode. This causes a deadlock as the former CPU, once it becomes the head of the MCS queue, will spin indefinitely until it's "next" pointer is set by its successor in the queue. Running stress-ng on a 16 core (16EC/16VP) shared LPAR, results in occasional lockups similar to the following: $ stress-ng --all 128 --vm-bytes 80% --aggressive \ --maximize --oomable --verify --syslog \ --metrics --times --timeout 5m watchdog: CPU 15 Hard LOCKUP ..... NIP [c0000000000b78f4] queued_spin_lock_slowpath+0x1184/0x1490 LR [c000000001037c5c] _raw_spin_lock+0x6c/0x90 Call Trace: 0xc000002cfffa3bf0 (unreliable) _raw_spin_lock+0x6c/0x90 raw_spin_rq_lock_nested.part.135+0x4c/0xd0 sched_ttwu_pending+0x60/0x1f0 __flush_smp_call_function_queue+0x1dc/0x670 smp_ipi_demux_relaxed+0xa4/0x100 xive_muxed_ipi_action+0x20/0x40 __handle_irq_event_percpu+0x80/0x240 handle_irq_event_percpu+0x2c/0x80 handle_percpu_irq+0x84/0xd0 generic_handle_irq+0x54/0x80 __do_irq+0xac/0x210 __do_IRQ+0x74/0xd0 0x0 do_IRQ+0x8c/0x170 hardware_interrupt_common_virt+0x29c/0x2a0 --- interrupt: 500 at queued_spin_lock_slowpath+0x4b8/0x1490 ..... NIP [c0000000000b6c28] queued_spin_lock_slowpath+0x4b8/0x1490 LR [c000000001037c5c] _raw_spin_lock+0x6c/0x90 --- interrupt: 500 0xc0000029c1a41d00 (unreliable) _raw_spin_lock+0x6c/0x90 futex_wake+0x100/0x260 do_futex+0x21c/0x2a0 sys_futex+0x98/0x270 system_call_exception+0x14c/0x2f0 system_call_vectored_common+0x15c/0x2ec The following code flow illustrates how the deadlock occurs. For the sake of brevity, assume that both locks (A and B) are contended and we call the queued_spin_lock_slowpath() function. CPU0 CPU1 ---- ---- spin_lock_irqsave(A) I spin_unlock_irqrestore(A) I spin_lock(B) I I I ▼ I id = qnodesp->count++; I (Note that nodes[0].lock == A) I I I ▼ I Interrupt I (happens before "nodes[0].lock = B") I I I ▼ I spin_lock_irqsave(A) I I I ▼ I id = qnodesp->count++ I nodes[1].lock = A I I I ▼ I Tail of MCS queue I I spin_lock_irqsave(A) ▼ I Head of MCS queue ▼ I CPU0 is previous tail ▼ I Spin indefinitely ▼ (until "nodes[1].next != NULL") prev = get_tail_qnode(A, CPU0) I ▼ prev == &qnodes[CPU0].nodes[0] (as qnodes ---truncated---	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46795	In the Linux kernel, the following vulnerability has been resolved: ksmbd: unset the binding mark of a reused connection Steve French reported null pointer dereference error from sha256 lib. cifs.ko can send session setup requests on reused connection. If reused connection is used for binding session, conn->binding can still remain true and generate_preauth_hash() will not set sess->Preauth_HashValue and it will be NULL. It is used as a material to create an encryption key in ksmbd_gen_smb311_encryptionkey. ->Preauth_HashValue cause null pointer dereference error from crypto_shash_update(). BUG: kernel NULL pointer dereference, address: 0000000000000000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP PTI CPU: 8 PID: 429254 Comm: kworker/8:39 Hardware name: LENOVO 20MAS08500/20MAS08500, BIOS N2CET69W (1.52) Workqueue: ksmbd-io handle_ksmbd_work [ksmbd] RIP: 0010:lib_sha256_base_do_update.isra.0+0x11e/0x1d0 [sha256_ssse3] <TASK> ? show_regs+0x6d/0x80 ? __die+0x24/0x80 ? page_fault_oops+0x99/0x1b0 ? do_user_addr_fault+0x2ee/0x6b0 ? exc_page_fault+0x83/0x1b0 ? asm_exc_page_fault+0x27/0x30 ? __pfx_sha256_transform_rorx+0x10/0x10 [sha256_ssse3] ? lib_sha256_base_do_update.isra.0+0x11e/0x1d0 [sha256_ssse3] ? __pfx_sha256_transform_rorx+0x10/0x10 [sha256_ssse3] ? __pfx_sha256_transform_rorx+0x10/0x10 [sha256_ssse3] _sha256_update+0x77/0xa0 [sha256_ssse3] sha256_avx2_update+0x15/0x30 [sha256_ssse3] crypto_shash_update+0x1e/0x40 hmac_update+0x12/0x20 crypto_shash_update+0x1e/0x40 generate_key+0x234/0x380 [ksmbd] generate_smb3encryptionkey+0x40/0x1c0 [ksmbd] ksmbd_gen_smb311_encryptionkey+0x72/0xa0 [ksmbd] ntlm_authenticate.isra.0+0x423/0x5d0 [ksmbd] smb2_sess_setup+0x952/0xaa0 [ksmbd] __process_request+0xa3/0x1d0 [ksmbd] __handle_ksmbd_work+0x1c4/0x2f0 [ksmbd] handle_ksmbd_work+0x2d/0xa0 [ksmbd] process_one_work+0x16c/0x350 worker_thread+0x306/0x440 ? __pfx_worker_thread+0x10/0x10 kthread+0xef/0x120 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x44/0x70 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1b/0x30 </TASK>	5.5	More Details
CVE-2024-46750	In the Linux kernel, the following vulnerability has been resolved: PCI: Add missing bridge lock to pci_bus_lock() One of the true positives that the cfg_access_lock lockdep effort identified is this sequence: WARNING: CPU: 14 PID: 1 at drivers/pci/pci.c:4886 pci_bridge_secondary_bus_reset+0x5d/0x70 RIP: 0010:pci_bridge_secondary_bus_reset+0x5d/0x70 Call Trace: <TASK> ? __warn+0x8c/0x190 ? pci_bridge_secondary_bus_reset+0x5d/0x70 ? report_bug+0x1f8/0x200 ? handle_bug+0x3c/0x70 ? exc_invalid_op+0x18/0x70 ? asm_exc_invalid_op+0x1a/0x20 ? pci_bridge_secondary_bus_reset+0x5d/0x70 pci_reset_bus+0x1d8/0x270 vmd_probe+0x778/0xa10 pci_device_probe+0x95/0x120 Where pci_reset_bus() users are triggering unlocked secondary bus resets. Ironically pci_bus_reset(), several calls down from pci_reset_bus(), uses pci_bus_lock() before issuing the reset which locks everything *but* the bridge itself. For the same motivation as adding: bridge = pci_upstream_bridge(dev); if (bridge) pci_dev_lock(bridge); to pci_reset_function() for the "bus" and "cxl_bus" reset cases, add pci_dev_lock() for @bus->self to pci_bus_lock(). [bhelgaas: squash in recursive locking deadlock fix from Keith Busch: https://lore.kernel.org/r/20240711193650.701834-1-kbusch@meta.com]	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46793	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: Boards: Fix NULL pointer deref in BYT/CHT boards harder Since commit 13f58267cda3 ("ASoC: soc.h: don't create dummy Component via COMP_DUMMY()") dummy codecs declared like this: SND_SOC_DAILINK_DEF(dummy, DAILINK_COMP_ARRAY(COMP_DUMMY())); expand to: static struct snd_soc_dai_link_component dummy[] = { }; Which means that dummy is a zero sized array and thus dais[i].codecs should not be dereferenced *at all* since it points to the address of the next variable stored in the data section as the "dummy" variable has an address but no size, so even dereferencing dais[0] is already an out of bounds array reference. Which means that the if (dais[i].codecs->name) check added in commit 7d99a70b6595 ("ASoC: Intel: Boards: Fix NULL pointer deref in BYT/CHT boards") relies on that the part of the next variable which the name member maps to just happens to be NULL. Which apparently so far it usually is, except when it isn't and then it results in crashes like this one: [28.795659] BUG: unable to handle page fault for address: 0000000000030011 ... [28.795780] Call Trace: [28.795787] <TASK> ... [28.795862] ? strcmp+0x18/0x40 [28.795872] 0xffffffffc150c605 [28.795887] platform_probe+0x40/0xa0 ... [28.795979] ? __pfx_init_module+0x10/0x10 [snd_soc_sst_bytcr_wm5102] Really fix things this time around by checking dais.num_codecs != 0.	5.5	More Details
CVE-2024-46791	In the Linux kernel, the following vulnerability has been resolved: can: mcp251x: fix deadlock if an interrupt occurs during mcp251x_open The mcp251x_hw_wake() function is called with the mpc_lock mutex held and disables the interrupt handler so that no interrupts can be processed while waking the device. If an interrupt has already occurred then waiting for the interrupt handler to complete will deadlock because it will be trying to acquire the same mutex. CPU0 CPU1 ---- ---- mcp251x_open() mutex_lock(&priv->mcp_lock) request_threaded_irq() <interrupt> mcp251x_can_ist() mutex_lock(&priv->mcp_lock) mcp251x_hw_wake() disable_irq() <-- deadlock Use disable_irq_nosync() instead because the interrupt handler does everything while holding the mutex so it doesn't matter if it's still running.	5.5	More Details
CVE-2024-46751	In the Linux kernel, the following vulnerability has been resolved: btrfs: don't BUG_ON() when 0 reference count at btrfs_lookup_extent_info() Instead of doing a BUG_ON() handle the error by returning -EUCLEAN, aborting the transaction and logging an error message.	5.5	More Details
CVE-2024-7846	YITH WooCommerce Ajax Search is vulnerable to a XSS vulnerability due to insufficient sanitization of user supplied block attributes. This makes it possible for Contributors+ attackers to inject arbitrary scripts.	5.4	More Details
CVE-2023-46948	A reflected Cross-Site Scripting (XSS) vulnerability was found on Temenos T24 Browser R19.40 that enables a remote attacker to execute arbitrary JavaScript code via the skin parameter in the about.jsp and genrequest.jsp components.	5.4	More Details
CVE-2024-8628	The Popup, Optin Form & Email Newsletters for Mailchimp, HubSpot, AWeber – MailOptin plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the plugin's 'post-meta' shortcode in all versions up to, and including, 1.2.70.3 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers, with contributor-level access and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.4	More Details
CVE-2024-47226	A stored cross-site scripting (XSS) vulnerability exists in NetBox 4.1.0 within the "Configuration History" feature of the "Admin" panel via a /core/config-revisions/ Add action. An authenticated user can inject arbitrary JavaScript or HTML into the "Top banner" field.	5.4	More Details
CVE-2024-5959	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Eliz Software Panel allows Stored XSS.This issue affects Panel: before v2.3.24.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47050	Prior to this patch being applied, Mautic's tracking was vulnerable to Cross-Site Scripting through the Page URL variable.	5.4	More Details
CVE-2024-45614	Puma is a Ruby/Rack web server built for parallelism. In affected versions clients could clobber values set by intermediate proxies (such as X-Forwarded-For) by providing a underscore version of the same header (X-Forwarded_For). Any users relying on proxy set variables is affected. v6.4.3/v5.6.9 now discards any headers using underscores if the non-underscore version also exists. Effectively, allowing the proxy defined headers to always win. Users are advised to upgrade. Nginx has a underscores_in_headers configuration variable to discard these headers at the proxy level as a mitigation. Any users that are implicitly trusting the proxy defined headers for security should immediately cease doing so until upgraded to the fixed versions.	5.4	More Details
CVE-2024-31167	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::QueuePropertyList::unpack13. This issue affects libfluid: 0.1.0.	5.3	More Details
CVE-2024-46979	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It's possible to get access to notification filters of any user by using a URL such as `<hostname>xwiki/bin/get/XWiki/Notifications/Code/NotificationFilterPreferenceLivetableResults?outputSyntax=plain&type=custom&user=<username>`. This vulnerability impacts all versions of XWiki since 13.2-rc-1. The filters do not provide much information (they mainly contain references which are public data in XWiki), though some info could be used in combination with other vulnerabilities. This vulnerability has been patched in XWiki 14.10.21, 15.5.5, 15.10.1, 16.0RC1. The patch consists in checking the rights of the user when sending the data. Users are advised to upgrade. It's possible to workaround the vulnerability by applying manually the patch: it's possible for an administrator to edit directly the document `XWiki.Notifications.Code.NotificationFilterPreferenceLivetableResults` to apply the same changes as in the patch. See commit c8c6545f9bde6f5aade994aa5b5903a67b5c2582.	5.3	More Details
CVE-2024-8651	A vulnerability in NetCat CMS allows an attacker to send a specially crafted http request that can be used to check whether a user exists in the system, which could be a basis for further attacks. This issue affects NetCat CMS v. 6.4.0.24126.2 and possibly others. Apply patch from vendor https://netcat.ru/ https://netcat.ru/] . Versions 6.4.0.24248 and on have the patch.	5.3	More Details
CVE-2024-45813	find-my-way is a fast, open source HTTP router, internally using a Radix Tree (aka compact Prefix Tree), supports route params, wildcards, and it's framework independent. A bad regular expression is generated any time one has two parameters within a single segment, when adding a `-` at the end, like `/:a-:b-`. This may cause a denial of service in some instances. Users are advised to update to find-my-way v8.2.2 or v9.0.1. or subsequent versions. There are no known workarounds for this issue.	5.3	More Details
CVE-2024-8891	An attacker with no knowledge of the current users in the web application, could build a dictionary of potential users and check the server responses as it indicates whether or not the user is present in CIRCUTOR Q-SMT in its firmware version 1.0.4.	5.3	More Details
CVE-2024-31198	Out-of-bounds Read vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::Port:unpack. This issue affects libfluid: 0.1.0.	5.3	More Details
CVE-2024-31197	Improper Null Termination vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of10::Port:unpack. This issue affects libfluid: 0.1.0.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-31196	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::ActionList::unpack10. This issue affects libfluid: 0.1.0.	5.3	More Details
CVE-2024-31185	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::MeterBandList::unpack. This issue affects libfluid: 0.1.0.	5.3	More Details
CVE-2024-31182	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::QueuePropertyList::unpack10. This issue affects libfluid: 0.1.0.	5.3	More Details
CVE-2024-31175	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::TablePropertiesList::unpack. This issue affects libfluid: 0.1.0.	5.3	More Details
CVE-2022-4533	The Limit Login Attempts Plus plugin for WordPress is vulnerable to IP Address Spoofing in versions up to, and including, 1.1.0. This is due to insufficient restrictions on where the 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 that will be logged and can be used to bypass settings that may have blocked out an IP address or country from logging in.	5.3	More Details
CVE-2024-8794	The BA Book Everything plugin for WordPress is vulnerable to arbitrary password reset in all versions up to, and including, 1.6.20. This is due to the reset_user_password() function not verifying a user's identity prior to setting a password. This makes it possible for unauthenticated attackers to reset any user's passwords, including administrators. It's important to note that the attacker will not have access to the generated password, therefore, privilege escalation is not possible.	5.3	More Details
CVE-2024-31165	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routine fluid_msg::of13::SetFieldAction::unpack. This issue affects libfluid: 0.1.0.	5.3	More Details
CVE-2024-6787	This vulnerability occurs when an attacker exploits a race condition between the time a file is checked and the time it is used (TOCTOU). By exploiting this race condition, an attacker can write arbitrary files to the system. This could allow the attacker to execute malicious code and potentially cause file losses.	5.3	More Details
CVE-2024-31164	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routines fluid_msg::ActionList::unpack13. This issue affects libfluid: 0.1.0.	5.3	More Details
CVE-2024-23916	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routines fluid_msg::ActionSet::unpack. This issue affects libfluid: 0.1.0.	5.3	More Details
CVE-2024-23915	Unchecked Return Value to NULL Pointer Dereference vulnerability in Open Networking Foundation (ONF) libfluid (libfluid_msg module). This vulnerability is associated with program routines fluid_msg::of13::InstructionSet::unpack. This issue affects libfluid: 0.1.0.	5.3	More Details
CVE-2024-8892	Vulnerability in CIRCUTOR TCP2RS+ firmware version 1.3b, which could allow an attacker to modify any configuration value, even if the device has the user/password authentication option enabled, without authentication by sending packets through the UDP protocol and port 2000, deconfiguring the device and thus disabling its use. This equipment is at the end of its useful life cycle.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-6641	The WP Hardening – Fix Your WordPress Security plugin for WordPress is vulnerable to Security Feature Bypass in all versions up to, and including, 1.2.6. This is due to use of an incorrect regular expression within the "Stop User Enumeration" feature. This makes it possible for unauthenticated attackers to bypass intended security restrictions and expose site usernames.	5.3	More Details
CVE-2024-45809	Envoy is a cloud-native high-performance edge/middle/service proxy. Jwt filter will lead to an Envoy crash when clear route cache with remote JWKs. In the following case: 1. remote JWKs are used, which requires async header processing; 2. clear_route_cache is enabled on the provider; 3. header operations are enabled in JWT filter, e.g. header to claims feature; 4. the routing table is configured in a way that the JWT header operations modify requests to not match any route. When these conditions are met, a crash is triggered in the upstream code due to nullptr reference conversion from route(). The root cause is the ordering of continueDecoding and clearRouteCache. This issue has been addressed in versions 1.31.2, 1.30.6, and 1.29.9. Users are advised to upgrade. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2024-46990	Directus is a real-time API and App dashboard for managing SQL database content. When relying on blocking access to localhost using the default `0.0.0.0` filter a user may bypass this block by using other registered loopback devices (like `127.0.0.2` - `127.127.127.127`). This issue has been addressed in release versions 10.13.3 and 11.1.0. Users are advised to upgrade. Users unable to upgrade may block this bypass by manually adding the `127.0.0.0/8` CIDR range which will block access to any `127.X.X.X` ip instead of just `127.0.0.1`.	5.0	More Details
CVE-2024-43188	IBM Business Automation Workflow 22.0.2, 23.0.1, 23.0.2, and 24.0.0 could allow a privileged user to perform unauthorized activities due to improper client side validation.	4.9	More Details
CVE-2024-38266	An improper restriction of operations within the bounds of a memory buffer in the parameter type parser of the Zyxel VMG8825-T50K firmware versions through 5.50(ABOM.8)C0 could allow an authenticated attacker with administrator privileges to cause potential memory corruptions, resulting in a thread crash on an affected device.	4.9	More Details
CVE-2024-38267	An improper restriction of operations within the bounds of a memory buffer in the IPv6 address parser of the Zyxel VMG8825-T50K firmware versions through 5.50(ABOM.8)C0 could allow an authenticated attacker with administrator privileges to cause potential memory corruptions, resulting in a thread crash on an affected device.	4.9	More Details
CVE-2024-38268	An improper restriction of operations within the bounds of a memory buffer in the MAC address parser of the Zyxel VMG8825-T50K firmware versions through 5.50(ABOM.8)C0 could allow an authenticated attacker with administrator privileges to cause potential memory corruptions, resulting in a thread crash on an affected device.	4.9	More Details
CVE-2024-38269	An improper restriction of operations within the bounds of a memory buffer in the USB file-sharing handler of the Zyxel VMG8825-T50K firmware versions through 5.50(ABOM.8)C0 could allow an authenticated attacker with administrator privileges to cause potential memory corruptions, resulting in a thread crash on an affected device.	4.9	More Details
CVE-2022-25774	Prior to the patched version, logged in users of Mautic are vulnerable to a self XSS vulnerability in the notifications within Mautic. Users could inject malicious code into the notification when saving Dashboards.	4.8	More Details
CVE-2024-8758	The Quiz and Survey Master (QSM) WordPress plugin before 9.1.3 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46654	A stored cross-site scripting (XSS) vulnerability in the Add Scheduled Task module of Maccms10 v2024.1000.4040 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	4.8	More Details
CVE-2024-37879	Improper input validation in /admin/config/save in User-friendly SVN (USVN) before v1.0.12 and below allows administrators to execute arbitrary code via the fields "siteTitle", "siteIco" and "siteLogo".	4.8	More Details
CVE-2024-45793	Confidant is a open source secret management service that provides user-friendly storage and access to secrets. The following endpoints are subject to a cross site scripting vulnerability: GET /v1/credentials, GET /v1/credentials/, GET /v1/archive/credentials/, GET /v1/archive/credentials, POST /v1/credentials, PUT /v1/credentials/, PUT /v1/credentials//<to_revision>, GET /v1/services, GET /v1/services/, GET /v1/archive/services/, GET /v1/archive/services, PUT /v1/services/, PUT /v1/services//<to_revision>. The attacker needs to be authenticated and have privileges to create new credentials, but could use this to show information and run scripts to other users into the same Confidant instance. This issue has been patched in version 6.6.2. All users are advised to upgrade. There are no known workarounds for this vulnerability.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46787	In the Linux kernel, the following vulnerability has been resolved: userfaultfd: fix checks for huge PMDs Patch series "userfaultfd: fix races around pmd_trans_huge() check", v2. The pmd_trans_huge() code in mfill_atomic() is wrong in three different ways depending on kernel version: 1. The pmd_trans_huge() check is racy and can lead to a BUG_ON() (if you hit the right two race windows) - I've tested this in a kernel build with some extra mdelay() calls. See the commit message for a description of the race scenario. On older kernels (before 6.5), I think the same bug can even theoretically lead to accessing transhuge page contents as a page table if you hit the right 5 narrow race windows (I haven't tested this case). 2. As pointed out by Qi Zheng, pmd_trans_huge() is not sufficient for detecting PMDs that don't point to page tables. On older kernels (before 6.5), you'd just have to win a single fairly wide race to hit this. I've tested this on 6.1 stable by racing migration (with a mdelay() patched into try_to_migrate()) against UFFDIO_ZEROPAGE - on my x86 VM, that causes a kernel oops in ptlock_ptr(). 3. On newer kernels (>=6.5), for shmem mappings, khugepaged is allowed to yank page tables out from under us (though I haven't tested that), so I think the BUG_ON() checks in mfill_atomic() are just wrong. I decided to write two separate fixes for these (one fix for bugs 1+2, one fix for bug 3), so that the first fix can be backported to kernels affected by bugs 1+2. This patch (of 2): This fixes two issues. I discovered that the following race can occur: mfill_atomic other thread ========== ========== <zap PMD> pmdp_get_lockless() [reads none pmd] <bail if trans_huge> <if none:> <pagefault creates transhuge zeropage> __pte_alloc [no-op] <zap PMD> <bail if pmd_trans_huge(*dst_pmd)> BUG_ON(pmd_none(*dst_pmd)) I have experimentally verified this in a kernel with extra mdelay() calls; the BUG_ON(pmd_none(*dst_pmd)) triggers. On kernels newer than commit 0d940a9b270b ("mm/pgtable: allow pte_offset_map[_lock]() to fail"), this can't lead to anything worse than a BUG_ON(), since the page table access helpers are actually designed to deal with page tables concurrently disappearing; but on older kernels (<=6.4), I think we could probably theoretically race past the two BUG_ON() checks and end up treating a hugepage as a page table. The second issue is that, as Qi Zheng pointed out, there are other types of huge PMDs that pmd_trans_huge() can't catch: devmap PMDs and swap PMDs (in particular, migration PMDs). On <=6.4, this is worse than the first issue: If mfill_atomic() runs on a PMD that contains a migration entry (which just requires winning a single, fairly wide race), it will pass the PMD to pte_offset_map_lock(), which assumes that the PMD points to a page table. Breakage follows: First, the kernel tries to take the PTE lock (which will crash or maybe worse if there is no "struct page" for the address bits in the migration entry PMD - I think at least on X86 there usually is no corresponding "struct page" thanks to the PTE inversion mitigation, amd64 looks different). If that didn't crash, the kernel would next try to write a PTE into what it wrongly thinks is a page table. As part of fixing these issues, get rid of the check for pmd_trans_huge() before __pte_alloc() - that's redundant, we're going to have to check for that after the __pte_alloc() anyway. Backport note: pmdp_get_lockless() is pmd_read_atomic() in older kernels.	4.7	More Details
CVE-2024-9076	A vulnerability was found in DedeCMS up to 5.7.115. It has been rated as critical. This issue affects some unknown processing of the file /dede/article_string_mix.php. The manipulation leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details
CVE-2022-39068	There is a buffer overflow vulnerability in ZTE MF296R. Due to insufficient validation of the SMS parameter length, an authenticated attacker could use the vulnerability to perform a denial of service attack.	4.5	More Details
CVE-2024-45770	A vulnerability was found in Performance Co-Pilot (PCP). This flaw can only be exploited if an attacker has access to a compromised PCP system account. The issue is related to the pmpost tool, which is used to log messages in the system. Under certain conditions, it runs with high-level privileges.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8680	The MC4WP: Mailchimp for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via admin settings in all versions up to, and including, 4.9.16 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	4.4	More Details
CVE-2024-9003	A vulnerability was found in Jinan Chicheng Company JFlow 2.0.0. It has been rated as problematic. This issue affects the function AttachmentUploadController of the file /WF/Ath/EntityMutliFile_Load.do of the component Attachment Handler. The manipulation of the argument oid leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	4.3	More Details
CVE-2024-38221	Microsoft Edge (Chromium-based) Spoofing Vulnerability	4.3	More Details
CVE-2023-7281	Inappropriate implementation in Compositing in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-7020	Inappropriate implementation in Autofill in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2024-7022	Uninitialized Use in V8 in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2024-9038	A vulnerability classified as problematic was found in Codezips Online Shopping Portal 1.0. Affected by this vulnerability is an unknown functionality of the file insert-product.php. The manipulation of the argument productimage1/productimage2/productimage3 leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	4.3	More Details
CVE-2024-8432	The Appointment & Event Booking Calendar Plugin – Webba Booking plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on the save_appearance() function in all versions up to, and including, 5.0.48. This makes it possible for authenticated attackers, with Subscriber-level access and above, to modify the booking form's CSS.	4.3	More Details
CVE-2024-47060	Zitadel is an open source identity management platform. In Zitadel, even after an organization is deactivated, associated projects, respectively their applications remain active. Users across other organizations can still log in and access through these applications, leading to unauthorized access. Additionally, if a project was deactivated access to applications was also still possible. The issue stems from the fact that when an organization is deactivated in Zitadel, the applications associated with it do not automatically deactivate. The application lifecycle is not tightly coupled with the organization's lifecycle, leading to a situation where the organization or project is marked as inactive, but its resources remain accessible. This vulnerability allows for unauthorized access to projects and their resources, which should have been restricted post-organization deactivation. Versions 2.62.1, 2.61.1, 2.60.2, 2.59.3, 2.58.5, 2.57.5, 2.56.6, 2.55.8, and 2.54.10 have been released which address this issue. Users are advised to upgrade. Users unable to upgrade may explicitly disable the application to make sure the client is not allowed anymore.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-7019	Inappropriate implementation in UI in Google Chrome prior to 124.0.6367.60 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-7282	Inappropriate implementation in Navigation in Google Chrome prior to 113.0.5672.63 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2024-47159	In JetBrains YouTrack before 2024.3.44799 user without appropriate permissions could restore workflows attached to a project	4.3	More Details
CVE-2024-47059	When logging in with the correct username and incorrect weak password, the user receives the notification, that their password is too weak. However when an incorrect username is provided alongside with a weak password, the application responds with 'Invalid credentials' notification. This difference could be used to perform username enumeration.	4.3	More Details
CVE-2024-45298	Wiki.js is an open source wiki app built on Node.js. A disabled user can still gain access to a wiki by abusing the password reset function. While setting up SMTP e-mail's on my server, I tested said e-mails by performing a password reset with my test user. To my shock, not only did it let me reset my password, but after resetting my password I can get into the wiki I was locked out of. The ramifications of this bug is a user can **bypass an account disabling by requesting their password be reset**. All users of wiki.js version `2.5.303` who use any account restrictions and have disabled user are affected. This issue has been addressed in version 2.5.304 and all users are advised to upgrade. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2024-47160	In JetBrains YouTrack before 2024.3.44799 access to global app config data without appropriate permissions was possible	4.3	More Details
CVE-2024-39081	An issue in SMART TYRE CAR & BIKE v4.2.0 allows attackers to perform a man-in-the-middle attack via Bluetooth communications.	4.2	More Details
CVE-2024-47162	In JetBrains YouTrack before 2024.3.44799 token could be revealed on Imports page	4.1	More Details
CVE-2024-8612	A flaw was found in QEMU, in the virtio-scsi, virtio-blk, and virtio-crypto devices. The size for virtqueue_push as set in virtio_scsi_complete_req / virtio_blk_req_complete / virito_crypto_req_complete could be larger than the true size of the data which has been sent to guest. Once virtqueue_push() finally calls dma_memory_unmap to ummap the in_iov, it may call the address_space_write function to write back the data. Some uninitialized data may exist in the bounce.buffer, leading to an information leak.	3.8	More Details
CVE-2024-46989	spicedb is an Open Source, Google Zanzibar-inspired permissions database to enable fine-grained authorization for customer applications. Multiple caveats over the same indirect subject type on the same relation can result in no permission being returned when permission is expected. If the resource has multiple groups, and each group is caveated, it is possible for the returned permission to be "no permission" when permission is expected. Permission is returned as NO_PERMISSION when PERMISSION is expected on the CheckPermission API. This issue has been addressed in release version 1.35.3. Users are advised to upgrade. Users unable to upgrade should not use caveats or avoid the use of caveats on an indirect subject type with multiple entries.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-45453	Authentication Bypass by Spoofing vulnerability in Peter Hardy-vanDoorn Maintenance Redirect allows Accessing Functionality Not Properly Constrained by ACLs.This issue affects Maintenance Redirect: from n/a through 2.0.1.	3.7	More Details
CVE-2024-9030	A vulnerability classified as problematic was found in CodeCanyon CRMGo SaaS 7.2. This vulnerability affects unknown code of the file /deal/{note_id}/note. The manipulation of the argument notes leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-9084	A vulnerability classified as problematic was found in code-projects Blood Bank System 1.0. This vulnerability affects unknown code of the file bbms.php. The manipulation of the argument fullname/age/bloodgroup/city/phno/gender as part of String leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-9089	A vulnerability was found in SourceCodester Modern Loan Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file update_loan_record.php. The manipulation of the argument amount leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-9033	A vulnerability has been found in SourceCodester Best House Rental Management System 1.0 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /ajax.php?action=save_category. The manipulation of the argument name leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-9092	A vulnerability was found in SourceCodester Profile Registration without Reload Refresh 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file add.php of the component Registration Form. The manipulation of the argument full_name leads to cross site scripting. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Other parameters might be affected as well.	3.5	More Details
CVE-2024-9031	A vulnerability, which was classified as problematic, has been found in CodeCanyon CRMGo SaaS up to 7.2. This issue affects some unknown processing of the file /project/task/{task_id}/show. The manipulation of the argument comment leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	3.5	More Details
CVE-2024-9007	A vulnerability classified as problematic has been found in jeanmarc77 123solar 1.8.4.5. This affects an unknown part of the file /detailed.php. The manipulation of the argument date1 leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The patch is named 94bf9ab7ad0ccb7fbdc02f172f37f0e2ea08d48f. It is recommended to apply a patch to fix this issue.	3.5	More Details
CVE-2024-9077	A vulnerability classified as problematic has been found in dingfangzu up to 29d67d9044f6f93378e6eb6ff92272217ff7225c. Affected is an unknown function of the file scripts/order.js of the component Order Checkout. The manipulation of the argument address-name leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. This product is using a rolling release to provide continious delivery. Therefore, no version details for affected nor updated releases are available. The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2024-46792	In the Linux kernel, the following vulnerability has been resolved: riscv: misaligned: Restrict user access to kernel memory raw_copy_{to,from}_user() do not call access_ok(), so this code allowed userspace to access any virtual memory address.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46794	In the Linux kernel, the following vulnerability has been resolved: x86/tdx: Fix data leak in mmio_read() The mmio_read() function makes a TDVMCALL to retrieve MMIO data for an address from the VMM. Sean noticed that mmio_read() unintentionally exposes the value of an initialized variable (val) on the stack to the VMM. This variable is only needed as an output value. It did not need to be passed to the VMM in the first place. Do not send the original value of *val to the VMM. [dhansen: clarify what 'val' is used for.]	3.3	More Details
CVE-2024-9048	A vulnerability was found in y_project RuoYi up to 4.7.9. It has been declared as problematic. Affected by this vulnerability is the function SysUserServiceImpl of the file ruoyi-system/src/main/java/com/ruoyi/system/service/impl/SysUserServiceImpl.java of the component Backend User Import. The manipulation of the argument loginName leads to cross site scripting. The attack can be launched remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The patch is named 9b68013b2af87b9c809c4637299abd929bc73510. It is recommended to apply a patch to fix this issue.	3.1	More Details
CVE-2024-47058	With access to edit a Mautic form, the attacker can add Cross-Site Scripting stored in the html filed. This could be used to steal sensitive information from the user's current session.	2.9	More Details
CVE-2024-8263	An improper privilege management vulnerability allowed arbitrary workflows to be committed using an improperly scoped PAT through the use of nested tags. This vulnerability affected all versions of GitHub Enterprise Server and was fixed in version 3.10.17, 3.11.15, 3.12.9, 3.13.4, and 3.14.1. This vulnerability was reported via the GitHub Bug Bounty program.	2.7	More Details
CVE-2024-9075	A vulnerability was found in Stirling-Tools Stirling-PDF up to 0.28.3. It has been declared as problematic. This vulnerability affects unknown code of the component Markdown-to-PDF. The manipulation leads to cross site scripting. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. Upgrading to version 0.29.0 is able to address this issue. It is recommended to upgrade the affected component. The vendor explains that "this functionality was removed in 0.29.0 already" and "we plan to re-add at later date with issue resolved".	2.6	More Details
CVE-2024-9083	A vulnerability classified as problematic has been found in SourceCodester Employee Management System 1.0. This affects an unknown part of the file /Admin/add-admin.php. The manipulation of the argument txtfullname leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2.4	More Details
CVE-2024-9040	A vulnerability, which was classified as problematic, was found in code-projects Blood Bank Management System 1.0. This affects an unknown part of the component Password Handler. The manipulation leads to cleartext storage in a file or on disk. An attack has to be approached locally.	2.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-47062	Navidrome is an open source web-based music collection server and streamer. Navidrome automatically adds parameters in the URL to SQL queries. This can be exploited to access information by adding parameters like `password=...` in the URL (ORM Leak). Furthermore, the names of the parameters are not properly escaped, leading to SQL Injections. Finally, the username is used in a `LIKE` statement, allowing people to log in with `%` instead of their username. When adding parameters to the URL, they are automatically included in an SQL `LIKE` statement (depending on the parameter's name). This allows attackers to potentially retrieve arbitrary information. For example, attackers can use the following request to test whether some encrypted passwords start with `AAA`. This results in an SQL query like `password LIKE 'AAA%'`, allowing attackers to slowly brute-force passwords. When adding parameters to the URL, they are automatically added to an SQL query. The names of the parameters are not properly escaped. This behavior can be used to inject arbitrary SQL code (SQL Injection). These vulnerabilities can be used to leak information and dump the contents of the database and have been addressed in release version 0.53.0. Users are advised to upgrade. There are no known workarounds for this vulnerability.	N/A	More Details
CVE-2024-46718	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Don't overmap identity VRAM mapping Overmapping the identity VRAM mapping is triggering hardware bugs on certain platforms. Use 2M pages for the last unaligned (to 1G) VRAM chunk. v2: - Always use 2M pages for last chunk (Fei Yang) - break loop when 2M pages are used - Add assert for usable_size being 2M aligned v3: - Fix checkpatch	N/A	More Details
CVE-2024-46729	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix incorrect size calculation for loop [WHY] fe_clk_en has size of 5 but sizeof(fe_clk_en) has byte size 20 which is lager than the array size. [HOW] Divide byte size 20 by its element size. This fixes 2 OVERRUN issues reported by Coverity.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46733	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix qgroup reserve leaks in cow_file_range In the buffered write path, the dirty page owns the qgroup reserve until it creates an ordered_extent. Therefore, any errors that occur before the ordered_extent is created must free that reservation, or else the space is leaked. The fstest generic/475 exercises various IO error paths, and is able to trigger errors in cow_file_range where we fail to get to allocating the ordered extent. Note that because we *do* clear delalloc, we are likely to remove the inode from the delalloc list, so the inodes/pages to not have invalidate/launder called on them in the commit abort path. This results in failures at the unmount stage of the test that look like: BTRFS: error (device dm-8 state EA) in cleanup_transaction:2018: errno=-5 IO failure BTRFS: error (device dm-8 state EA) in btrfs_replace_file_extents:2416: errno=-5 IO failure BTRFS warning (device dm-8 state EA): qgroup 0/5 has unreleased space, type 0 rsv 28672 ------------[cut here]------------ WARNING: CPU: 3 PID: 22588 at fs/btrfs/disk-io.c:4333 close_ctree+0x222/0x4d0 [btrfs] Modules linked in: btrfs blake2b_generic libcrc32c xor zstd_compress raid6_pq CPU: 3 PID: 22588 Comm: umount Kdump: loaded Tainted: G W 6.10.0-rc7-gab56fde445b8 #21 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS Arch Linux 1.16.3-1-1 04/01/2014 RIP: 0010:close_ctree+0x222/0x4d0 [btrfs] RSP: 0018:ffffb4465283be00 EFLAGS: 00010202 RAX: 0000000000000001 RBX: ffffa1a1818e1000 RCX: 0000000000000001 RDX: 0000000000000000 RSI: ffffb4465283bbe0 RDI: ffffa1a19374fcb8 RBP: ffffa1a1818e13c0 R08: 0000000100028b16 R09: 0000000000000000 R10: 0000000000000003 R11: 0000000000000003 R12: ffffa1a18ad7972c R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 00007f9168312b80(0000) GS:ffffa1a4afcc0000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f91683c9140 CR3: 000000010acaa000 CR4: 00000000000006f0 Call Trace: <TASK> ? close_ctree+0x222/0x4d0 [btrfs] ? __warn.cold+0x8e/0xea ? close_ctree+0x222/0x4d0 [btrfs] ? report_bug+0xff/0x140 ? handle_bug+0x3b/0x70 ? exc_invalid_op+0x17/0x70 ? asm_exc_invalid_op+0x1a/0x20 ? close_ctree+0x222/0x4d0 [btrfs] generic_shutdown_super+0x70/0x160 kill_anon_super+0x11/0x40 btrfs_kill_super+0x11/0x20 [btrfs] deactivate_locked_super+0x2e/0xa0 cleanup_mnt+0xb5/0x150 task_work_run+0x57/0x80 syscall_exit_to_user_mode+0x121/0x130 do_syscall_64+0xab/0x1a0 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f916847a887 ---[end trace 0000000000000000]--- BTRFS error (device dm-8 state EA): qgroup reserved space leaked Cases 2 and 3 in the out_reserve path both pertain to this type of leak and must free the reserved qgroup data. Because it is already an error path, I opted not to handle the possible errors in btrfs_free_qgroup_data.	N/A	More Details
CVE-2024-46736	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix double put of @cfile in smb2_rename_path() If smb2_set_path_attr() is called with a valid @cfile and returned -EINVAL, we need to call cifs_get_writable_path() again as the reference of @cfile was already dropped by previous smb2_compound_op() call.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46734	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix race between direct IO write and fsync when using same fd If we have 2 threads that are using the same file descriptor and one of them is doing direct IO writes while the other is doing fsync, we have a race where we can end up either: 1) Attempt a fsync without holding the inode's lock, triggering an assertion failures when assertions are enabled; 2) Do an invalid memory access from the fsync task because the file private points to memory allocated on stack by the direct IO task and it may be used by the fsync task after the stack was destroyed. The race happens like this: 1) A user space program opens a file descriptor with O_DIRECT; 2) The program spawns 2 threads using libpthread for example; 3) One of the threads uses the file descriptor to do direct IO writes, while the other calls fsync using the same file descriptor. 4) Call task A the thread doing direct IO writes and task B the thread doing fsyncs; 5) Task A does a direct IO write, and at btrfs_direct_write() sets the file's private to an on stack allocated private with the member 'fsync_skip_inode_lock' set to true; 6) Task B enters btrfs_sync_file() and sees that there's a private structure associated to the file which has 'fsync_skip_inode_lock' set to true, so it skips locking the inode's VFS lock; 7) Task A completes the direct IO write, and resets the file's private to NULL since it had no prior private and our private was stack allocated. Then it unlocks the inode's VFS lock; 8) Task B enters btrfs_get_ordered_extents_for_logging(), then the assertion that checks the inode's VFS lock is held fails, since task B never locked it and task A has already unlocked it. The stack trace produced is the following: assertion failed: inode_is_locked(&inode->vfs_inode), in fs/btrfs/ordered-data.c:983 ------------[cut here]------------ kernel BUG at fs/btrfs/ordered-data.c:983! Oops: invalid opcode: 0000 [#1] PREEMPT SMP PTI CPU: 9 PID: 5072 Comm: worker Tainted: G U OE 6.10.5-1-default #1 openSUSE Tumbleweed 69f48d427608e1c09e60ea24c6c55e2ca1b049e8 Hardware name: Acer Predator PH315-52/Covini_CFS, BIOS V1.12 07/28/2020 RIP: 0010:btrfs_get_ordered_extents_for_logging.cold+0x1f/0x42 [btrfs] Code: 50 d6 86 c0 e8 (...) RSP: 0018:ffff9e4a03dcfc78 EFLAGS: 00010246 RAX: 0000000000000054 RBX: ffff9078a9868e98 RCX: 0000000000000000 RDX: 0000000000000000 RSI: ffff907dce4a7800 RDI: ffff907dce4a7800 RBP: ffff907805518800 R08: 0000000000000000 R09: ffff9e4a03dcfb38 R10: ffff9e4a03dcfb30 R11: 0000000000000003 R12: ffff907684ae7800 R13: 0000000000000001 R14: ffff90774646b600 R15: 0000000000000000 FS: 00007f04b96006c0(0000) GS:ffff907dce480000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f32acbfc000 CR3: 00000001fd4fa005 CR4: 00000000003726f0 Call Trace: <TASK> ? __die_body.cold+0x14/0x24 ? die+0x2e/0x50 ? do_trap+0xca/0x110 ? do_error_trap+0x6a/0x90 ? btrfs_get_ordered_extents_for_logging.cold+0x1f/0x42 [btrfs bb26272d49b4cdc847cf3f7faadd459b62caee9a] ? exc_invalid_op+0x50/0x70 ? btrfs_get_ordered_extents_for_logging.cold+0x1f/0x42 [btrfs bb26272d49b4cdc847cf3f7faadd459b62caee9a] ? asm_exc_invalid_op+0x1a/0x20 ? btrfs_get_ordered_extents_for_logging.cold+0x1f/0x42 [btrfs bb26272d49b4cdc847cf3f7faadd459b62caee9a] ? btrfs_get_ordered_extents_for_logging.cold+0x1f/0x42 [btrfs bb26272d49b4cdc847cf3f7faadd459b62caee9a] btrfs_sync_file+0x21a/0x4d0 [btrfs bb26272d49b4cdc847cf3f7faadd459b62caee9a] ? __seccomp_filter+0x31d/0x4f0 __x64_sys_fdatasync+0x4f/0x90 do_syscall_64+0x82/0x160 ? do_futex+0xcb/0x190 ? __x64_sys_futex+0x10e/0x1d0 ? switch_fpu_return+0x4f/0xd0 ? syscall_exit_to_user_mode+0x72/0x220 ? do_syscall_64+0x8e/0x160 ? syscall_exit_to_user_mod ---truncated---	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46717	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: SHAMPO, Fix incorrect page release Under the following conditions: 1) No skb created yet 2) header_size == 0 (no SHAMPO header) 3) header_index + 1 % MLX5E_SHAMPO_WQ_HEADER_PER_PAGE == 0 (this is the last page fragment of a SHAMPO header page) a new skb is formed with a page that is NOT a SHAMPO header page (it is a regular data page). Further down in the same function (mlx5e_handle_rx_cqe_mpwrq_shampo()), a SHAMPO header page from header_index is released. This is wrong and it leads to SHAMPO header pages being released more than once.	N/A	More Details
CVE-2024-46716	In the Linux kernel, the following vulnerability has been resolved: dmaengine: altera-msgdma: properly free descriptor in msgdma_free_descriptor Remove list_del call in msgdma_chan_desc_cleanup, this should be the role of msgdma_free_descriptor. In consequence replace list_add_tail with list_move_tail in msgdma_free_descriptor. This fixes the path: msgdma_free_chan_resources -> msgdma_free_descriptors -> msgdma_free_desc_list -> msgdma_free_descriptor which does not correctly free the descriptors as first nodes were not removed from the list.	N/A	More Details
CVE-2024-46715	In the Linux kernel, the following vulnerability has been resolved: driver: iio: add missing checks on iio_info's callback access Some callbacks from iio_info structure are accessed without any check, so if a driver doesn't implement them trying to access the corresponding sysfs entries produce a kernel oops such as: [2203.527791] Unable to handle kernel NULL pointer dereference at virtual address 00000000 when execute [...] [2203.783416] Call trace: [2203.783429] iio_read_channel_info_avail from dev_attr_show+0x18/0x48 [2203.789807] dev_attr_show from sysfs_kf_seq_show+0x90/0x120 [2203.794181] sysfs_kf_seq_show from seq_read_iter+0xd0/0x4e4 [2203.798555] seq_read_iter from vfs_read+0x238/0x2a0 [2203.802236] vfs_read from ksys_read+0xa4/0xd4 [2203.805385] ksys_read from ret_fast_syscall+0x0/0x54 [2203.809135] Exception stack(0xe0badfa8 to 0xe0badff0) [2203.812880] dfa0: 00000003 b6f10f80 00000003 b6eab000 00020000 00000000 [2203.819746] dfc0: 00000003 b6f10f80 7ff00000 00000003 00000003 00000000 00020000 00000000 [2203.826619] dfe0: b6e1bc88 bed80958 b6e1bc94 b6e1bcb0 [2203.830363] Code: bad PC value [2203.832695] ---[end trace 0000000000000000]---	N/A	More Details
CVE-2024-7785	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Ece Software Electronic Ticket System allows Reflected XSS, Cross-Site Scripting (XSS).This issue affects Electronic Ticket System: before 2024.08.	N/A	More Details
CVE-2024-46745	In the Linux kernel, the following vulnerability has been resolved: Input: uinput - reject requests with unreasonable number of slots When exercising uinput interface syzkaller may try setting up device with a really large number of slots, which causes memory allocation failure in input_mt_init_slots(). While this allocation failure is handled properly and request is rejected, it results in syzkaller reports. Additionally, such request may put undue burden on the system which will try to free a lot of memory for a bogus request. Fix it by limiting allowed number of slots to 100. This can easily be extended if we see devices that can track more than 100 contacts.	N/A	More Details
CVE-2024-7207	Rejected reason: Duplicate of CVE-2024-45806.	N/A	More Details
CVE-2024-7254	Any project that parses untrusted Protocol Buffers data containing an arbitrary number of nested groups / series of SGROUP tags can corrupted by exceeding the stack limit i.e. StackOverflow. Parsing nested groups as unknown fields with DiscardUnknownFieldsParser or Java Protobuf Lite parser, or against Protobuf map fields, creates unbounded recursions that can be abused by an attacker.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-8375	There exists a use after free vulnerability in Reverb. Reverb supports the VARIANT datatype, which is supposed to represent an arbitrary object in C++. When a tensor proto of type VARIANT is unpacked, memory is first allocated to store the entire tensor, and a ctor is called on each instance. Afterwards, Reverb copies the content in tensor_content to the previously mentioned pre-allocated memory, which results in the bytes in tensor_content overwriting the vtable pointers of all the objects which were previously allocated. Reverb exposes 2 relevant gRPC endpoints: InsertStream and SampleStream. The attacker can insert this stream into the server's database, then when the client next calls SampleStream they will unpack the tensor into RAM, and when any method on that object is called (including its destructor) the attacker gains control of the Program Counter. We recommend upgrading past git commit https://github.com/google-deepmind/reverb/commit/6a0dcf4c9e842b7f999912f792aaa6f6bd261a25	N/A	More Details
CVE-2024-6878	Files or Directories Accessible to External Parties vulnerability in Eliz Software Panel allows Collect Data from Common Resource Locations.This issue affects Panel: before v2.3.24.	N/A	More Details
CVE-2024-45229	The Versa Director offers REST APIs for orchestration and management. By design, certain APIs, such as the login screen, banner display, and device registration, do not require authentication. However, it was discovered that for Directors directly connected to the Internet, one of these APIs can be exploited by injecting invalid arguments into a GET request, potentially exposing the authentication tokens of other currently logged-in users. These tokens can then be used to invoke additional APIs on port 9183. This exploit does not disclose any username or password information. Currently, there are no workarounds in Versa Director. However, if there is Web Application Firewall (WAF) or API Gateway fronting the Versa Director, it can be used to block access to the URLs of vulnerable API. /vnms/devicereg/device/* (on ports 9182 & 9183) and /versa/vnms/devicereg/device/* (on port 443). Versa recommends that Directors be upgraded to one of the remediated software versions. This vulnerability is not exploitable on Versa Directors not exposed to the Internet.We have validated that no Versa-hosted head ends have been affected by this vulnerability. Please contact Versa Technical Support or Versa account team for any further assistance.	N/A	More Details
CVE-2022-48945	In the Linux kernel, the following vulnerability has been resolved: media: vivid: fix compose size exceed boundary syzkaller found a bug: BUG: unable to handle page fault for address: ffffc9000a3b1000 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 100000067 P4D 100000067 PUD 10015f067 PMD 1121ca067 PTE 0 Oops: 0002 [#1] PREEMPT SMP CPU: 0 PID: 23489 Comm: vivid-000-vid-c Not tainted 6.1.0-rc1+ #512 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.13.0-1ubuntu1.1 04/01/2014 RIP: 0010:memcpy_erms+0x6/0x10 [...] Call Trace: <TASK> ? tpg_fill_plane_buffer+0x856/0x15b0 vivid_fillbuff+0x8ac/0x1110 vivid_thread_vid_cap_tick+0x361/0xc90 vivid_thread_vid_cap+0x21a/0x3a0 kthread+0x143/0x180 ret_from_fork+0x1f/0x30 </TASK> This is because we forget to check boundary after adjust compose->height int V4L2_SEL_TGT_CROP case. Add v4l2_rect_map_inside() to fix this problem for this case.	N/A	More Details
CVE-2024-7735	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Exnet Informatics Software Ferry Reservation System allows SQL Injection.This issue affects Ferry Reservation System: before 240805-002.	N/A	More Details
CVE-2024-7835	Improper Neutralization of Input During Web Page Generation (XSS or 'Cross-site Scripting') vulnerability in Exnet Informatics Software Ferry Reservation System allows Reflected XSS.This issue affects Ferry Reservation System: before 240805-002.	N/A	More Details
CVE-2024-47219	An issue was discovered in vesoft NebulaGraph through 3.8.0. It allows shell command injection.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2024-46748	In the Linux kernel, the following vulnerability has been resolved: cachefiles: Set the max subreq size for cache writes to MAX_RW_COUNT Set the maximum size of a subrequest that writes to cachefiles to be MAX_RW_COUNT so that we don't overrun the maximum write we can make to the backing filesystem.	N/A	More Details
CVE-2024-8986	The grafana plugin SDK bundles build metadata into the binaries it compiles; this metadata includes the repository URI for the plugin being built, as retrieved by running `git remote get-url origin`. If credentials are included in the repository URI (for instance, to allow for fetching of private dependencies), the final binary will contain the full URI, including said credentials.	N/A	More Details
CVE-2024-6406	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Yordam Information Technology Mobile Library Application allows Retrieve Embedded Sensitive Data.This issue affects Mobile Library Application: before 5.0.	N/A	More Details
CVE-2024-46767	In the Linux kernel, the following vulnerability has been resolved: net: phy: Fix missing of_node_put() for leds The call of of_get_child_by_name() will cause refcount incremented for leds, if it succeeds, it should call of_node_put() to decrease it, fix it.	N/A	More Details
CVE-2024-46764	In the Linux kernel, the following vulnerability has been resolved: bpf: add check for invalid name in btf_name_valid_section() If the length of the name string is 1 and the value of name[0] is NULL byte, an OOB vulnerability occurs in btf_name_valid_section() and the return value is true, so the invalid name passes the check. To solve this, you need to check if the first position is NULL byte and if the first character is printable.	N/A	More Details
CVE-2024-46754	In the Linux kernel, the following vulnerability has been resolved: bpf: Remove tst_run from lwt_seg6local_prog_ops. The syzbot reported that the lwt_seg6 related BPF ops can be invoked via bpf_test_run() without without entering input_action_end_bpf() first. Martin KaFai Lau said that self test for BPF_PROG_TYPE_LWT_SEG6LOCAL probably didn't work since it was introduced in commit 04d4b274e2a ("ipv6: sr: Add seg6local action End.BPF"). The reason is that the per-CPU variable seg6_bpf_srh_states::srh is never assigned in the self test case but each BPF function expects it. Remove test_run for BPF_PROG_TYPE_LWT_SEG6LOCAL.	N/A	More Details
CVE-2024-46753	In the Linux kernel, the following vulnerability has been resolved: btrfs: handle errors from btrfs_dec_ref() properly In walk_up_proc() we BUG_ON(ret) from btrfs_dec_ref(). This is incorrect, we have proper error handling here, return the error.	N/A	More Details
CVE-2024-46752	In the Linux kernel, the following vulnerability has been resolved: btrfs: replace BUG_ON() with error handling at update_ref_for_cow() Instead of a BUG_ON() just return an error, log an error message and abort the transaction in case we find an extent buffer belonging to the relocation tree that doesn't have the full backref flag set. This is unexpected and should never happen (save for bugs or a potential bad memory).	N/A	More Details
CVE-2024-8903	Local active protection service settings manipulation due to unnecessary privileges assignment. The following products are affected: Acronis Cyber Protect Cloud Agent (Windows, macOS) before build 38565.	N/A	More Details