تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 5 يناير إلى ١١ يناير. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- عالي جدًا: النتيجة الأساسية لـCVSS 9.0-10.0
- عالي: النتيجة الأساسية لـCVSS 7.0-8.9
- متوسط: النتيجة الأساسية لـCVSS 4.0-6.9
- منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 5th of January to 11th of January. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

- Critical: CVSS base score of 9.0-10.0
- High: CVSS base score of 7.0-8.9
- Medium: CVSS base score 4.0-6.9
- Low: CVSS base score 0.0-3.9

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2025-0247	mozilla - multiple products	Memory safety bugs present in Firefox 133 and Thunderbird 133. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 134 and Thunderbird < 134.	2025-01-07	9.8
CVE-2018-4301	apple - Smart Card Services	This issue is fixed in SCSSU-201801. A potential stack based buffer overflow existed in GemaltoKeyHandle.cpp.	2025-01-08	9.8
CVE-2024-54676	apache - openmeetings	Vendor: The Apache Software Foundation Versions Affected: Apache OpenMeetings from 2.1.0 before 8.0.0 Description: Default clustering instructions at https://openmeetings.apache.org/Clustering.html doesn't specify white/black lists for OpenJPA this leads to possible deserialisation of untrusted data. Users are recommended to upgrade to version 8.0.0 and update their startup scripts to include the relevant 'openjpa.serialization.class.blacklist' and 'openjpa.serialization.class.whitelist' configurations as shown in the documentation.	2025-01-08	9.8
CVE-2024-40762	sonicwall - SonicOS	Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG) in the SonicOS SSLVPN authentication token generator that, in certain cases, can be predicted by an attacker potentially resulting in authentication bypass.	2025-01-09	9.8
CVE-2024-53704	sonicwall - SonicOS	An Improper Authentication vulnerability in the SSLVPN authentication mechanism allows a remote attacker to bypass authentication.	2025-01-09	9.8
CVE-2024-40765	sonicwall - SonicOS	An Integer-based buffer overflow vulnerability in the SonicOS via IPSec allows a remote attacker in specific conditions to cause Denial of Service (DoS) and potentially execute arbitrary code by sending a specially crafted IKEv2 payload.	2025-01-09	9.8
CVE-2024-13239	drupal - Two-factor Authentication (TFA)	Weak Authentication vulnerability in Drupal Two-factor Authentication (TFA) allows Authentication Abuse.This issue affects Two-factor Authentication (TFA): from 0.0.0 before 1.5.0.	2025-01-09	9.8
CVE-2024-13258	drupal - Drupal REST & JSON API Authentication	Incorrect Authorization vulnerability in Drupal Drupal REST & JSON API Authentication allows Forceful Browsing.This issue affects Drupal REST & JSON API Authentication: from 0.0.0 before 2.0.13.	2025-01-09	9.8
CVE-2024-13264	drupal - Opigno module	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') vulnerability in Drupal Opigno module allows PHP Local File Inclusion.This issue affects Opigno module: from 0.0.0 before 3.1.2.	2025-01-09	9.8
CVE-2024-13279	drupal - Two-factor Authentication (TFA)	Session Fixation vulnerability in Drupal Two-factor Authentication (TFA) allows Session Fixation.This issue affects Two-factor Authentication (TFA): from 0.0.0 before 1.8.0.	2025-01-09	9.8
CVE-2024-13280	drupal - Persistent Login	Insufficient Session Expiration vulnerability in Drupal Persistent Login allows Forceful Browsing.This issue affects Persistent Login: from 0.0.0 before 1.8.0, from 2.0.* before 2.2.2.	2025-01-09	9.8
CVE-2024-13285	drupal - wkhtmltopdf	Vulnerability in Drupal wkhtmltopdf.This issue affects wkhtmltopdf: *.*.	2025-01-09	9.8

CVE-2024-41787	ibm - Engineering Requirements Management DOORS Next	IBM Engineering Requirements Management DOORS Next 7.0.2 and 7.0.3 could allow a remote attacker to bypass security restrictions, caused by a race condition. By sending a specially crafted request, an attacker could exploit this vulnerability to remotely execute code.	2025-01-10	9.8
CVE-2024-12847	netgear - DGN1000	NETGEAR DGN1000 before 1.1.00.48 is vulnerable to an authentication bypass vulnerability. A remote and unauthenticated attacker can execute arbitrary operating system commands as root by sending crafted HTTP requests to the setup.cgi endpoint. This vulnerability has been exploited in the wild since at least 2017.	2025-01-10	9.8
CVE-2024-12802	sonicwall - SonicOS	SSL-VPN MFA Bypass in SonicWALL SSL-VPN can arise in specific cases due to the separate handling of UPN (User Principal Name) and SAM (Security Account Manager) account names when integrated with Microsoft Active Directory, allowing MFA to be configured independently for each login method and potentially enabling attackers to bypass MFA by exploiting the alternative account name.	2025-01-09	9.1
CVE-2024-13241	drupal - Open Social	Improper Authorization vulnerability in Drupal Open Social allows Collect Data from Common Resource Locations.This issue affects Open Social: from 0.0.0 before 12.0.5.	2025-01-09	9.1
CVE-2024-13242	drupal - Swift Mailer (abandoned)	Exposed Dangerous Method or Function vulnerability in Drupal Swift Mailer allows Resource Location Spoofing.This issue affects Swift Mailer: *.*.	2025-01-09	9.1
CVE-2024-13253	drupal - Advanced PWA inc Push Notifications	Incorrect Authorization vulnerability in Drupal Advanced PWA inc Push Notifications allows Forceful Browsing.This issue affects Advanced PWA inc Push Notifications: from 0.0.0 before 1.5.0.	2025-01-09	9.1
CVE-2024-13277	drupal - Smart IP Ban	Incorrect Authorization vulnerability in Drupal Smart IP Ban allows Forceful Browsing.This issue affects Smart IP Ban: from 7.X-1.0 before 7.X-1.1.	2025-01-09	9.1
CVE-2024-13278	drupal - Diff	Incorrect Authorization vulnerability in Drupal Diff allows Functionality Misuse.This issue affects Diff: from 0.0.0 before 1.8.0.	2025-01-09	9.1
CVE-2024-13281	drupal - Monster Menus	Incorrect Authorization vulnerability in Drupal Monster Menus allows Forceful Browsing.This issue affects Monster Menus: from 0.0.0 before 9.3.2.	2025-01-09	9.1
CVE-2025-0282	ivanti - multiple products	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a remote unauthenticated attacker to achieve remote code execution.	2025-01-08	9
CVE-2024-13244	drupal - Migrate Tools	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Migrate Tools allows Cross Site Request Forgery.This issue affects Migrate Tools: from 0.0.0 before 6.0.3.	2025-01-09	8.8
CVE-2024-13250	drupal - Drupal Symfony Mailer Lite	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Drupal Symfony Mailer Lite allows Cross Site Request Forgery.This issue affects Drupal Symfony Mailer Lite: from 0.0.0 before 1.0.6.	2025-01-09	8.8
CVE-2024-13251	drupal - Registration role	Incorrect Privilege Assignment vulnerability in Drupal Registration role allows Privilege Escalation.This issue affects Registration role: from 0.0.0 before 2.0.1.	2025-01-09	8.8
CVE-2024-13260	drupal - Migrate queue importer	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Migrate queue importer allows Cross Site Request Forgery.This issue affects Migrate queue importer: from 0.0.0 before 2.1.1.	2025-01-09	8.8
CVE-2024-13282	drupal - Block permissions	Incorrect Authorization vulnerability in Drupal Block permissions allows Forceful Browsing.This issue affects Block permissions: from 1.0.0 before 1.2.0.	2025-01-09	8.8
CVE-2024-13284	drupal - Gutenberg	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Gutenberg allows Cross Site Request Forgery.This issue affects Gutenberg: from 0.0.0 before 2.13.0, from 3.0.0 before 3.0.5.	2025-01-09	8.8
CVE-2025-21385	microsoft - Microsoft Purview	A Server-Side Request Forgery (SSRF) vulnerability in Microsoft Purview allows an authorized attacker to disclose information over a network.	2025-01-09	8.8
CVE-2025-21380	microsoft - Marketplace SaaS	Improper access control in Azure SaaS Resources allows an authorized attacker to disclose information over a network.	2025-01-09	8.8
CVE-2024-21464	qualcomm - fastconnect_6700_firmware	Memory corruption while processing IPA statistics, when there are no active clients registered.	2025-01-06	8.4
CVE-2024-45555	qualcomm - msm8996au_firmware	Memory corruption can occur if an already verified IFS2 image is overwritten, bypassing boot verification. This allows unauthorized programs to be injected into security-sensitive images, enabling the booting of a tampered IFS2 system image.	2025-01-06	8.4
CVE-2025-0291	google - Chrome	Type Confusion in V8 in Google Chrome prior to 131.0.6778.264 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2025-01-08	8.3
CVE-2025-22395	dell - Dell Update Package (DUP) Framework	Dell Update Package Framework, versions prior to 22.01.02, contain(s) a Local Privilege Escalation Vulnerability. A local low privileged attacker could potentially exploit this vulnerability, leading to the execution of arbitrary remote scripts on the server. Exploitation may lead to a denial of service by an attacker.	2025-01-07	8.2
CVE-2024-40702	ibm - multiple products	IBM Cognos Controller 11.0.0 through 11.0.1 and IBM Controller 11.1.0 could allow an unauthorized user to obtain valid tokens to gain access to protected resources due to improper certificate validation.	2025-01-07	8.2
CVE-2024-45033	apache software foundation - Apache Airflow Fab Provider	Insufficient Session Expiration vulnerability in Apache Airflow Fab Provider. This issue affects Apache Airflow Fab Provider: before 1.5.2. When user password has been changed with admin CLI, the sessions for that user have not been cleared, leading to insufficient session expiration, thus logged users could continue to be logged in even after the password was changed. This only happened when the password was changed with CLI. The problem does not happen in case change was done with webserver thus this is different from CVE-2023-40273 https://github.com/advisories/GHSA-pm87-24wq-r8w9 which was addressed in Apache-Airflow 2.7.0 Users are recommended to upgrade to version 1.5.2, which fixes the issue.	2025-01-08	8.1
CVE-2024-45541	qualcomm - aqt1000_firmware	Memory corruption when IOCTL call is invoked from user-space to read board data.	2025-01-06	7.8
CVE-2024-45542	qualcomm - aqt1000_firmware	Memory corruption when IOCTL call is invoked from user-space to write board data to WLAN driver.	2025-01-06	7.8

CVE-2024-45546	qualcomm - fastconnect_6900_firmware	Memory corruption while processing FIPS encryption or decryption IOCTL call invoked from user-space.	2025-01-06	7.8
CVE-2024-45547	qualcomm - fastconnect_6900_firmware	Memory corruption while processing IOCTL call invoked from user-space to verify non extension FIPS encryption and decryption functionality.	2025-01-06	7.8
CVE-2024-45548	qualcomm - fastconnect_6900_firmware	Memory corruption while processing FIPS encryption or decryption validation functionality IOCTL call.	2025-01-06	7.8
CVE-2024-45550	qualcomm - fastconnect_6900_firmware	Memory corruption occurs when invoking any IOCTL-calling application that executes all MCDM driver IOCTL calls.	2025-01-06	7.8
CVE-2024-45553	qualcomm - ar8035_firmware	Memory corruption can occur when process-specific maps are added to the global list. If a map is removed from the global list while another thread is using it for a process-specific task, issues may arise.	2025-01-06	7.8
CVE-2024-56759	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix use-after-free when COWing tree bock and tracing is enabled When a COWing a tree block, at btrfs_cow_block(), and we have the tracepoint trace_btrfs_cow_block() enabled and preemption is also enabled (CONFIG_PREEMPT=y), we can trigger a use-after-free in the COWed extent buffer while inside the tracepoint code. This is because in some paths that call btrfs_cow_block(), such as btrfs_search_slot(), we are holding the last reference on the extent buffer @buf so btrfs_force_cow_block() drops the last reference on the @buf extent buffer when it calls free_extent_buffer_stale(buf), which schedules the release of the extent buffer with RCU. This means that if we are on a kernel with preemption, the current task may be preempted before calling trace_btrfs_cow_block() and the extent buffer already released by the time trace_btrfs_cow_block() is called, resulting in a use-after-free. Fix this by moving the trace_btrfs_cow_block() from btrfs_cow_block() to btrfs_force_cow_block() before the COWed extent buffer is freed. This also has a side effect of invoking the tracepoint in the tree defrag code, at defrag.c:btrfs_realloc_node(), since btrfs_force_cow_block() is called there, but this is fine and it was actually missing there.	2025-01-06	7.8
CVE-2024-56764	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ublk: detach gendisk from ublk device if add_disk() fails Inside ublk_abort_requests(), gendisk is grabbed for aborting all inflight requests. And ublk_abort_requests() is called when exiting the uring context or handling timeout. If add_disk() fails, the gendisk may have been freed when calling ublk_abort_requests(), so use-after-free can be caused when getting disk's reference in ublk_abort_requests(). Fixes the bug by detaching gendisk from ublk device if add_disk() fails.	2025-01-06	7.8
CVE-2024-56765	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries/vas: Add close() callback in vas_vm_ops struct The mapping VMA address is saved in VAS window struct when the paste address is mapped. This VMA address is used during migration to unmap the paste address if the window is active. The paste address mapping will be removed when the window is closed or with the munmap(). But the VMA address in the VAS window is not updated with munmap() which is causing invalid access during migration. The KASAN report shows: [16386.254991] BUG: KASAN: slab-use-after-free in reconfig_close_windows+0x1a0/0x4e8 [16386.255043] Read of size 8 at addr c00000014a819670 by task drmgr/696928 [16386.255096] CPU: 29 UID: 0 PID: 696928 Comm: drmgr Kdump: loaded Tainted: G B 6.11.0-rc5-nxgzip #2 [16386.255128] Tainted: [B]=BAD_PAGE [16386.255148] Hardware name: IBM,9080-HEX Power11 (architected) 0x820200 0xf000007 of:IBM,FW1110.00 (NH1110_016) hv:phyp pSeries [16386.255181] Call Trace: [16386.255202] [c00000016b297660] [c0000000018ad0ac] dump_stack_lvl+0x84/0xe8 (unreliable) [16386.255246] [c00000016b297690] [c0000000006e8a90] print_report+0x19c/0x764 [16386.255285] [c00000016b297760] [c0000000006e9490] kasan_report+0x128/0x1f8 [16386.255309] [c00000016b297880] [c0000000006eb5c8] __asan_load8+0xac/0xe0 [16386.255326] [c00000016b2978a0] [c00000000013f898] reconfig_close_windows+0x1a0/0x4e8 [16386.255343] [c00000016b297990] [c000000000140e58] vas_migration_handler+0x3a4/0x3fc [16386.255368] [c00000016b297a90] [c000000000128848] pseries_migrate_partition+0x4c/0x4c4 ...	2025-01-06	7.8

		[16386.256136] Allocated by task 696554 on cpu 31 at 16377.277618s: [16386.256149] kasan_save_stack+0x34/0x68 [16386.256163] kasan_save_track+0x34/0x80 [16386.256175] kasan_save_alloc_info+0x58/0x74 [16386.256196] __kasan_slab_alloc+0xb8/0xdc [16386.256209] kmem_cache_alloc_noprof+0x200/0x3d0 [16386.256225] vm_area_alloc+0x44/0x150 [16386.256245] mmap_region+0x214/0x10c4 [16386.256265] do_mmap+0x5fc/0x750 [16386.256277] vm_mmap_pgoff+0x14c/0x24c [16386.256292] ksys_mmap_pgoff+0x20c/0x348 [16386.256303] sys_mmap+0xd0/0x160 ... [16386.256350] Freed by task 0 on cpu 31 at 16386.204848s: [16386.256363] kasan_save_stack+0x34/0x68 [16386.256374] kasan_save_track+0x34/0x80 [16386.256384] kasan_save_free_info+0x64/0x10c [16386.256396] __kasan_slab_free+0x120/0x204 [16386.256415] kmem_cache_free+0x128/0x450 [16386.256428] vm_area_free_rcu_cb+0xa8/0xd8 [16386.256441] rcu_do_batch+0x2c8/0xcf0 [16386.256458] rcu_core+0x378/0x3c4 [16386.256473] handle_softirqs+0x20c/0x60c [16386.256495] do_softirq_own_stack+0x6c/0x88 [16386.256509] do_softirq_own_stack+0x58/0x88 [16386.256521] __irq_exit_rcu+0x1a4/0x20c [16386.256533] irq_exit+0x20/0x38 [16386.256544] interrupt_async_exit_prepare.constprop.0+0x18/0x2c ... [16386.256717] Last potentially related work creation: [16386.256729] kasan_save_stack+0x34/0x68 [16386.256741] __kasan_record_aux_stack+0xcc/0x12c [16386.256753] __call_rcu_common.constprop.0+0x94/0xd04 [16386.256766] vm_area_free+0x28/0x3c [16386.256778] remove_vma+0xf4/0x114 [16386.256797] do_vmi_align_munmap.constprop.0+0x684/0x870 [16386.256811] __vm_munmap+0xe0/0x1f8 [16386.256821] sys_munmap+0x54/0x6c [16386.256830] system_call_exception+0x1a0/0x4a0 [16386.256841] system_call_vectored_common+0x15c/0x2ec [16386.256868] The buggy address belongs to the object at c00000014a819670 which belongs to the cache vm_area_struct of size 168 [16386.256887] The buggy address is located 0 bytes inside of freed 168-byte region [c00000014a819670, c00000014a819718) [16386.256915] The buggy address belongs to the physical page: [16386.256928] page: refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x14a81 [16386.256950] memcg:c0000000ba430001 [16386.256961] anon flags: 0x43ffff800000000(node=4|zone=0|lastcpupid=0x7ffff) [16386.256975] page_type: 0xfdffffff(slab) [16386 ---truncated---		
CVE-2024-56766	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mtd: rawnand: fix double free in atmel_pmecc_create_user() The "user" pointer was converted from being allocated with kzalloc() to being allocated by devm_kzalloc(). Calling kfree(user) will lead to a double free.	2025-01-06	7.8
CVE-2024-56447	huawei - multiple products	Vulnerability of improper permission control in the window management module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-01-08	7.8
CVE-2023-35685	google - android	In DevmemIntMapPages of devicemem_server.c, there is a possible physical page uaf due to a logic error in the code. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-08	7.8
CVE-2024-56772	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: kunit: string-stream: Fix a UAF bug in kunit_init_suite() In kunit_debugfs_create_suite(), if alloc_string_stream() fails in the kunit_suite_for_each_test_case() loop, the "suite->log = stream" has assigned before, and the error path only free the suite->log's stream memory but not set it to NULL, so the later string_stream_clear() of suite->log in kunit_init_suite() will cause below UAF bug. Set stream pointer to NULL after free to fix it. Unable to handle kernel paging request at virtual address 006440150000030d	2025-01-08	7.8

		Mem abort info: ESR = 0x0000000096000004 EC = 0x25: DABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault Data abort info: ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 CM = 0, WnR = 0, TnD = 0, TagAccess = 0 GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [006440150000030d] address between user and kernel address ranges Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP Dumping ftrace buffer: (ftrace buffer empty) Modules linked in: iio_test_gts industrialio_gts_helper cfg80211 rfkill ipv6 [last unloaded: iio_test_gts] CPU: 5 UID: 0 PID: 6253 Comm: modprobe Tainted: G B W N 6.12.0-rc4+ #458 Tainted: [B]=BAD_PAGE, [W]=WARN, [N]=TEST Hardware name: linux,dummy-virt (DT) pstate: 40000005 (nZcv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : string_stream_clear+0x54/0x1ac lr : string_stream_clear+0x1a8/0x1ac sp : ffffffc080b47410 x29: ffffffc080b47410 x28: 006440550000030d x27: ffffff80c96b5e98 x26: ffffff80c96b5e80 x25: ffffffe461b3f6c0 x24: 0000000000000003 x23: ffffff80c96b5e88 x22: 1ffffff019cdf4fc x21: dfffffc000000000 x20: ffffff80ce6fa7e0 x19: 032202a80000186d x18: 0000000000001840 x17: 0000000000000000 x16: 0000000000000000 x15: ffffffe45c355cb4 x14: ffffffe45c35589c x13: ffffffe45c03da78 x12: ffffffb810168e75 x11: 1ffffff810168e74 x10: ffffffb810168e74 x9 : dfffffc000000000 x8 : 0000000000000004 x7 : 0000000000000003 x6 : 0000000000000001 x5 : ffffffc080b473a0 x4 : 0000000000000000 x3 : 0000000000000000 x2 : 0000000000000001 x1 : ffffffe462fbf620 x0 : dfffffc000000000 Call trace: string_stream_clear+0x54/0x1ac __kunit_test_suites_init+0x108/0x1d8 kunit_exec_run_tests+0xb8/0x100 kunit_module_notify+0x400/0x55c notifier_call_chain+0xfc/0x3b4 blocking_notifier_call_chain+0x68/0x9c do_init_module+0x24c/0x5c8 load_module+0x4acc/0x4e90 init_module_from_file+0xd4/0x128 idempotent_init_module+0x2d4/0x57c __arm64_sys_finit_module+0xac/0x100 invoke_syscall+0x6c/0x258 el0_svc_common.constprop.0+0x160/0x22c do_el0_svc+0x44/0x5c el0_svc+0x48/0xb8 el0t_64_sync_handler+0x13c/0x158 el0t_64_sync+0x190/0x194 Code: f9400753 d2dff800 f2fbffe0 d343fe7c (38e06b80) ---[end trace 0000000000000000]--- Kernel panic - not syncing: Oops: Fatal exception		
CVE-2024-56775	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix handling of plane refcount [Why] The mechanism to backup and restore plane states doesn't maintain refcount, which can cause issues if the refcount of the plane changes in between backup and restore operations, such as memory leaks if the refcount was supposed to go down, or double frees / invalid memory accesses if the refcount was supposed to go up. [How] Cache and re-apply current refcount when restoring plane states.	2025-01-08	7.8
CVE-2024-56784	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Adding array index check to prevent memory corruption [Why & How] Array indices out of bound caused memory corruption. Adding checks to ensure that array index stays in bound.	2025-01-08	7.8
CVE-2024-53706	sonicwall - SonicOS	A vulnerability in the Gen7 SonicOS Cloud platform NSv, allows a remote authenticated local low-privileged attacker to elevate privileges to `root` and potentially lead to code execution.	2025-01-09	7.8
CVE-2024-43064	qualcomm - qam8255p_firmware	Uncontrolled resource consumption when a driver, an application or a SMMU client tries to access the global registers through SMMU.	2025-01-06	7.5

CVE-2024-45558	qualcomm - ar8035_firmware	Transient DOS can occur when the driver parses the per STA profile IE and tries to access the EXTN element ID without checking the IE length.	2025-01-06	7.5
CVE-2024-56439	huawei - harmonyos	Access control vulnerability in the identity authentication module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-01-08	7.5
CVE-2024-56444	huawei - harmonyos	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-01-08	7.5
CVE-2025-21102	dell - Dell VxRail HCI	Dell VxRail, versions 7.0.000 through 7.0.532, contain(s) a Plaintext Storage of a Password vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	2025-01-08	7.5
CVE-2025-21111	dell - Dell VxRail HCI	Dell VxRail, versions 8.0.000 through 8.0.311, contain(s) a Plaintext Storage of a Password vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Information exposure.	2025-01-08	7.5
CVE-2024-53705	sonicwall - SonicOS	A Server-Side Request Forgery vulnerability in the SonicOS SSH management interface allows a remote attacker to establish a TCP connection to an IP address on any port when the user is logged in to the firewall.	2025-01-09	7.5
CVE-2024-13240	drupal - Open Social	Improper Access Control vulnerability in Drupal Open Social allows Collect Data from Common Resource Locations.This issue affects Open Social: from 0.0.0 before 12.05.	2025-01-09	7.5
CVE-2024-13254	drupal - REST Views	Insertion of Sensitive Information Into Sent Data vulnerability in Drupal REST Views allows Forceful Browsing.This issue affects REST Views: from 0.0.0 before 3.0.1.	2025-01-09	7.5
CVE-2024-13255	drupal - RESTful Web Services	Exposure of Sensitive Information Through Data Queries vulnerability in Drupal RESTful Web Services allows Forceful Browsing.This issue affects RESTful Web Services: from 7.X-2.0 before 7.X-2.10.	2025-01-09	7.5
CVE-2024-13256	drupal - Email Contact	Insufficient Granularity of Access Control vulnerability in Drupal Email Contact allows Forceful Browsing.This issue affects Email Contact: from 0.0.0 before 2.0.4.	2025-01-09	7.5
CVE-2024-13259	drupal - Image Sizes	Insertion of Sensitive Information Into Sent Data vulnerability in Drupal Image Sizes allows Forceful Browsing.This issue affects Image Sizes: from 0.0.0 before 3.0.2.	2025-01-09	7.5
CVE-2024-13265	drupal - Opigno Learning path	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') vulnerability in Drupal Opigno Learning path allows PHP Local File Inclusion.This issue affects Opigno Learning path: from 0.0.0 before 3.1.2.	2025-01-09	7.5
CVE-2024-13267	drupal - Opigno TinCan Question Type	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') vulnerability in Drupal Opigno TinCan Question Type allows PHP Local File Inclusion.This issue affects Opigno TinCan Question Type: from 7.X-1.0 before 7.X-1.3.	2025-01-09	7.5
CVE-2024-13276	drupal - File Entity (fieldable files)	Insertion of Sensitive Information Into Sent Data vulnerability in Drupal File Entity (fieldable files) allows Forceful Browsing.This issue affects File Entity (fieldable files): from 7.X-* before 7.X-2.39.	2025-01-09	7.5
CVE-2025-0306	red hat - multiple products	A vulnerability was found in Ruby. The Ruby interpreter is vulnerable to the Marvin Attack. This attack allows the attacker to decrypt previously encrypted messages or forge signatures by exchanging a large number of messages with the vulnerable service.	2025-01-09	7.4
CVE-2024-56451	huawei - harmonyos	Integer overflow vulnerability during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability.	2025-01-08	7.3
CVE-2024-13291	drupal - Basic HTTP Authentication	Incorrect Authorization vulnerability in Drupal Basic HTTP Authentication allows Forceful Browsing.This issue affects Basic HTTP Authentication: from 7.X-1.0 before 7.X-1.4.	2025-01-09	7.3
CVE-2024-54006	hewlett packard enterprise (hpe) - HPE Aruba Networking 501 Wireless Client Bridge	Multiple command injection vulnerabilities exist in the web interface of the 501 Wireless Client Bridge which could lead to authenticated remote command execution. Successful exploitation of these vulnerabilities result in the ability of an attacker to execute arbitrary commands as a privileged user on the underlying operating system. Exploitation requires administrative authentication credentials on the host system.	2025-01-07	7.2
CVE-2024-54007	hewlett packard enterprise (hpe) - HPE Aruba Networking 501 Wireless Client Bridge	Multiple command injection vulnerabilities exist in the web interface of the 501 Wireless Client Bridge which could lead to authenticated remote command execution. Successful exploitation of these vulnerabilities result in the ability of an attacker to execute arbitrary commands as a privileged user on the underlying operating system. Exploitation requires administrative authentication credentials on the host system.	2025-01-07	7.2
CVE-2024-12803	sonicwall - SonicOS	A post-authentication stack-based buffer overflow vulnerability in SonicOS management allows a remote attacker to crash a firewall and potentially leads to code execution.	2025-01-09	7.2
CVE-2024-12805	sonicwall - SonicOS	A post-authentication format string vulnerability in SonicOS management allows a remote attacker to crash a firewall and potentially leads to code execution.	2025-01-09	7.2
CVE-2025-0283	ivanti - multiple products	A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a local authenticated attacker to escalate their privileges.	2025-01-08	7
CVE-2024-33061	qualcomm - qcs8550_firmware	Information disclosure while processing IOCTL call made for releasing a trusted VM process release or opening a channel without initializing the process.	2025-01-06	6.8
CVE-2024-56453	huawei - harmonyos	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability.	2025-01-08	6.8
CVE-2024-56456	huawei - harmonyos	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability.	2025-01-08	6.8
CVE-2024-33041	qualcomm - fastconnect_6900_firmware	Memory corruption when input parameter validation for number of fences is missing for fence frame IOCTL calls,	2025-01-06	6.7
CVE-2024-33055	qualcomm - fastconnect_6900_firmware	Memory corruption while invoking IOCTL calls to unmap the DMA buffers.	2025-01-06	6.7
CVE-2024-33059	qualcomm - fastconnect_6900_firmware	Memory corruption while processing frame command IOCTL calls.	2025-01-06	6.7
CVE-2024-56448	huawei - multiple products	Vulnerability of improper access control in the home screen widget module Impact: Successful exploitation of this vulnerability may affect availability.	2025-01-08	6.7

CVE-2024-23366	qualcomm - qam8255p_firmware	Information Disclosure while invoking the mailbox write API when message received from user is larger than mailbox size.	2025-01-06	6.6
CVE-2024-56449	huawei - multiple products	Privilege escalation vulnerability in the Account module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-01-08	6.6
CVE-2024-13295	drupal - Node export	Deserialization of Untrusted Data vulnerability in Drupal Node export allows Object Injection.This issue affects Node export: from 7.X-* before 7.X-3.3.	2025-01-09	6.6
CVE-2024-13296	drupal - Mailjet	Deserialization of Untrusted Data vulnerability in Drupal Mailjet allows Object Injection.This issue affects Mailjet: from 0.0.0 before 4.0.1.	2025-01-09	6.6
CVE-2024-13297	drupal - Eloqua	Deserialization of Untrusted Data vulnerability in Drupal Eloqua allows Object Injection.This issue affects Eloqua: from 7.X-* before 7.X-1.15.	2025-01-09	6.6
CVE-2024-13299	drupal - Megamenu Framework	Vulnerability in Drupal Megamenu Framework.This issue affects Megamenu Framework: *.*.	2025-01-09	6.6
CVE-2024-13300	drupal - Print Anything	Vulnerability in Drupal Print Anything.This issue affects Print Anything: *.*.	2025-01-09	6.6
CVE-2024-28778	ibm - multiple products	IBM Cognos Controller 11.0.0 through 11.0.1 and IBM Controller 11.1.0 is vulnerable to exposure of Artifactory API keys. This vulnerability allows users to publish code to private packages or repositories under the name of the organization.	2025-01-07	6.5
CVE-2025-0242	mozilla - multiple products	Memory safety bugs present in Firefox 133, Thunderbird 133, Firefox ESR 115.18, Firefox ESR 128.5, Thunderbird 115.18, and Thunderbird 128.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 134, Firefox ESR < 128.6, Firefox ESR < 115.19, Thunderbird < 134, and Thunderbird < 128.6.	2025-01-07	6.5
CVE-2025-0246	mozilla - Firefox	When using an invalid protocol scheme, an attacker could spoof the address bar. *Note: This issue only affected Android operating systems. Other operating systems are unaffected.* *Note: This issue is a different issue from CVE-2025-0244. This vulnerability affects Firefox < 134.	2025-01-07	6.5
CVE-2023-52955	huawei - multiple products	Vulnerability of improper authentication in the ANS system service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	2025-01-08	6.5
CVE-2024-47239	dell - PowerScale OneFS	Dell PowerScale OneFS versions 8.2.2.x through 9.9.0.0 contain an uncontrolled resource consumption vulnerability. A remote low privileged attacker could potentially exploit this vulnerability, leading to denial of service.	2025-01-08	6.5
CVE-2024-13243	drupal - Entity Delete Log	Missing Authorization vulnerability in Drupal Entity Delete Log allows Forceful Browsing.This issue affects Entity Delete Log: from 0.0.0 before 1.1.1.	2025-01-09	6.5
CVE-2025-23109	mozilla - Firefox for iOS	Long hostnames in URLs could be leveraged to obscure the actual host of the website or spoof the website address This vulnerability affects Firefox for iOS < 134.	2025-01-11	6.5
CVE-2024-31914	ibm - Sterling B2B Integrator Standard Edition	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.2.5 and 6.2.0.0 through 6.2.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-01-06	6.4
CVE-2024-56450	huawei - multiple products	Buffer overflow vulnerability in the component driver module Impact: Successful exploitation of this vulnerability may affect availability.	2025-01-08	6.3
CVE-2024-13272	drupal - Paragraphs table	Insufficient Granularity of Access Control vulnerability in Drupal Paragraphs table allows Content Spoofing.This issue affects Paragraphs table: from 0.0.0 before 1.23.0, from 2.0.0 before 2.0.2.	2025-01-09	6.3
CVE-2024-56435	huawei - harmonyos	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-01-08	6.2
CVE-2023-52953	huawei - multiple products	Path traversal vulnerability in the Medialibrary module Impact: Successful exploitation of this vulnerability will affect integrity and confidentiality.	2025-01-08	6.2
CVE-2024-56440	huawei - multiple products	Permission control vulnerability in the Connectivity module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	2025-01-08	6.2
CVE-2024-56443	huawei - harmonyos	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-01-08	6.2
CVE-2024-54121	huawei - harmonyos	Startup control vulnerability in the ability module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	2025-01-08	6.2
CVE-2024-33067	qualcomm - ar8035_firmware	Information disclosure while invoking callback function of sound model driver from ADSP for every valid opcode received from sound model driver.	2025-01-06	6.1
CVE-2024-43063	qualcomm - qam8255p_firmware	information disclosure while invoking the mailbox read API.	2025-01-06	6.1
CVE-2024-13283	drupal - Facets	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Facets allows Cross-Site Scripting (XSS).This issue affects Facets: from 0.0.0 before 2.0.9.	2025-01-09	6.1
CVE-2024-13301	drupal - OAuth & OpenID Connect Single Sign On – SSO (OAuth/OIDC Client)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal OAuth & OpenID Connect Single Sign On – SSO (OAuth/OIDC Client) allows Cross-Site Scripting (XSS).This issue affects OAuth & OpenID Connect Single Sign On – SSO (OAuth/OIDC Client): from 3.0.0 before 3.44.0, from 4.0.0 before 4.0.19.	2025-01-09	6.1
CVE-2024-56438	huawei - multiple products	Vulnerability of improper memory address protection in the HUKS module Impact: Successful exploitation of this vulnerability may affect availability.	2025-01-08	6.0
CVE-2024-52366	ibm - Concert Software	IBM Concert Software 1.0.0, 1.0.1, 1.0.2, 1.0.2.1, and 1.0.3 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.	2025-01-07	5.9
CVE-2024-56437	huawei - harmonyos	Vulnerability of input parameters not being verified in the widget framework module Impact: Successful exploitation of this vulnerability may affect availability.	2025-01-08	5.7
CVE-2024-56826	red hat - multiple products	A flaw was found in the OpenJPEG project. A heap buffer overflow condition may be triggered when certain options are specified while using the opj_decompress utility. This can lead to an application crash or other undefined behavior.	2025-01-09	5.6

CVE-2024-56827	red hat - multiple products	A flaw was found in the OpenJPEG project. A heap buffer overflow condition may be triggered when certain options are specified while using the opj_decompress utility. This can lead to an application crash or other undefined behavior.	2025-01-09	5.6
CVE-2024-45559	qualcomm - qam8255p_firmware	Transient DOS can occur when GVM sends a specific message type to the Vdev-FastRPC backend.	2025-01-06	5.5
CVE-2024-31913	ibm - Sterling B2B Integrator Standard Edition	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.2.5 and 6.2.0.0 through 6.2.0.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-01-06	5.5
CVE-2024-56757	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btusb: mediatek: add intf release flow when usb disconnect MediaTek claim an special usb intr interface for ISO data transmission. The interface need to be released before unregistering hci device when usb disconnect. Removing BT usb dongle without properly releasing the interface may cause Kernel panic while unregister hci device.	2025-01-06	5.5
CVE-2024-56758	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: btrfs: check folio mapping after unlock in relocate_one_folio() When we call btrfs_read_folio() to bring a folio uptodate, we unlock the folio. The result of that is that a different thread can modify the mapping (like remove it with invalidate) before we call folio_lock(). This results in an invalid page and we need to try again. In particular, if we are relocating concurrently with aborting a transaction, this can result in a crash like the following: BUG: kernel NULL pointer dereference, address: 0000000000000000 PGD 0 P4D 0 Oops: 0000 [#1] SMP CPU: 76 PID: 1411631 Comm: kworker/u322:5 Workqueue: events_unbound btrfs_reclaim_bgs_work RIP: 0010:set_page_extent_mapped+0x20/0xb0 RSP: 0018:ffffc900516a7be8 EFLAGS: 00010246 RAX: ffffea009e851d08 RBX: ffffea009e0b1880 RCX: 0000000000000000 RDX: 0000000000000000 RSI: ffffc900516a7b90 RDI: ffffea009e0b1880 RBP: 0000000003573000 R08: 0000000000000001 R09: ffff88c07fd2f3f0 R10: 0000000000000000 R11: 0000194754b575be R12: 0000000003572000 R13: 0000000003572fff R14: 0000000000100cca R15: 0000000005582fff FS: 0000000000000000(0000) GS:ffff88c07fd00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000000 CR3: 000000407d00f002 CR4: 00000000007706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <TASK> ? __die+0x78/0xc0 ? page_fault_oops+0x2a8/0x3a0 ? __switch_to+0x133/0x530 ? wq_worker_running+0xa/0x40 ? exc_page_fault+0x63/0x130 ? asm_exc_page_fault+0x22/0x30 ? set_page_extent_mapped+0x20/0xb0 relocate_file_extent_cluster+0x1a7/0x940 relocate_data_extent+0xaf/0x120 relocate_block_group+0x20f/0x480 btrfs_relocate_block_group+0x152/0x320 btrfs_relocate_chunk+0x3d/0x120 btrfs_reclaim_bgs_work+0x2ae/0x4e0 process_scheduled_works+0x184/0x370 worker_thread+0xc6/0x3e0 ? blk_add_timer+0xb0/0xb0 kthread+0xae/0xe0 ? flush_tlb_kernel_range+0x90/0x90 ret_from_fork+0x2f/0x40 ? flush_tlb_kernel_range+0x90/0x90 ret_from_fork_asm+0x11/0x20 </TASK> This occurs because cleanup_one_transaction() calls destroy_delalloc_inodes() which calls invalidate_inode_pages2() which takes the folio_lock before setting mapping to NULL. We fail to check this, and subsequently call set_extent_mapping(), which assumes that mapping != NULL (in fact it asserts that in debug mode) Note that the "fixes" patch here is not the one that introduced the	2025-01-06	5.5

		race (the very first iteration of this code from 2009) but a more recent change that made this particular crash happen in practice.		
CVE-2024-56760	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: PCI/MSI: Handle lack of irqdomain gracefully Alexandre observed a warning emitted from pci_msi_setup_msi_irqs() on a RISCV platform which does not provide PCI/MSI support: WARNING: CPU: 1 PID: 1 at drivers/pci/msi/msi.h:121 pci_msi_setup_msi_irqs+0x2c/0x32 __pci_enable_msix_range+0x30c/0x596 pci_msi_setup_msi_irqs+0x2c/0x32 pci_alloc_irq_vectors_affinity+0xb8/0xe2 RISCV uses hierarchical interrupt domains and correctly does not implement the legacy fallback. The warning triggers from the legacy fallback stub. That warning is bogus as the PCI/MSI layer knows whether a PCI/MSI parent domain is associated with the device or not. There is a check for MSI-X, which has a legacy assumption. But that legacy fallback assumption is only valid when legacy support is enabled, but otherwise the check should simply return -ENOTSUPP. Loongarch tripped over the same problem and blindly enabled legacy support without implementing the legacy fallbacks. There are weak implementations which return an error, so the problem was papered over. Correct pci_msi_domain_supports() to evaluate the legacy mode and add the missing supported check into the MSI enable path to complete it.	2025-01-06	5.5
CVE-2024-56761	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: x86/fred: Clear WFE in missing-ENDBRANCH #CPs An indirect branch instruction sets the CPU indirect branch tracker (IBT) into WAIT_FOR_ENDBRANCH (WFE) state and WFE stays asserted across the instruction boundary. When the decoder finds an inappropriate instruction while WFE is set ENDBR, the CPU raises a #CP fault. For the "kernel IBT no ENDBR" selftest where #CPs are deliberately triggered, the WFE state of the interrupted context needs to be cleared to let execution continue. Otherwise when the CPU resumes from the instruction that just caused the previous #CP, another missing-ENDBRANCH #CP is raised and the CPU enters a dead loop. This is not a problem with IDT because it doesn't preserve WFE and IRET doesn't set WFE. But FRED provides space on the entry stack (in an expanded CS area) to save and restore the WFE state, thus the WFE state is no longer clobbered, so software must clear it. Clear WFE to avoid dead looping in ibt_clear_fred_wfe() and the !ibt_fatal code path when execution is allowed to continue. Clobbering WFE in any other circumstance is a security-relevant bug. [dhansen: changelog rewording]	2025-01-06	5.5
CVE-2024-56763	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: tracing: Prevent bad count for tracing_cpumask_write If a large count is provided, it will trigger a warning in bitmap_parse_user. Also check zero for it.	2025-01-06	5.5
CVE-2024-56767	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: dmaengine: at_xdmac: avoid null_prt_deref in at_xdmac_prep_dma_memset The at_xdmac_memset_create_desc may return NULL, which will lead to a null pointer dereference. For example, the len input is error, or the atchan->free_descs_list is empty and memory is exhausted. Therefore, add check to avoid this.	2025-01-06	5.5
CVE-2024-56768	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix bpf_get_smp_processor_id() on !CONFIG_SMP On x86-64 calling bpf_get_smp_processor_id() in a kernel with CONFIG_SMP disabled can trigger the following bug, as pcpu_hot is unavailable: [8.471774] BUG: unable to handle page fault for address: 00000000936a290c [8.471849] #PF: supervisor read access in kernel mode [8.471881] #PF: error_code(0x0000) - not-present page	2025-01-06	5.5

		Fix by inlining a return 0 in the !CONFIG_SMP case.		
CVE-2024-56769	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: dib3000mb: fix uninit-value in dib3000_write_reg Syzbot reports [1] an uninitialized value issue found by KMSAN in dib3000_read_reg(). Local u8 rb[2] is used in i2c_transfer() as a read buffer; in case that call fails, the buffer may end up with some undefined values. Since no elaborate error handling is expected in dib3000_write_reg(), simply zero out rb buffer to mitigate the problem. [1] Syzkaller report dvb-usb: bulk message failed: -22 (6/0) ========== BUG: KMSAN: uninit-value in dib3000mb_attach+0x2d8/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 dib3000mb_attach+0x2d8/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 dibusb_dib3000mb_frontend_attach+0x155/0x2f0 drivers/media/usb/dvb-usb/dibusb-mb.c:31 dvb_usb_adapter_frontend_init+0xed/0x9a0 drivers/media/usb/dvb-usb/dvb-usb-dvb.c:290 dvb_usb_adapter_init drivers/media/usb/dvb-usb/dvb-usb-init.c:90 [inline] dvb_usb_init drivers/media/usb/dvb-usb/dvb-usb-init.c:186 [inline] dvb_usb_device_init+0x25a8/0x3760 drivers/media/usb/dvb-usb/dvb-usb-init.c:310 dibusb_probe+0x46/0x250 drivers/media/usb/dvb-usb/dibusb-mb.c:110 ... Local variable rb created at: dib3000_read_reg+0x86/0x4e0 drivers/media/dvb-frontends/dib3000mb.c:54 dib3000mb_attach+0x123/0x3c0 drivers/media/dvb-frontends/dib3000mb.c:758 ...	2025-01-06	5.5
CVE-2024-40679	ibm - Db2	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 is vulnerable to an information disclosure vulnerability as sensitive information may be included in a log file under specific conditions.	2025-01-08	5.5
CVE-2024-56436	huawei - harmonyos	Cross-process screen stack vulnerability in the UIExtension module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-01-08	5.5
CVE-2024-56442	huawei - multiple products	Vulnerability of native APIs not being implemented in the NFC service module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	2025-01-08	5.5
CVE-2024-56452	huawei - harmonyos	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability.	2025-01-08	5.5
CVE-2024-56454	huawei - harmonyos	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability.	2025-01-08	5.5
CVE-2024-56455	huawei - harmonyos	Vulnerability of input parameters not being verified during glTF model loading in the 3D engine module Impact: Successful exploitation of this vulnerability may affect availability.	2025-01-08	5.5

CVE-2024-56770	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved:
		
		net/sched: netem: account for backlog updates from child qdisc
		
		In general, 'qlen' of any classful qdisc should keep track of the
		number of packets that the qdisc itself and all of its children holds.
		In case of netem, 'qlen' only accounts for the packets in its internal
		tfifo. When netem is used with a child qdisc, the child qdisc can use
		'qdisc_tree_reduce_backlog' to inform its parent, netem, about created
		or dropped SKBs. This function updates 'qlen' and the backlog statistics
		of netem, but netem does not account for changes made by a child qdisc.
		'qlen' then indicates the wrong number of packets in the tfifo.
		If a child qdisc creates new SKBs during enqueue and informs its parent
		about this, netem's 'qlen' value is increased. When netem dequeues the
		newly created SKBs from the child, the 'qlen' in netem is not updated.
		If 'qlen' reaches the configured sch->limit, the enqueue function stops
		working, even though the tfifo is not full.
		
		Reproduce the bug:
		Ensure that the sender machine has GSO enabled. Configure netem as root
		qdisc and tbf as its child on the outgoing interface of the machine
		as follows:
		$ tc qdisc add dev <oif> root handle 1: netem delay 100ms limit 100
		$ tc qdisc add dev <oif> parent 1:0 tbf rate 50Mbit burst 1542 latency 50ms
		
		Send bulk TCP traffic out via this interface, e.g., by running an iPerf3
		client on the machine. Check the qdisc statistics:
		$ tc -s qdisc show dev <oif>
		
		Statistics after 10s of iPerf3 TCP test before the fix (note that
		netem's backlog > limit, netem stopped accepting packets):
		qdisc netem 1: root refcnt 2 limit 1000 delay 100ms
			2025-01-08	5.5

		Sent 2767766 bytes 1848 pkt (dropped 652, overlimits 0 requeues 0) backlog 4294528236b 1155p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 2767766 bytes 1848 pkt (dropped 327, overlimits 7601 requeues 0) backlog 0b 0p requeues 0 Statistics after the fix: qdisc netem 1: root refcnt 2 limit 1000 delay 100ms Sent 37766372 bytes 24974 pkt (dropped 9, overlimits 0 requeues 0) backlog 0b 0p requeues 0 qdisc tbf 10: parent 1:1 rate 50Mbit burst 1537b lat 50ms Sent 37766372 bytes 24974 pkt (dropped 327, overlimits 96017 requeues 0) backlog 0b 0p requeues 0 tbf segments the GSO SKBs (tbf_segment) and updates the netem's 'qlen'. The interface fully stops transferring packets and "locks". In this case, the child qdisc and tfifo are empty, but 'qlen' indicates the tfifo is at its limit and no more packets are accepted. This patch adds a counter for the entries in the tfifo. Netem's 'qlen' is only decreased when a packet is returned by its dequeue function, and not during enqueuing into the child qdisc. External updates to 'qlen' are thus accounted for and only the behavior of the backlog statistics changes. As in other qdiscs, 'qlen' then keeps track of how many packets are held in netem and all of its children. As before, sch->limit remains as the maximum number of packets in the tfifo. The same applies to netem's backlog statistics.		
CVE-2024-56771	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: mtd: spinand: winbond: Fix 512GW, 01GW, 01JW and 02JW ECC information These four chips: * W25N512GW * W25N01GW * W25N01JW * W25N02JW all require a single bit of ECC strength and thus feature an on-die Hamming-like ECC engine. There is no point in filling a ->get_status() callback for them because the main ECC status bytes are located in standard places, and retrieving the number of bitflips in case of corrected chunk is both useless and unsupported (if there are bitflips, then there is 1 at most, so no need to query the chip for that). Without this change, a kernel warning triggers every time a bit flips.	2025-01-08	5.5
CVE-2024-56773	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: kunit: Fix potential null dereference in kunit_device_driver_test() kunit_kzalloc() may return a NULL pointer, dereferencing it without NULL check may lead to NULL dereference. Add a NULL check for test_state.	2025-01-08	5.5
CVE-2024-56774	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: btrfs: add a sanity check for btrfs root in btrfs_search_slot() Syzbot reports a null-ptr-deref in btrfs_search_slot(). The reproducer is using rescue=ibadroots, and the extent tree root is corrupted thus the extent tree is NULL. When scrub tries to search the extent tree to gather the needed extent info, btrfs_search_slot() doesn't check if the target root is NULL or not, resulting the null-ptr-deref. Add sanity check for btrfs root before using it in btrfs_search_slot().	2025-01-08	5.5
CVE-2024-56776	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure.	2025-01-08	5.5
CVE-2024-56777	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_gdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure.	2025-01-08	5.5

CVE-2024-56778	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/sti: avoid potential dereference of error pointers in sti_hqvdp_atomic_check The return value of drm_atomic_get_crtc_state() needs to be checked. To avoid use of error pointer 'crtc_state' in case of the failure.	2025-01-08	5.5

CVE-2024-56779	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved:
		
		nfsd: fix nfs4_openowner leak when concurrent nfsd4_open occur
		
		The action force umount(umount -f) will attempt to kill all rpc_task even
		umount operation may ultimately fail if some files remain open.
		Consequently, if an action attempts to open a file, it can potentially
		send two rpc_task to nfs server.
		
		NFS CLIENT
		thread1 thread2
		open("file")
		...
		nfs4_do_open
		_nfs4_do_open
		_nfs4_open_and_get_state
		_nfs4_proc_open
		nfs4_run_open_task
		/* rpc_task1 */
		rpc_run_task
		rpc_wait_for_completion_task
		
		umount -f
		nfs_umount_begin
		rpc_killall_tasks
		rpc_signal_task
		rpc_task1 been wakeup
		and return -512
		_nfs4_do_open // while loop
		...
		nfs4_run_open_task
		/* rpc_task2 */
		rpc_run_task
		rpc_wait_for_completion_task
		
		While processing an open request, nfsd will first attempt to find or
		allocate an nfs4_openowner. If it finds an nfs4_openowner that is not
		marked as NFS4_OO_CONFIRMED, this nfs4_openowner will released. Since
		two rpc_task can attempt to open the same file simultaneously from the
		client to server, and because two instances of nfsd can run
		concurrently, this situation can lead to lots of memory leak.
		Additionally, when we echo 0 to /proc/fs/nfsd/threads, warning will be
		triggered.
		
		NFS SERVER
		nfsd1 nfsd2 echo 0 > /proc/fs/nfsd/threads
		
		nfsd4_open
		nfsd4_process_open1
		find_or_alloc_open_stateowner
		// alloc oo1, stateid1
		nfsd4_open
		nfsd4_process_open1
		find_or_alloc_open_stateowner
		// find oo1, without NFS4_OO_CONFIRMED
		release_openowner
		unhash_openowner_locked
		list_del_init(&oo->oo_perclient)
		// cannot find this oo
		// from client, LEAK!!!
		alloc_stateowner // alloc oo2
		
		nfsd4_process_open2
		init_open_stateid
		// associate oo1
		// with stateid1, stateid1 LEAK!!!
		nfs4_get_vfs_file
		// alloc nfsd_file1 and nfsd_file_mark1
		// all LEAK!!!
		
		nfsd4_process_open2
		...
			2025-01-08	5.5

		write_threads
		...
		nfsd_destroy_serv
		nfsd_shutdown_net
		nfs4_state_shutdown_net
		nfs4_state_destroy_net
		destroy_client
		__destroy_client
		// won't find oo1!!!
		nfsd_shutdown_generic
		nfsd_file_cache_shutdown
		kmem_cache_destroy
		for nfsd_file_slab
		and nfsd_file_mark_slab
		// bark since nfsd_file1
		// and nfsd_file_mark1
		// still alive
		
		==========
		BUG nfsd_file (Not tainted): Objects remaining in nfsd_file on
		__kmem_cache_shutdown()
		---------- 	
		
		Slab 0xffd4000004438a80 objects=34 used=1 fp=0xff11000110e2ad28
		flags=0x17ffffc0000240(workingset|head|node=0|zone=2|lastcpupid=0x1fffff)
		CPU: 4 UID: 0 PID: 757 Comm: sh Not tainted 6.12.0-rc6+ #19
		Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS
		1.16.1-2.fc37 04/01/2014
		Call Trace:
		<TASK>
		dum
		---truncated---		

CVE-2024-56780	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: quota: flush quota_release_work upon quota writeback One of the paths quota writeback is called from is: freeze_super() sync_filesystem() ext4_sync_fs() dquot_writeback_dquots() Since we currently don't always flush the quota_release_work queue in this path, we can end up with the following race: 1. dquot are added to releasing_dquots list during regular operations. 2. FS Freeze starts, however, this does not flush the quota_release_work queue. 3. Freeze completes. 4. Kernel eventually tries to flush the workqueue while FS is frozen which hits a WARN_ON since transaction gets started during frozen state: ext4_journal_check_start+0x28/0x110 [ext4] (unreliable) __ext4_journal_start_sb+0x64/0x1c0 [ext4] ext4_release_dquot+0x90/0x1d0 [ext4] quota_release_workfn+0x43c/0x4d0 Which is the following line: WARN_ON(sb->s_writers.frozen == SB_FREEZE_COMPLETE); Which ultimately results in generic/390 failing due to dmesg noise. This was detected on powerpc machine 15 cores. To avoid this, make sure to flush the workqueue during dquot_writeback_dquots() so we dont have any pending workitems after freeze.	2025-01-08	5.5
CVE-2024-56781	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: powerpc/prom_init: Fixup missing powermac #size-cells On some powermacs `escc` nodes are missing `#size-cells` properties, which is deprecated and now triggers a warning at boot since commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"). For example: Missing '#size-cells' in /pci@f2000000/mac-io@c/escc@13000 WARNING: CPU: 0 PID: 0 at drivers/of/base.c:133 of_bus_n_size_cells+0x98/0x108	2025-01-08	5.5

		Hardware name: PowerMac3,1 7400 0xc0209 PowerMac ... Call Trace: of_bus_n_size_cells+0x98/0x108 (unreliable) of_bus_default_count_cells+0x40/0x60 __of_get_address+0xc8/0x21c __of_address_to_resource+0x5c/0x228 pmz_init_port+0x5c/0x2ec pmz_probe.isra.0+0x144/0x1e4 pmz_console_init+0x10/0x48 console_init+0xcc/0x138 start_kernel+0x5c4/0x694 As powermacs boot via prom_init it's possible to add the missing properties to the device tree during boot, avoiding the warning. Note that `escc-legacy` nodes are also missing `#size-cells` properties, but they are skipped by the macio driver, so leave them alone. Depends-on: 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling")		
CVE-2024-56782	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: ACPI: x86: Add adev NULL check to acpi_quirk_skip_serdev_enumeration() acpi_dev_hid_match() does not check for adev == NULL, dereferencing it unconditional. Add a check for adev being NULL before calling acpi_dev_hid_match(). At the moment acpi_quirk_skip_serdev_enumeration() is never called with a controller_parent without an ACPI companion, but better safe than sorry.	2025-01-08	5.5
CVE-2024-56783	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_socket: remove WARN_ON_ONCE on maximum cgroup level cgroup maximum depth is INT_MAX by default, there is a cgroup toggle to restrict this maximum depth to a more reasonable value not to harm performance. Remove unnecessary WARN_ON_ONCE which is reachable from userspace.	2025-01-08	5.5
CVE-2024-56785	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: MIPS: Loongson64: DTS: Really fix PCIe port nodes for ls7a Fix the dtc warnings: arch/mips/boot/dts/loongson/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a000000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongson/ls7a-pch.dtsi:68.16-416.5: Warning (interrupt_provider): /bus@10000000/pci@1a000000: '#interrupt-cells' found, but node is not an interrupt provider arch/mips/boot/dts/loongson/loongson64g_4core_ls7a.dtb: Warning (interrupt_map): Failed prerequisite 'interrupt_provider' And a runtime warning introduced in commit 045b14ca5c36 ("of: WARN on deprecated #address-cells/#size-cells handling"): WARNING: CPU: 0 PID: 1 at drivers/of/base.c:106 of_bus_n_addr_cells+0x9c/0xe0 Missing '#address-cells' in /bus@10000000/pci@1a000000/pci_bridge@9,0 The fix is similar to commit d89a415ff8d5 ("MIPS: Loongson64: DTS: Fix PCIe port nodes for ls7a"), which has fixed the issue for ls2k (despite its subject mentions ls7a).	2025-01-08	5.5
CVE-2024-56786	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: bpf: put bpf_link's program when link is safe to be deallocated In general, BPF link's underlying BPF program should be considered to be reachable through attach hook -> link -> prog chain, and, pessimistically, we have to assume that as long as link's memory is not safe to free, attach hook's code might hold a pointer to BPF program and use it. As such, it's not (generally) correct to put link's program early before waiting for RCU GPs to go through. More eager bpf_prog_put() that we currently do is mostly correct due to BPF program's release code doing similar RCU GP waiting, but as will be shown in the following patches, BPF program can be non-sleepable (and, thus, reliant on only "classic" RCU GP), while BPF link's attach hook can have sleepable semantics and needs to be protected by RCU Tasks Trace, and for such cases BPF link has to go through RCU Tasks Trace + "classic" RCU GPs before being deallocated. And so, if we put BPF program early, we might free BPF program before we free BPF link, leading to use-after-free situation.	2025-01-08	5.5

		So, this patch defers bpf_prog_put() until we are ready to perform bpf_link's deallocation. At worst, this delays BPF program freeing by one extra RCU GP, but that seems completely acceptable. Alternatively, we'd need more elaborate ways to determine BPF hook, BPF link, and BPF program lifetimes, and how they relate to each other, which seems like an unnecessary complication. Note, for most BPF links we still will perform eager bpf_prog_put() and link dealloc, so for those BPF links there are no observable changes whatsoever. Only BPF links that use deferred dealloc might notice slightly delayed freeing of BPF programs. Also, to reduce code and logic duplication, extract program put + link dealloc logic into bpf_link_dealloc() helper.		
CVE-2024-56787	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: soc: imx8m: Probe the SoC driver as platform driver With driver_async_probe=* on kernel command line, the following trace is produced because on i.MX8M Plus hardware because the soc-imx8m.c driver calls of_clk_get_by_name() which returns -EPROBE_DEFER because the clock driver is not yet probed. This was not detected during regular testing without driver_async_probe. Convert the SoC code to platform driver and instantiate a platform device in its current device_initcall() to probe the platform driver. Rework .soc_revision callback to always return valid error code and return SoC revision via parameter. This way, if anything in the .soc_revision callback return -EPROBE_DEFER, it gets propagated to .probe and the .probe will get retried later. " ------------[cut here]------------ WARNING: CPU: 1 PID: 1 at drivers/soc/imx/soc-imx8m.c:115 imx8mm_soc_revision+0xdc/0x180 CPU: 1 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.11.0-next-20240924-00002-g2062bb554dea #603 Hardware name: DH electronics i.MX8M Plus DHCOM Premium Developer Kit (3) (DT) pstate: 20000005 (nzCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : imx8mm_soc_revision+0xdc/0x180 lr : imx8mm_soc_revision+0xd0/0x180 sp : ffff8000821fbcc0 x29: ffff8000821fbce0 x28: 0000000000000000 x27: ffff800081810120 x26: ffff8000818a9970 x25: 0000000000000006 x24: 0000000000824311 x23: ffff8000817f42c8 x22: ffff0000df8be210 x21: fffffffffffffdfb x20: ffff800082780000 x19: 0000000000000001 x18: ffffffffffffffff x17: ffff800081fff418 x16: ffff8000823e1000 x15: ffff0000c03b65e8 x14: ffff0000c00051b0 x13: ffff800082790000 x12: 0000000000000801 x11: ffff80008278ffff x10: ffff80008209d3a6 x9 : ffff80008062e95c x8 : ffff8000821fb9a0 x7 : 0000000000000000 x6 : 00000000000080e3 x5 : ffff0000df8c03d8 x4 : 0000000000000000 x3 : 0000000000000000 x2 : 0000000000000000 x1 : fffffffffffffdfb x0 : fffffffffffffdfb Call trace: imx8mm_soc_revision+0xdc/0x180 imx8_soc_init+0xb0/0x1e0 do_one_initcall+0x94/0x1a8 kernel_init_freeable+0x240/0x2a8 kernel_init+0x28/0x140 ret_from_fork+0x10/0x20 ---[end trace 0000000000000000]--- SoC: i.MX8MP revision 1.1 "	2025-01-08	5.5
CVE-2022-22491	ibm - App Connect Enterprise Certified Container	IBM App Connect Enterprise Certified Container 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, 12.1, 12.2, 12.3, and 12.4 operands running in Red Hat OpenShift do not restrict writing to the local filesystem, which may result in exhausting the available storage in a Pod, resulting in that Pod being restarted.	2025-01-09	5.5
CVE-2024-13248	drupal - Private content	Incorrect Privilege Assignment vulnerability in Drupal Private content allows Target Influence via Framing.This issue affects Private content: from 0.0.0 before 2.1.0.	2025-01-09	5.5
CVE-2024-13263	drupal - Opigno group manager	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection') vulnerability in Drupal Opigno group manager allows PHP Local File Inclusion.This issue affects Opigno group manager: from 0.0.0 before 3.1.1.	2025-01-09	5.5
CVE-2024-53689	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: block: Fix potential deadlock while freezing queue and acquiring sysfs_lock For storing a value to a queue attribute, the queue_attr_store function first freezes the queue (->q_usage_counter(io)) and then acquire ->sysfs_lock. This seems not correct as the usual ordering should be to acquire ->sysfs_lock before freezing the queue. This incorrect ordering causes the following lockdep splat which we are able to reproduce always simply by accessing /sys/kernel/debug file using ls command:	2025-01-11	5.5

		[57.597146] WARNING: possible circular locking dependency detected [57.597154] 6.12.0-10553-gb86545e02e8c #20 Tainted: G W [57.597162] ---------- [57.597168] ls/4605 is trying to acquire lock: [57.597176] c00000003eb56710 (&mm->mmap_lock){++++}-{4:4}, at: __might_fault+0x58/0xc0 [57.597200] but task is already holding lock: [57.597207] c0000018e27c6810 (&sb->s_type->i_mutex_key#3){++++}-{4:4}, at: iterate_dir+0x94/0x1d4 [57.597226] which lock already depends on the new lock. [57.597233] the existing dependency chain (in reverse order) is: [57.597241] -> #5 (&sb->s_type->i_mutex_key#3){++++}-{4:4}: [57.597255] down_write+0x6c/0x18c [57.597264] start_creating+0xb4/0x24c [57.597274] debugfs_create_dir+0x2c/0x1e8 [57.597283] blk_register_queue+0xec/0x294 [57.597292] add_disk_fwnode+0x2e4/0x548 [57.597302] brd_alloc+0x2c8/0x338 [57.597309] brd_init+0x100/0x178 [57.597317] do_one_initcall+0x88/0x3e4 [57.597326] kernel_init_freeable+0x3cc/0x6e0 [57.597334] kernel_init+0x34/0x1cc [57.597342] ret_from_kernel_user_thread+0x14/0x1c [57.597350] -> #4 (&q->debugfs_mutex){+.+.}-{4:4}: [57.597362] __mutex_lock+0xfc/0x12a0 [57.597370] blk_register_queue+0xd4/0x294 [57.597379] add_disk_fwnode+0x2e4/0x548 [57.597388] brd_alloc+0x2c8/0x338 [57.597395] brd_init+0x100/0x178 [57.597402] do_one_initcall+0x88/0x3e4 [57.597410] kernel_init_freeable+0x3cc/0x6e0 [57.597418] kernel_init+0x34/0x1cc [57.597426] ret_from_kernel_user_thread+0x14/0x1c [57.597434] -> #3 (&q->sysfs_lock){+.+.}-{4:4}: [57.597446] __mutex_lock+0xfc/0x12a0 [57.597454] queue_attr_store+0x9c/0x110 [57.597462] sysfs_kf_write+0x70/0xb0 [57.597471] kernfs_fop_write_iter+0x1b0/0x2ac [57.597480] vfs_write+0x3dc/0x6e8 [57.597488] ksys_write+0x84/0x140 [57.597495] system_call_exception+0x130/0x360 [57.597504] system_call_common+0x160/0x2c4 [57.597516] -> #2 (&q->q_usage_counter(io)#21){++++}-{0:0}: [57.597530] __submit_bio+0x5ec/0x828 [57.597538] submit_bio_noacct_nocheck+0x1e4/0x4f0 [57.597547] iomap_readahead+0x2a0/0x448 [57.597556] xfs_vm_readahead+0x28/0x3c [57.597564] read_pages+0x88/0x41c [57.597571] page_cache_ra_unbounded+0x1ac/0x2d8 [57.597580] filemap_get_pages+0x188/0x984 [57.597588] filemap_read+0x13c/0x4bc [57.597596] xfs_file_buffered_read+0x88/0x17c [57.597605] xfs_file_read_iter+0xac/0x158 [57.597614] vfs_read+0x2d4/0x3b4 [57.597622] ksys_read+0x84/0x144 [57.597629] system_call_exception+0x130/0x360 [57.597637] system_call_common+0x160/0x2c4 [57.597647] -> #1 (mapping.invalidate_lock#2){++++}-{4:4}: [57.597661] down_read+0x6c/0x220 [57.597669] filemap_fault+0x870/0x100c [57.597677] xfs_filemap_fault+0xc4/0x18c [57.597684] __do_fault+0x64/0x164 [57.597693] __handle_mm_fault+0x1274/0x1dac [57.597702] handle_mm_fault+0x248/0x48 ---truncated---		
CVE-2024-54191	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: iso: Fix circular lock in iso_conn_big_sync This fixes the circular locking dependency warning below, by reworking iso_sock_recvmsg, to ensure that the socket lock is always released	2025-01-11	5.5

		before calling a function that locks hdev. [561.670344] == [561.670346] WARNING: possible circular locking dependency detected [561.670349] 6.12.0-rc6+ #26 Not tainted [561.670351] -- [561.670353] iso-tester/3289 is trying to acquire lock: [561.670355] ffff88811f600078 (&hdev->lock){+.+.}-{3:3}, at: iso_conn_big_sync+0x73/0x260 [bluetooth] [561.670405] but task is already holding lock: [561.670407] ffff88815af58258 (sk_lock-AF_BLUETOOTH){+.+.}-{0:0}, at: iso_sock_recvmsg+0xbf/0x500 [bluetooth] [561.670450] which lock already depends on the new lock. [561.670452] the existing dependency chain (in reverse order) is: [561.670453] -> #2 (sk_lock-AF_BLUETOOTH){+.+.}-{0:0}: [561.670458] lock_acquire+0x7c/0xc0 [561.670463] lock_sock_nested+0x3b/0xf0 [561.670467] bt_accept_dequeue+0x1a5/0x4d0 [bluetooth] [561.670510] iso_sock_accept+0x271/0x830 [bluetooth] [561.670547] do_accept+0x3dd/0x610 [561.670550] __sys_accept4+0xd8/0x170 [561.670553] __x64_sys_accept+0x74/0xc0 [561.670556] x64_sys_call+0x17d6/0x25f0 [561.670559] do_syscall_64+0x87/0x150 [561.670563] entry_SYSCALL_64_after_hwframe+0x76/0x7e [561.670567] -> #1 (sk_lock-AF_BLUETOOTH-BTPROTO_ISO){+.+.}-{0:0}: [561.670571] lock_acquire+0x7c/0xc0 [561.670574] lock_sock_nested+0x3b/0xf0 [561.670577] iso_sock_listen+0x2de/0xf30 [bluetooth] [561.670617] __sys_listen_socket+0xef/0x130 [561.670620] __x64_sys_listen+0xe1/0x190 [561.670623] x64_sys_call+0x2517/0x25f0 [561.670626] do_syscall_64+0x87/0x150 [561.670629] entry_SYSCALL_64_after_hwframe+0x76/0x7e [561.670632] -> #0 (&hdev->lock){+.+.}-{3:3}: [561.670636] __lock_acquire+0x32ad/0x6ab0 [561.670639] lock_acquire.part.0+0x118/0x360 [561.670642] lock_acquire+0x7c/0xc0 [561.670644] __mutex_lock+0x18d/0x12f0 [561.670647] mutex_lock_nested+0x1b/0x30 [561.670651] iso_conn_big_sync+0x73/0x260 [bluetooth] [561.670687] iso_sock_recvmsg+0x3e9/0x500 [bluetooth] [561.670722] sock_recvmsg+0x1d5/0x240 [561.670725] sock_read_iter+0x27d/0x470 [561.670727] vfs_read+0x9a0/0xd30 [561.670731] ksys_read+0x1a8/0x250 [561.670733] __x64_sys_read+0x72/0xc0 [561.670736] x64_sys_call+0x1b12/0x25f0 [561.670738] do_syscall_64+0x87/0x150 [561.670741] entry_SYSCALL_64_after_hwframe+0x76/0x7e [561.670744] other info that might help us debug this: [561.670745] Chain exists of: &hdev->lock --> sk_lock-AF_BLUETOOTH-BTPROTO_ISO --> sk_lock-AF_BLUETOOTH [561.670751] Possible unsafe locking scenario: [561.670753] CPU0 CPU1 [561.670754] ---- ---- [561.670756] lock(sk_lock-AF_BLUETOOTH); [561.670758] lock(sk_lock AF_BLUETOOTH-BTPROTO_ISO); [561.670761] lock(sk_lock-AF_BLUETOOTH); [561.670764] lock(&hdev->lock); [561.670767] *** DEADLOCK ***		
CVE-2024-54460	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: iso: Fix circular lock in iso_listen_bis This fixes the circular locking dependency warning below, by releasing the socket lock before enterning iso_listen_bis, to	2025-01-11	5.5

		avoid any potential deadlock with hdev lock. [75.307983] == [75.307984] WARNING: possible circular locking dependency detected [75.307985] 6.12.0-rc6+ #22 Not tainted [75.307987] -- [75.307987] kworker/u81:2/2623 is trying to acquire lock: [75.307988] ffff8fde1769da58 (sk_lock-AF_BLUETOOTH-BTPROTO_ISO) at: iso_connect_cfm+0x253/0x840 [bluetooth] [75.308021] but task is already holding lock: [75.308022] ffff8fdd61a10078 (&hdev->lock) at: hci_le_per_adv_report_evt+0x47/0x2f0 [bluetooth] [75.308053] which lock already depends on the new lock. [75.308054] the existing dependency chain (in reverse order) is: [75.308055] -> #1 (&hdev->lock){+.+.}-{3:3}: [75.308057] __mutex_lock+0xad/0xc50 [75.308061] mutex_lock_nested+0x1b/0x30 [75.308063] iso_sock_listen+0x143/0x5c0 [bluetooth] [75.308085] __sys_listen_socket+0x49/0x60 [75.308088] __x64_sys_listen+0x4c/0x90 [75.308090] x64_sys_call+0x2517/0x25f0 [75.308092] do_syscall_64+0x87/0x150 [75.308095] entry_SYSCALL_64_after_hwframe+0x76/0x7e [75.308098] -> #0 (sk_lock-AF_BLUETOOTH-BTPROTO_ISO){+.+.}-{0:0}: [75.308100] __lock_acquire+0x155e/0x25f0 [75.308103] lock_acquire+0xc9/0x300 [75.308105] lock_sock_nested+0x32/0x90 [75.308107] iso_connect_cfm+0x253/0x840 [bluetooth] [75.308128] hci_connect_cfm+0x6c/0x190 [bluetooth] [75.308155] hci_le_per_adv_report_evt+0x27b/0x2f0 [bluetooth] [75.308180] hci_le_meta_evt+0xe7/0x200 [bluetooth] [75.308206] hci_event_packet+0x21f/0x5c0 [bluetooth] [75.308230] hci_rx_work+0x3ae/0xb10 [bluetooth] [75.308254] process_one_work+0x212/0x740 [75.308256] worker_thread+0x1bd/0x3a0 [75.308258] kthread+0xe4/0x120 [75.308259] ret_from_fork+0x44/0x70 [75.308261] ret_from_fork_asm+0x1a/0x30 [75.308263] other info that might help us debug this: [75.308264] Possible unsafe locking scenario: [75.308264] CPU0 CPU1 [75.308265] ---- ---- [75.308265] lock(&hdev->lock); [75.308267] lock(sk_lock- AF_BLUETOOTH-BTPROTO_ISO); [75.308268] lock(&hdev->lock); [75.308269] lock(sk_lock-AF_BLUETOOTH-BTPROTO_ISO); [75.308270] *** DEADLOCK *** [75.308271] 4 locks held by kworker/u81:2/2623: [75.308272] #0: ffff8fdd66e52148 ((wq_completion)hci0#2){+.+.}-{0:0}, at: process_one_work+0x443/0x740 [75.308276] #1: ffffafb488b7fe48 ((work_completion)(&hdev->rx_work)), at: process_one_work+0x1ce/0x740 [75.308280] #2: ffff8fdd61a10078 (&hdev->lock){+.+.}-{3:3} at: hci_le_per_adv_report_evt+0x47/0x2f0 [bluetooth] [75.308304] #3: ffffffffb6ba4900 (rcu_read_lock){....}-{1:2}, at: hci_connect_cfm+0x29/0x190 [bluetooth]		
CVE-2024-54680	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix TCP timers deadlock after rmmod Commit ef7134c7fc48 ("smb: client: Fix use-after-free of network namespace.") fixed a netns UAF by manually enabled socket refcounting (sk->sk_net_refcnt=1 and sock_inuse_add(net, 1)). The reason the patch worked for that bug was because we now hold references to the netns (get_net_track() gets a ref internally) and they're properly released (internally, on __sk_destruct()), but only because sk->sk_net_refcnt was set.	2025-01-11	5.5

		Problem:
		(this happens regardless of CONFIG_NET_NS_REFCNT_TRACKER and regardless
		if init_net or other)
		
		Setting sk->sk_net_refcnt=1 *manually* and *after* socket creation is not
		only out of cifs scope, but also technically wrong -- it's set conditionally
		based on user (=1) vs kernel (=0) sockets. And net/ implementations
		seem to base their user vs kernel space operations on it.
		
		e.g. upon TCP socket close, the TCP timers are not cleared because
		sk->sk_net_refcnt=1:
		(cf. commit 151c9c724d05 ("tcp: properly terminate timers for kernel sockets"))
		
		net/ipv4/tcp.c:
		void tcp_close(struct sock *sk, long timeout)
		{
		lock_sock(sk);
		__tcp_close(sk, timeout);
		release_sock(sk);
		if (!sk->sk_net_refcnt)
		inet_csk_clear_xmit_timers_sync(sk);
		sock_put(sk);
		}
		
		Which will throw a lockdep warning and then, as expected, deadlock on
		tcp_write_timer().
		
		A way to reproduce this is by running the reproducer from ef7134c7fc48
		and then 'rmmod cifs'. A few seconds later, the deadlock/lockdep
		warning shows up.
		
		Fix:
		We shouldn't mess with socket internals ourselves, so do not set
		sk_net_refcnt manually.
		
		Also change __sock_create() to sock_create_kern() for explicitness.
		
		As for non-init_net network namespaces, we deal with it the best way
		we can -- hold an extra netns reference for server->ssocket and drop it
		when it's released. This ensures that the netns still exists whenever
		we need to create/destroy server->ssocket, but is not directly tied to
		it.		

CVE-2024-54683	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netfilter: IDLETIMER: Fix for possible ABBA deadlock Deletion of the last rule referencing a given idletimer may happen at the same time as a read of its file in sysfs: | == | WARNING: possible circular locking dependency detected | 6.12.0-rc7-01692-g5e9a28f41134-dirty #594 Not tainted | -- | iptables/3303 is trying to acquire lock: | ffff8881057e04b8 (kn->active#48){++++}-{0:0}, at: __kernfs_remove+0x20 | | but task is already holding lock: | ffffffffa0249068 (list_mutex){+.+.}-{3:3}, at: idletimer_tg_destroy_v] | | which lock already depends on the new lock. A simple reproducer is: | #!/bin/bash | | while true; do | iptables -A INPUT -i foo -j IDLETIMER --timeout 10 --label "testme" | iptables -D INPUT -i foo -j IDLETIMER --timeout 10 --label "testme" | done & | while true; do | cat /sys/class/xt_idletimer/timers/testme >/dev/null | done Avoid this by freeing list_mutex right after deleting the element from the list, then continuing with the teardown.	2025-01-11	5.5
CVE-2024-55642	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: block: Prevent potential deadlocks in zone write plug error recovery	2025-01-11	5.5

		Zone write plugging for handling writes to zones of a zoned block device always execute a zone report whenever a write BIO to a zone fails. The intent of this is to ensure that the tracking of a zone write pointer is always correct to ensure that the alignment to a zone write pointer of write BIOs can be checked on submission and that we can always correctly emulate zone append operations using regular write BIOs. However, this error recovery scheme introduces a potential deadlock if a device queue freeze is initiated while BIOs are still plugged in a zone write plug and one of these write operation fails. In such case, the disk zone write plug error recovery work is scheduled and executes a report zone. This in turn can result in a request allocation in the underlying driver to issue the report zones command to the device. But with the device queue freeze already started, this allocation will block, preventing the report zone execution and the continuation of the processing of the plugged BIOs. As plugged BIOs hold a queue usage reference, the queue freeze itself will never complete, resulting in a deadlock. Avoid this problem by completely removing from the zone write plugging code the use of report zones operations after a failed write operation, instead relying on the device user to either execute a report zones, reset the zone, finish the zone, or give up writing to the device (which is a fairly common pattern for file systems which degrade to read-only after write failures). This is not an unreasonnable requirement as all well-behaved applications, FSes and device mapper already use report zones to recover from write errors whenever possible by comparing the current position of a zone write pointer with what their assumption about the position is. The changes to remove the automatic error recovery are as follows: - Completely remove the error recovery work and its associated resources (zone write plug list head, disk error list, and disk zone_wplugs_work work struct). This also removes the functions disk_zone_wplug_set_error() and disk_zone_wplug_clear_error(). - Change the BLK_ZONE_WPLUG_ERROR zone write plug flag into BLK_ZONE_WPLUG_NEED_WP_UPDATE. This new flag is set for a zone write plug whenever a write opration targetting the zone of the zone write plug fails. This flag indicates that the zone write pointer offset is not reliable and that it must be updated when the next report zone, reset zone, finish zone or disk revalidation is executed. - Modify blk_zone_write_plug_bio_endio() to set the BLK_ZONE_WPLUG_NEED_WP_UPDATE flag for the target zone of a failed write BIO. - Modify the function disk_zone_wplug_set_wp_offset() to clear this new flag, thus implementing recovery of a correct write pointer offset with the reset (all) zone and finish zone operations. - Modify blkdev_report_zones() to always use the disk_report_zones_cb() callback so that disk_zone_wplug_sync_wp_offset() can be called for any zone marked with the BLK_ZONE_WPLUG_NEED_WP_UPDATE flag. This implements recovery of a correct write pointer offset for zone write plugs marked with BLK_ZONE_WPLUG_NEED_WP_UPDATE and within the range of the report zones operation executed by the user. - Modify blk_revalidate_seq_zone() to call disk_zone_wplug_sync_wp_offset() for all sequential write required zones when a zoned block device is revalidated, thus always resolving any inconsistency between the write pointer offset of zone write plugs and the actual write pointer position of sequential zones.		
CVE-2024-55916	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: Drivers: hv: util: Avoid accessing a ringbuffer not initialized yet If the KVP (or VSS) daemon starts before the VMBus channel's ringbuffer is fully initialized, we can hit the panic below: hv_utils: Registering HyperV Utility Driver hv_vmbus: registering driver hv_utils ... BUG: kernel NULL pointer dereference, address: 0000000000000000 CPU: 44 UID: 0 PID: 2552 Comm: hv_kvp_daemon Tainted: G E 6.11.0-rc3+ #1 RIP: 0010:hv_pkt_iter_first+0x12/0xd0 Call Trace: ... vmbus_recvpacket	2025-01-11	5.5

		hv_kvp_onchannelcallback vmbus_on_event tasklet_action_common tasklet_action handle_softirqs irq_exit_rcu sysvec_hyperv_stimer0 </IRQ> <TASK> asm_sysvec_hyperv_stimer0 ... kvp_register_done hvt_op_read vfs_read ksys_read __x64_sys_read This can happen because the KVP/VSS channel callback can be invoked even before the channel is fully opened: 1) as soon as hv_kvp_init() -> hvutil_transport_init() creates /dev/vmbus/hv_kvp, the kvp daemon can open the device file immediately and register itself to the driver by writing a message KVP_OP_REGISTER1 to the file (which is handled by kvp_on_msg() ->kvp_handle_handshake()) and reading the file for the driver's response, which is handled by hvt_op_read(), which calls hvt->on_read(), i.e. kvp_register_done(). 2) the problem with kvp_register_done() is that it can cause the channel callback to be called even before the channel is fully opened, and when the channel callback is starting to run, util_probe()-> vmbus_open() may have not initialized the ringbuffer yet, so the callback can hit the panic of NULL pointer dereference. To reproduce the panic consistently, we can add a "ssleep(10)" for KVP in __vmbus_open(), just before the first hv_ringbuffer_init(), and then we unload and reload the driver hv_utils, and run the daemon manually within the 10 seconds. Fix the panic by reordering the steps in util_probe() so the char dev entry used by the KVP or VSS daemon is not created until after vmbus_open() has completed. This reordering prevents the race condition from happening.		
CVE-2024-56369	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/modes: Avoid divide by zero harder in drm_mode_vrefresh() drm_mode_vrefresh() is trying to avoid divide by zero by checking whether htotal or vtotal are zero. But we may still end up with a div-by-zero of vtotal*htotal*...	2025-01-11	5.5
CVE-2024-57799	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: phy: rockchip: samsung-hdptx: Set drvdata before enabling runtime PM In some cases, rk_hdptx_phy_runtime_resume() may be invoked before platform_set_drvdata() is executed in ->probe(), leading to a NULL pointer dereference when using the return of dev_get_drvdata(). Ensure platform_set_drvdata() is called before devm_pm_runtime_enable().	2025-01-11	5.5

CVE-2024-57807	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved:
		
		scsi: megaraid_sas: Fix for a potential deadlock
		
		This fixes a 'possible circular locking dependency detected' warning
		CPU0 CPU1
		---- ----
		lock(&instance->reset_mutex);
		lock(&shost->scan_mutex);
		lock(&instance->reset_mutex);
		lock(&shost->scan_mutex);
		
		Fix this by temporarily releasing the reset_mutex.
			2025-01-11	5.5

CVE-2024-57872	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: pltfrm: Dellocate HBA during ufshcd_pltfrm_remove() This will ensure that the scsi host is cleaned up properly using scsi_host_dev_release(). Otherwise, it may lead to memory leaks.	2025-01-11	5.5
CVE-2024-57881	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mm/page_alloc: don't call pfn_to_page() on possibly non-existent PFN in split_large_buddy()	2025-01-11	5.5

		In split_large_buddy(), we might call pfn_to_page() on a PFN that might not exist. In corner cases, such as when freeing the highest pageblock in the last memory section, this could result with CONFIG_SPARSEMEM && !CONFIG_SPARSEMEM_EXTREME in __pfn_to_section() returning NULL and and __section_mem_map_addr() dereferencing that NULL pointer. Let's fix it, and avoid doing a pfn_to_page() call for the first iteration, where we already have the page. So far this was found by code inspection, but let's just CC stable as the fix is easy.		
CVE-2024-52891	ibm - Concert Software	IBM Concert Software 1.0.0, 1.0.1, 1.0.2, 1.0.2.1, and 1.0.3 could allow an authenticated user to inject malicious information or obtain information from log files due to improper log neutralization.	2025-01-07	5.4
CVE-2025-0237	mozilla - multiple products	The WebChannel API, which is used to transport various information across processes, did not check the sending principal but rather accepted the principal being sent. This could have led to privilege escalation attacks. This vulnerability affects Firefox < 134, Firefox ESR < 128.6, Thunderbird < 134, and Thunderbird < 128.6.	2025-01-07	5.4
CVE-2025-20166	cisco - Cisco Common Services Platform Collector Software	A vulnerability in the web-based management interface of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface._x000D_ _x000D_ This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have at least a low-privileged account on an affected device._x000D_ Cisco has not released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2025-01-08	5.4
CVE-2025-20167	cisco - Cisco Common Services Platform Collector Software	A vulnerability in the web-based management interface of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface._x000D_ _x000D_ This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have at least a low-privileged account on an affected device._x000D_ Cisco has not released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2025-01-08	5.4
CVE-2025-20168	cisco - Cisco Common Services Platform Collector Software	A vulnerability in the web-based management interface of Cisco Common Services Platform Collector (CSPC) could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface._x000D_ _x000D_ This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have at least a low-privileged account on an affected device._x000D_ Cisco has not released software updates that address this vulnerability. There are no workarounds that address this vulnerability.	2025-01-08	5.4
CVE-2024-43176	ibm - OpenPages	IBM OpenPages 9.0 could allow an authenticated user to obtain sensitive information such as configurations that should only be available to privileged users.	2025-01-09	5.4
CVE-2024-13237	drupal - File Entity (fieldable files)	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal File Entity (fieldable files) allows Cross-Site Scripting (XSS).This issue affects File Entity (fieldable files): from 7.X-* before 7.X-2.38.	2025-01-09	5.4
CVE-2024-13238	drupal - Typogrify	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Typogrify allows Cross-Site Scripting (XSS).This issue affects Typogrify: from 0.0.0 before 1.3.0.	2025-01-09	5.4
CVE-2024-13245	drupal - CKEditor 4 LTS - WYSIWYG HTML editor	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal CKEditor 4 LTS - WYSIWYG HTML editor allows Cross-Site Scripting (XSS).This issue affects CKEditor 4 LTS - WYSIWYG HTML editor: from 1.0.0 before 1.0.1.	2025-01-09	5.4
CVE-2024-13249	drupal - Node Access Rebuild Progressive	Improper Ownership Management vulnerability in Drupal Node Access Rebuild Progressive allows Target Influence via Framing.This issue affects Node Access Rebuild Progressive: from 7.X-1.0 before 7.X-1.2.	2025-01-09	5.4
CVE-2024-13252	drupal - TacJS	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal TacJS allows Cross-Site Scripting (XSS).This issue affects TacJS: from 0.0.0 before 6.5.0.	2025-01-09	5.4
CVE-2024-13273	drupal - Open Social	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Open Social allows Cross-Site Scripting (XSS).This issue affects Open Social: from 0.0.0 before 12.3.8, from 12.4.0 before 12.4.5, from 13.0.0 before 13.0.0-alpha11.	2025-01-09	5.4
CVE-2024-13286	drupal - SVG Embed	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal SVG Embed allows Cross-Site Scripting (XSS).This issue affects SVG Embed: from 0.0.0 before 2.1.2.	2025-01-09	5.4
CVE-2024-13287	drupal - Views SVG Animation	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Views SVG Animation allows Cross-Site Scripting (XSS).This issue affects Views SVG Animation: from 0.0.0 before 1.0.1.	2025-01-09	5.4

CVE-2024-13289	drupal - Cookiebot + GTM	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Cookiebot + GTM allows Cross-Site Scripting (XSS).This issue affects Cookiebot + GTM: from 0.0.0 before 1.0.18.	2025-01-09	5.4
CVE-2024-13294	drupal - POST File	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal POST File allows Cross-Site Scripting (XSS).This issue affects POST File: from 0.0.0 before 1.0.2.	2025-01-09	5.4
CVE-2024-52367	ibm - Concert Software	IBM Concert Software 1.0.0, 1.0.1, 1.0.2, 1.0.2.1, and 1.0.3 could disclose sensitive system information to an unauthorized actor that could be used in further attacks against the system.	2025-01-07	5.3
CVE-2024-52893	ibm - Concert Software	IBM Concert Software 1.0.0, 1.0.1, 1.0.2, 1.0.2.1, and 1.0.3 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.	2025-01-07	5.3
CVE-2024-45640	ibm - Security QRadar EDR	IBM Security ReaQta 3.12 returns sensitive information in an HTTP response that could be used in further attacks against the system.	2025-01-07	5.3
CVE-2025-0238	mozilla - multiple products	Assuming a controlled failed memory allocation, an attacker could have caused a use-after-free, leading to a potentially exploitable crash. This vulnerability affects Firefox < 134, Firefox ESR < 128.6, Firefox ESR < 115.19, Thunderbird < 134, and Thunderbird < 128.6.	2025-01-07	5.3
CVE-2025-0244	mozilla - Firefox	When redirecting to an invalid protocol scheme, an attacker could spoof the address bar. *Note: This issue only affected Android operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 134.	2025-01-07	5.3
CVE-2024-13246	drupal - Node Access Rebuild Progressive	Improper Ownership Management vulnerability in Drupal Node Access Rebuild Progressive allows Target Influence via Framing.This issue affects Node Access Rebuild Progressive: from 0.0.0 before 2.0.2.	2025-01-09	5.3
CVE-2024-13257	drupal - Commerce View Receipt	Incorrect Authorization vulnerability in Drupal Commerce View Receipt allows Forceful Browsing.This issue affects Commerce View Receipt: from 0.0.0 before 1.0.3.	2025-01-09	5.3
CVE-2024-13266	drupal - Responsive and off-canvas menu	Incorrect Authorization vulnerability in Drupal Responsive and off-canvas menu allows Forceful Browsing.This issue affects Responsive and off-canvas menu: from 0.0.0 before 4.4.4.	2025-01-09	5.3
CVE-2024-13274	drupal - Open Social	Improper Control of Interaction Frequency vulnerability in Drupal Open Social allows Functionality Misuse.This issue affects Open Social: from 0.0.0 before 12.3.8, from 12.4.0 before 12.4.5.	2025-01-09	5.3
CVE-2024-13275	drupal - Security Kit	Access of Resource Using Incompatible Type ('Type Confusion') vulnerability in Drupal Security Kit allows HTTP DoS.This issue affects Security Kit: from 0.0.0 before 2.0.3.	2025-01-09	5.3
CVE-2024-13290	drupal - OhDear Integration	Incorrect Authorization vulnerability in Drupal OhDear Integration allows Forceful Browsing.This issue affects OhDear Integration: from 0.0.0 before 2.0.4.	2025-01-09	5.3
CVE-2024-13302	drupal - Pages Restriction Access	Incorrect Authorization vulnerability in Drupal Pages Restriction Access allows Forceful Browsing.This issue affects Pages Restriction Access: from 2.0.0 before 2.0.3.	2025-01-09	5.3
CVE-2024-13303	drupal - Download All Files	Missing Authorization vulnerability in Drupal Download All Files allows Forceful Browsing.This issue affects Download All Files: from 0.0.0 before 2.0.2.	2025-01-09	5.3
CVE-2025-0243	mozilla - multiple products	Memory safety bugs present in Firefox 133, Thunderbird 133, Firefox ESR 128.5, and Thunderbird 128.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 134, Firefox ESR < 128.6, Thunderbird < 134, and Thunderbird < 128.6.	2025-01-07	5.1
CVE-2024-47475	dell - multiple products	Dell PowerScale OneFS 8.2.2.x through 9.8.0.x contains an incorrect permission assignment for critical resource vulnerability. A locally authenticated attacker could potentially exploit this vulnerability, leading to denial of service.	2025-01-06	5.0
CVE-2024-45100	ibm - Security QRadar EDR	IBM Security ReaQta 3.12 could allow a privileged user to cause a denial of service by sending multiple administration requests due to improper allocation of resources.	2025-01-07	4.9
CVE-2024-12806	sonicwall - SonicOS	A post-authentication absolute path traversal vulnerability in SonicOS management allows a remote attacker to read an arbitrary file.	2025-01-09	4.9
CVE-2025-20123	cisco - Cisco Crosswork Network Change Automation	Multiple vulnerabilities in the web-based management interface of Cisco Crosswork Network Controller could allow an authenticated, remote attacker to conduct cross-site scripting (XSS) attacks against users of the interface of an affected system._x000D_ _x000D_ These vulnerabilities exist because the web-based management interface does not properly validate user-supplied input. An attacker could exploit these vulnerabilities by inserting malicious data into specific data fields in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker must have valid administrative credentials._x000D_ Cisco has released software updates that address these vulnerabilities. There are no workarounds that address these vulnerabilities.	2025-01-08	4.8
CVE-2025-20126	cisco - Cisco ThousandEyes Endpoint Agent	A vulnerability in certification validation routines of Cisco ThousandEyes Endpoint Agent for macOS and RoomOS could allow an unauthenticated, remote attacker to intercept or manipulate metrics information._x000D_ _x000D_ This vulnerability exists because the affected software does not properly validate certificates for hosted metrics services. An on-path attacker could exploit this vulnerability by intercepting network traffic using a crafted certificate. A successful exploit could allow the attacker to masquerade as a trusted host and monitor or change communications between the remote metrics service and the vulnerable client.	2025-01-08	4.8
CVE-2024-13247	drupal - Coffee	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Coffee allows Cross-Site Scripting (XSS).This issue affects Coffee: from 0.0.0 before 1.4.0.	2025-01-09	4.8
CVE-2024-13262	drupal - View Password	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal View Password allows Cross-Site Scripting (XSS).This issue affects View Password: from 0.0.0 before 6.0.4.	2025-01-09	4.8
CVE-2024-13292	drupal - Tooltip	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Tooltip allows Cross-Site Scripting (XSS).This issue affects Tooltip: from 0.0.0 before 1.1.2.	2025-01-09	4.8

CVE-2024-13298	drupal - Tarte au Citron	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Tarte au Citron allows Cross-Site Scripting (XSS).This issue affects Tarte au Citron: from 2.0.0 before 2.0.5.	2025-01-09	4.8
CVE-2024-13305	drupal - Entity Form Steps	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Drupal Entity Form Steps allows Cross-Site Scripting (XSS).This issue affects Entity Form Steps: from 0.0.0 before 1.1.4.	2025-01-09	4.8
CVE-2024-13304	drupal - Minify JS	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Minify JS allows Cross Site Request Forgery.This issue affects Minify JS: from 0.0.0 before 3.0.3.	2025-01-09	4.5
CVE-2024-56434	huawei - multiple products	UAF vulnerability in the device node access module Impact: Successful exploitation of this vulnerability may cause service exceptions of the device.	2025-01-08	4.4
CVE-2023-52954	huawei - multiple products	Vulnerability of improper permission control in the Gallery module Impact: Successful exploitation of this vulnerability may affect availability.	2025-01-08	4.4
CVE-2022-22363	ibm - multiple products	IBM Cognos Controller 11.0.0 through 11.0.1 and IBM Controller 11.1.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.	2025-01-07	4.3
CVE-2024-25037	ibm - multiple products	IBM Cognos Controller 11.0.0 through 11.0.1 and IBM Controller 11.1.0 could allow a remote attacker to obtain sensitive information when a stack trace is returned in the browser.	2025-01-07	4.3
CVE-2024-56445	huawei - harmonyos	Instruction authentication bypass vulnerability in the Findnetwork module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	2025-01-08	4.3
CVE-2025-22215	vmware - multiple products	VMware Aria Automation contains a server-side request forgery (SSRF) vulnerability. A malicious actor with "Organization Member" access to Aria Automation may exploit this vulnerability enumerate internal services running on the host/network.	2025-01-08	4.3
CVE-2024-13288	drupal - Monster Menus	Deserialization of Untrusted Data vulnerability in Drupal Monster Menus allows Object Injection.This issue affects Monster Menus: from 0.0.0 before 9.3.4, from 9.4.0 before 9.4.2.	2025-01-09	4.3
CVE-2025-23108	mozilla - Firefox for iOS	Opening Javascript links in a new tab via long-press in the Firefox iOS client could result in a malicious script spoofing the URL of the new tab. This vulnerability affects Firefox for iOS < 134.	2025-01-11	4.3
CVE-2024-54120	huawei - harmonyos	Race condition vulnerability in the distributed notification module Impact: Successful exploitation of this vulnerability may cause features to perform abnormally.	2025-01-08	4.1
CVE-2024-56441	huawei - multiple products	Race condition vulnerability in the Bastet module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-01-08	4.1
CVE-2025-0239	mozilla - multiple products	When using Alt-Svc, ALPN did not properly validate certificates when the original server is redirecting to an insecure site. This vulnerability affects Firefox < 134, Firefox ESR < 128.6, Thunderbird < 134, and Thunderbird < 128.6.	2025-01-07	4.0
CVE-2025-0240	mozilla - multiple products	Parsing a JavaScript module as JSON could under some circumstances cause cross-compartment access, which may result in a use-after-free. This vulnerability affects Firefox < 134, Firefox ESR < 128.6, Thunderbird < 134, and Thunderbird < 128.6.	2025-01-07	4.0
CVE-2024-56446	huawei - harmonyos	Vulnerability of variables not being initialized in the notification module Impact: Successful exploitation of this vulnerability may affect availability.	2025-01-08	4.0
CVE-2021-20455	ibm - multiple products	IBM Cognos Controller 11.0.0 through 11.0.1 and IBM Controller 11.1.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.	2025-01-07	3.7
CVE-2024-13261	drupal - Acquia DAM	Cross-Site Request Forgery (CSRF) vulnerability in Drupal Acquia DAM allows Cross Site Request Forgery.This issue affects Acquia DAM: from 0.0.0 before 1.0.13, from 1.1.0 before 1.1.0-beta3.	2025-01-09	3.5
CVE-2024-54010	hewlett packard enterprise (hpe) - AOS-CX	A vulnerability in the firewall component of HPE Aruba Networking CX 10000 Series Switches exists. It could allow an unauthenticated adjacent attacker to conduct a packet forwarding attack against the ICMP and UDP protocol. For this attack to be successful an attacker requires a switch configuration that allows packets routing (at layer 3). Configurations that do not allow network traffic routing are not impacted. Successful exploitation could allow an attacker to bypass security policies, potentially leading to unauthorized data exposure.	2025-01-08	3.4
CVE-2025-0245	mozilla - Firefox	Under certain circumstances, a user opt-in setting that Focus should require authentication before use could have been be bypassed. This vulnerability affects Firefox < 134.	2025-01-07	3.3
CVE-2024-51472	ibm - multiple products	IBM UrbanCode Deploy (UCD) 7.2 through 7.2.3.13, 7.3 through 7.3.2.8, and IBM DevOps Deploy 8.0 through 8.0.1.3 are vulnerable to HTML injection. This vulnerability may allow a user to embed arbitrary HTML tags in the Web UI potentially leading to sensitive information disclosure.	2025-01-06	3.1
CVE-2024-13293	drupal - POST File	Cross-Site Request Forgery (CSRF) vulnerability in Drupal POST File allows Cross Site Request Forgery.This issue affects POST File: from 0.0.0 before 1.0.2.	2025-01-09	3.1