الهيئة الوطنية للأمن السيبراني
Nat onal Cybersecurity Authority

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

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

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 28th of July to 3rd of August. 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**

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 ٢٨ يوليو إلى ٣ اغسطس. 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**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2024-40782	Apple	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 16.7.9 and iPadOS 16.7.9, Safari 17.6, iOS 17.6 and iPadOS 17.6, watchOS 10.6, tvOS 17.6, visionOS 1.3, macOS Sonoma 14.6. Processing maliciously crafted web content may lead to an unexpected process crash.	2024-07-29	9.8	Critical
CVE-2024-42154	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp_metrics: validate source addr length I don't see anything checking that TCP_METRICS_ATTR_SADDR_IPV4 is at least 4 bytes long, and the policy doesn't have an entry for this attribute at all (neither does it for IPv6 but v6 is manually validated).	2024-07-30	9.8	Critical
CVE-2024-38182	Microsoft	Weak authentication in Microsoft Dynamics 365 allows an unauthenticated attacker to elevate privileges over a network.	2024-07-31	9	Critical
CVE-2024-6990	Google	Uninitialized Use in Dawn in Google Chrome on Android prior to 127.0.6533.88 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Critical)	2024-08-01	8.8	High
CVE-2024-7256	Google	Insufficient data validation in Dawn in Google Chrome on Android prior to 127.0.6533.88 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2024-08-01	8.8	High
CVE-2024-38879	Siemens	A vulnerability has been identified in Omnivise T3000 Application Server (All versions). The affected system exposes the port of an internal application on the public network interface allowing an attacker to circumvent authentication and directly access the exposed application.	2024-08-02	8.7	High
CVE-2023-42918	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14. A sandboxed process may be able to circumvent sandbox restrictions.	2024-07-29	8.6	High
CVE-2024-38876	Siemens	A vulnerability has been identified in Omnivise T3000 Application Server (All versions >= R9.2), Omnivise T3000 Domain Controller (All versions >= R9.2), Omnivise T3000 Product Data Management (PDM) (All versions >= R9.2), Omnivise T3000 Terminal Server (All versions >= R9.2), Omnivise T3000 Thin Client (All versions >= R9.2), Omnivise T3000 Whitelisting Server (All versions >= R9.2). The affected application regularly executes user modifiable code as a privileged user. This could allow a local authenticated attacker to execute arbitrary code with elevated privileges.	2024-08-02	8.5	High
CVE-2024-37381	Ivanti	An unspecified SQL Injection vulnerability in Core server of Ivanti EPM 2024 flat allows an authenticated attacker within the same network to execute arbitrary code.	2024-07-29	8.4	High
CVE-2024-40781	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.6, macOS Monterey 12.7.6, macOS Ventura 13.6.8. A local attacker may be able to elevate their privileges.	2024-07-29	8.4	High

CVE-2024-40800	Apple	An input validation issue was addressed with improved input validation. This issue is fixed in macOS Sonoma 14.6, macOS Monterey 12.7.6, macOS Ventura 13.6.8. An app may be able to modify protected parts of the file system.	2024-07-29	8.4	High
CVE-2024-40811	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.6. An app may be able to modify protected parts of the file system.	2024-07-29	8.4	High
CVE-2024-40821	Apple	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sonoma 14.6, macOS Monterey 12.7.6, macOS Ventura 13.6.8. Third party app extensions may not receive the correct sandbox restrictions.	2024-07-29	8.4	High
CVE-2024-40828	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.6, macOS Monterey 12.7.6, macOS Ventura 13.6.8. A malicious app may be able to gain root privileges.	2024-07-29	8.4	High
CVE-2024-6748	ManageEngine	Zohocorp ManageEngine OpManager, OpManager Plus, OpManager MSP and RMM versions 128317 and below are vulnerable to authenticated SQL injection in the URL monitoring.	2024-07-29	8.3	High
CVE-2024-38877	Siemens	A vulnerability has been identified in Omnivise T3000 Application Server (All versions), Omnivise T3000 Domain Controller (All versions), Omnivise T3000 Network Intrusion Detection System (NIDS) (All versions), Omnivise T3000 Product Data Management (PDM) (All versions), Omnivise T3000 Security Server (All versions), Omnivise T3000 Terminal Server (All versions), Omnivise T3000 Thin Client (All versions), Omnivise T3000 Whitelisting Server (All versions). The affected devices stores initial system credentials without sufficient protection. An attacker with remote shell access or physical access could retrieve the credentials leading to confidentiality loss allowing the attacker to laterally move within the affected network.	2024-08-02	8.3	High
CVE-2024-41087	Linux	In the Linux kernel, the following vulnerability has been resolved: ata: libata-core: Fix double free on error If e.g. the ata_port_alloc() call in ata_host_alloc() fails, we will jump to the err_out label, which will call devres_release_group(). devres_release_group() will trigger a call to ata_host_release(). ata_host_release() calls kfree(host), so executing the kfree(host) in ata_host_alloc() will lead to a double free: kernel BUG at mm/slub.c:553! Oops: invalid opcode: 0000 [#1] PREEMPT SMP NOPTI CPU: 11 PID: 599 Comm: (udev-worker) Not tainted 6.10.0-rc5 #47 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-2.fc40 04/01/2014 RIP: 0010:kfree+0x2cf/0x2f0 Code: 5d 41 5e 41 5f 5d e9 80 d6 ff ff 4d 89 f1 41 b8 01 00 00 00 48 89 d9 48 89 da RSP: 0018:ffffc90000f377f0 EFLAGS: 00010246 RAX: ffff888112b1f2c0 RBX: ffff888112b1f2c0 RCX: ffff888112b1f320 RDX: 000000000000400b RSI: ffffffffc02c9de5 RDI: ffff888112b1f2c0 RBP: ffffc90000f37830 R08: 0000000000000000 R09: 0000000000000000 R10: ffffc90000f37610 R11: 617461203a736b6e R12: ffffea00044ac780 R13: ffff888100046400 R14: ffffffffc02c9de5 R15: 0000000000000006 FS: 00007f2f1cabe980(0000) GS:ffff88813b380000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f2f1c3acf75 CR3: 0000000111724000 CR4: 0000000000750ef0 PKRU: 55555554 Call Trace: <TASK> ? __die_body.cold+0x19/0x27 ? die+0x2e/0x50 ? do_trap+0xca/0x110 ? do_error_trap+0x6a/0x90 ? kfree+0x2cf/0x2f0 ? exc_invalid_op+0x50/0x70 ? kfree+0x2cf/0x2f0 ? asm_exc_invalid_op+0x1a/0x20 ? ata_host_alloc+0xf5/0x120 [libata] ? ata_host_alloc+0xf5/0x120 [libata] ? kfree+0x2cf/0x2f0 ata_host_alloc+0xf5/0x120 [libata] ata_host_alloc_pinfo+0x14/0xa0 [libata]	2024-07-29	7.8	High

		ahci_init_one+0x6c9/0xd20 [ahci] Ensure that we will not call kfree(host) twice, by performing the kfree() only if the devres_open_group() call failed.			
CVE-2024-41092	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/i915/gt: Fix potential UAF by revoke of fence registers CI has been sporadically reporting the following issue triggered by igt@i915_selftest@live@hangcheck on ADL-P and similar machines: <6> [414.049203] i915: Running intel_hangcheck_live_selftests/igt_reset_evict_fence ... <6> [414.068804] i915 0000:00:02.0: [drm] GT0: GUC: submission enabled <6> [414.068812] i915 0000:00:02.0: [drm] GT0: GUC: SLPC enabled <3> [414.070354] Unable to pin Y-tiled fence; err:-4 <3> [414.071282] i915_vma_revoke_fence:301 GEM_BUG_ON(!i915_active_is_idle(&fence->active)) ... <4>[609.603992] ------------[cut here]------------ <2>[609.603995] kernel BUG at drivers/gpu/drm/i915/gt/intel_ggtt_fencing.c:301! <4>[609.604003] invalid opcode: 0000 [#1] PREEMPT SMP NOPTI <4>[609.604006] CPU: 0 PID: 268 Comm: kworker/u64:3 Tainted: G U W 6.9.0-CI_DRM_14785-g1ba62f8cea9c+ #1 <4>[609.604008] Hardware name: Intel Corporation Alder Lake Client Platform/AlderLake-P DDR4 RVP, BIOS RPLPFWI1.R00.4035.A00.2301200723 01/20/2023 <4>[609.604010] Workqueue: i915 __i915_gem_free_work [i915] <4>[609.604149] RIP: 0010:i915_vma_revoke_fence+0x187/0x1f0 [i915] ... <4>[609.604271] Call Trace: <4>[609.604273] <TASK> ... <4>[609.604716] __i915_vma_evict+0x2e9/0x550 [i915] <4>[609.604852] __i915_vma_unbind+0x7c/0x160 [i915] <4>[609.604977] force_unbind+0x24/0xa0 [i915] <4>[609.605098] i915_vma_destroy+0x2f/0xa0 [i915] <4>[609.605210] __i915_gem_object_pages_fini+0x51/0x2f0 [i915] <4>[609.605330] __i915_gem_free_objects.isra.0+0x6a/0xc0 [i915] <4>[609.605440] process_scheduled_works+0x351/0x690 ... In the past, there were similar failures reported by CI from other IGT tests, observed on other platforms. Before commit 63baf4f3d587 ("drm/i915/gt: Only wait for GPU activity before unbinding a GGTT fence"), i915_vma_revoke_fence() was waiting for idleness of vma->active via fence_update(). That commit introduced vma->fence->active in order for the fence_update() to be able to wait selectively on that one instead of vma->active since only idleness of fence registers was needed. But then, another commit 0d86ee35097a ("drm/i915/gt: Make fence revocation unequivocal") replaced the call to fence_update() in i915_vma_revoke_fence() with only fence_write(), and also added that GEM_BUG_ON(!i915_active_is_idle(&fence->active)) in front. No justification was provided on why we might then expect idleness of vma->fence->active without first waiting on it. The issue can be potentially caused by a race among revocation of fence registers on one side and sequential execution of signal callbacks	2024-07-29	7.8	High

		invoked on completion of a request that was using them on the other, still processed in parallel to revocation of those fence registers. Fix it by waiting for idleness of vma->fence->active in i915_vma_revoke_fence(). (cherry picked from commit 24bb052d3dd499c5956abad5f7d8e4fd07da7fb1)			
CVE-2024-41096	Linux	In the Linux kernel, the following vulnerability has been resolved: PCI/MSI: Fix UAF in msi_capability_init KFENCE reports the following UAF: BUG: KFENCE: use-after-free read in __pci_enable_msi_range+0x2c0/0x488 Use-after-free read at 0x0000000024629571 (in kfence-#12): __pci_enable_msi_range+0x2c0/0x488 pci_alloc_irq_vectors_affinity+0xec/0x14c pci_alloc_irq_vectors+0x18/0x28 kfence-#12: 0x0000000008614900-0x00000000e06c228d, size=104, cache=kmalloc-128 allocated by task 81 on cpu 7 at 10.808142s: __kmem_cache_alloc_node+0x1f0/0x2bc kmalloc_trace+0x44/0x138 msi_alloc_desc+0x3c/0x9c msi_domain_insert_msi_desc+0x30/0x78 msi_setup_msi_desc+0x13c/0x184 __pci_enable_msi_range+0x258/0x488 pci_alloc_irq_vectors_affinity+0xec/0x14c pci_alloc_irq_vectors+0x18/0x28 freed by task 81 on cpu 7 at 10.811436s: msi_domain_free_descs+0xd4/0x10c msi_domain_free_locked.part.0+0xc0/0x1d8 msi_domain_alloc_irqs_all_locked+0xb4/0xbc pci_msi_setup_msi_irqs+0x30/0x4c __pci_enable_msi_range+0x2a8/0x488 pci_alloc_irq_vectors_affinity+0xec/0x14c pci_alloc_irq_vectors+0x18/0x28 Descriptor allocation done in: __pci_enable_msi_range msi_capability_init msi_setup_msi_desc msi_insert_msi_desc msi_domain_insert_msi_desc msi_alloc_desc ... Freed in case of failure in __msi_domain_alloc_locked() __pci_enable_msi_range msi_capability_init pci_msi_setup_msi_irqs msi_domain_alloc_irqs_all_locked msi_domain_alloc_locked __msi_domain_alloc_locked => fails msi_domain_free_locked ... That failure propagates back to pci_msi_setup_msi_irqs() in msi_capability_init() which accesses the descriptor for unmasking in the error exit path. Cure it by copying the descriptor and using the copy for the error exit path unmask operation. [tglx: Massaged change log]	2024-07-29	7.8	High
CVE-2024-42072	Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix may_goto with negative offset. Zac's syzbot crafted a bpf prog that exposed two bugs in may_goto.	2024-07-29	7.8	High

		The 1st bug is the way may_goto is patched. When offset is negative it should be patched differently. The 2nd bug is in the verifier: when current state may_goto_depth is equal to visited state may_goto_depth it means there is an actual infinite loop. It's not correct to prune exploration of the program at this point. Note, that this check doesn't limit the program to only one may_goto insn, since 2nd and any further may_goto will increment may_goto_depth only in the queued state pushed for future exploration. The current state will have may_goto_depth == 0 regardless of number of may_goto insns and the verifier has to explore the program until bpf_exit.			
CVE-2023-42958	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Ventura 13.4. An app may be able to gain elevated privileges.	2024-07-29	7.8	High
CVE-2024-27826	Apple	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.6.8, macOS Sonoma 14.5, macOS Monterey 12.7.6, watchOS 10.5, visionOS 1.3, tvOS 17.5, iOS 17.5 and iPadOS 17.5. An app may be able to execute arbitrary code with kernel privileges.	2024-07-29	7.8	High
CVE-2024-40784	Apple	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 16.7.9 and iPadOS 16.7.9, macOS Ventura 13.6.8, iOS 17.6 and iPadOS 17.6, watchOS 10.6, tvOS 17.6, visionOS 1.3, macOS Sonoma 14.6. Processing a maliciously crafted file may lead to unexpected app termination.	2024-07-29	7.8	High
CVE-2024-40802	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.6, macOS Monterey 12.7.6, macOS Ventura 13.6.8. A local attacker may be able to elevate their privileges.	2024-07-29	7.8	High
CVE-2024-42159	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: mpi3mr: Sanitise num_phys Information is stored in mr_sas_port->phy_mask, values larger then size of this field shouldn't be allowed.	2024-07-30	7.8	High
CVE-2024-42160	Linux	In the Linux kernel, the following vulnerability has been resolved: f2fs: check validation of fault attrs in f2fs_build_fault_attr() - It missed to check validation of fault attrs in parse_options(), let's fix to add check condition in f2fs_build_fault_attr(). - Use f2fs_build_fault_attr() in __sbi_store() to clean up code.	2024-07-30	7.8	High
CVE-2024-42161	Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Avoid uninitialized value in BPF_CORE_READ_BITFIELD [Changes from V1: - Use a default branch in the switch statement to initialize `val'.]  GCC warns that `val' may be used uninitialized in the BPF_CRE_READ_BITFIELD macro, defined in bpf_core_read.h as: [...] unsigned long long val; \ [...] \ switch (__CORE_RELO(s, field, BYTE_SIZE)) { \ case 1: val = *(const unsigned char *)p; break; \ case 2: val = *(const unsigned short *)p; break; \ case 4: val = *(const unsigned int *)p; break; \ case 8: val = *(const unsigned long long *)p; break; \ } \ [...] val; \ } \ This patch adds a default entry in the switch statement that sets `val' to zero in order to avoid the warning, and random values to be used in case __builtin_preserve_field_info returns unexpected values for BPF_FIELD_BYTE_SIZE. Tested in bpf-next master. No regressions.	2024-07-30	7.8	High

CVE-2024-42224	Linux	In the Linux kernel, the following vulnerability has been resolved: net: dsa: mv88e6xxx: Correct check for empty list Since commit a3c53be55c95 ("net: dsa: mv88e6xxx: Support multiple MDIO busses") mv88e6xxx_default_mdio_bus() has checked that the return value of list_first_entry() is non-NULL. This appears to be intended to guard against the list chip->mdios being empty. However, it is not the correct check as the implementation of list_first_entry is not designed to return NULL for empty lists. Instead, use list_first_entry_or_null() which does return NULL if the list is empty. Flagged by Smatch. Compile tested only.	2024-07-30	7.8	High
CVE-2024-32857	Dell	Dell Peripheral Manager, versions prior to 1.7.6, contain an uncontrolled search path element vulnerability. An attacker could potentially exploit this vulnerability through preloading malicious DLL or symbolic link exploitation, leading to arbitrary code execution and escalation of privilege	2024-07-31	7.8	High
CVE-2024-37127	Dell	Dell Peripheral Manager, versions prior to 1.7.6, contain an uncontrolled search path element vulnerability. An attacker could potentially exploit this vulnerability through preloading malicious DLL or symbolic link exploitation, leading to arbitrary code execution and escalation of privilege	2024-07-31	7.8	High
CVE-2024-37142	Dell	Dell Peripheral Manager, versions prior to 1.7.6, contain an uncontrolled search path element vulnerability. An attacker could potentially exploit this vulnerability through preloading malicious DLL or symbolic link exploitation, leading to arbitrary code execution and escalation of privilege	2024-07-31	7.8	High
CVE-2019-6197	Lenovo	A vulnerability was reported in Lenovo PC Manager prior to version 2.8.90.11211 that could allow a local attacker to escalate privileges.	2024-07-31	7.8	High
CVE-2019-6198	Lenovo	A vulnerability was reported in Lenovo PC Manager prior to version 2.8.90.11211 that could allow a local attacker to escalate privileges.	2024-07-31	7.8	High
CVE-2023-1577	Lenovo	A path hijacking vulnerability was reported in Lenovo Driver Manager prior to version 3.1.1307.1308 that could allow a local user to execute code with elevated privileges.	2024-07-31	7.8	High
CVE-2024-39392	Adobe	InDesign Desktop versions ID18.5.2, ID19.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-02	7.8	High
CVE-2024-40805	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in watchOS 10.6, macOS Sonoma 14.6, iOS 17.6 and iPadOS 17.6, tvOS 17.6. An app may be able to bypass Privacy preferences.	2024-07-29	7.7	High
CVE-2024-40824	Apple	This issue was addressed through improved state management. This issue is fixed in watchOS 10.6, macOS Sonoma 14.6, iOS 17.6 and iPadOS 17.6, tvOS 17.6. An app may be able to bypass Privacy preferences.	2024-07-29	7.7	High
CVE-2024-27886	Apple	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sonoma 14.4. An unprivileged app may be able to log keystrokes in other apps including those using secure input mode.	2024-07-29	7.5	High
CVE-2024-40829	Apple	The issue was addressed with improved checks. This issue is fixed in watchOS 10.6, iOS 17.6 and iPadOS 17.6, iOS 16.7.9 and iPadOS 16.7.9, macOS Ventura 13.6.8. An attacker may be able to view restricted content from the lock screen.	2024-07-29	7.5	High
CVE-2024-40836	Apple	A logic issue was addressed with improved checks. This issue is fixed in watchOS 10.6, macOS Sonoma 14.6, iOS 17.6 and iPadOS 17.6, iOS 16.7.9 and iPadOS 16.7.9. A shortcut may be able to use sensitive data with certain actions without prompting the user.	2024-07-29	7.5	High
CVE-2024-42225	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: replace skb_put with skb_put_zero Avoid potentially reusing uninitialized data	2024-07-30	7.5	High
CVE-2024-27888	Apple	A permissions issue was addressed by removing vulnerable code and adding additional checks. This issue is fixed in macOS Sonoma 14.4. An app may be able to modify protected parts of the file system.	2024-07-29	7.1	High

CVE-2024-40783	Apple	The issue was addressed with improved restriction of data container access. This issue is fixed in macOS Sonoma 14.6, macOS Monterey 12.7.6, macOS Ventura 13.6.8. A malicious application may be able to bypass Privacy preferences.	2024-07-29	7.1	High
CVE-2024-40814	Apple	A downgrade issue was addressed with additional code-signing restrictions. This issue is fixed in macOS Sonoma 14.6. An app may be able to bypass Privacy preferences.	2024-07-29	7.1	High
CVE-2023-28074	Dell	Dell BSAFE Crypto-C Micro Edition 4.1.5 and Dell BSAFE Micro Edition Suite, versions 4.0 through 4.6.1 and version 5.0 contain a buffer over-read vulnerability.	2024-07-31	7.1	High
CVE-2023-42959	Apple	A race condition was addressed with improved state handling. This issue is fixed in macOS Sonoma 14. An app may be able to execute arbitrary code with kernel privileges.	2024-07-29	7	High
CVE-2024-42162	Linux	In the Linux kernel, the following vulnerability has been resolved: gve: Account for stopped queues when reading NIC stats We now account for the fact that the NIC might send us stats for a subset of queues. Without this change, gve_get_ethtool_stats might make an invalid access on the priv->stats_report->stats array.	2024-07-30	7	High
CVE-2024-42228	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Using uninitialized value *size when calling amdgpu_vce_cs_reloc Initialize the size before calling amdgpu_vce_cs_reloc, such as case 0x03000001. V2: To really improve the handling we would actually need to have a separate value of 0xffffffff.(Christian)	2024-07-30	7	High
CVE-2024-38878	Siemens	A vulnerability has been identified in Omnivise T3000 Application Server (All versions). Affected devices allow authenticated users to export diagnostics data. The corresponding API endpoint is susceptible to path traversal and could allow an authenticated attacker to download arbitrary files from the file system.	2024-08-02	6.9	Medium
CVE-2024-37129	Dell	Dell Inventory Collector, versions prior to 12.3.0.6 contains a Path Traversal vulnerability. A local authenticated malicious user could potentially exploit this vulnerability, leading to arbitrary code execution on the system.	2024-07-31	6.7	Medium
CVE-2023-40396	Apple	The issue was addressed with improved memory handling. This issue is fixed in iOS 17 and iPadOS 17, macOS Sonoma 14, watchOS 10, tvOS 17. An app may be able to execute arbitrary code with kernel privileges.	2024-07-29	6.6	Medium
CVE-2024-38482	Dell	CloudLink, versions 7.1.x and 8.x, contain an Improper check or handling of Exceptional Conditions Vulnerability in Cluster Component. A highly privileged malicious user with remote access could potentially exploit this vulnerability, leading to execute unauthorized actions and retrieve sensitive information from the database.	2024-08-02	6.6	Medium
CVE-2024-27878	Apple	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.6. An app with root privileges may be able to execute arbitrary code with kernel privileges.	2024-07-29	6.5	Medium
CVE-2023-38001	IBM	IBM Aspera Orchestrator 4.0.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 260206.	2024-07-30	6.5	Medium
CVE-2024-27877	Apple	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.6, macOS Monterey 12.7.6, macOS Ventura 13.6.8. Processing a maliciously crafted file may lead to a denial-of-service or potentially disclose memory contents.	2024-07-29	6.1	Medium
CVE-2024-28972	Dell	Dell InsightIQ, Verion 5.0.0, contains a use of a broken or risky cryptographic algorithm vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to information disclosure.	2024-08-01	5.9	Medium
CVE-2024-41037	Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: Intel: hda: fix null deref on system suspend entry When system enters suspend with an active stream, SOF core calls hw_params_upon_resume(). On Intel platforms with HDA DMA used to manage the link DMA, this leads to call chain of hda_dsp_set_hw_params_upon_resume() -> hda_dsp_dais_suspend() -> hda_dai_suspend() -> hda_ipc4_post_trigger()	2024-07-29	5.5	Medium

		A bug is hit in hda_dai_suspend() as hda_link_dma_cleanup() is run first, which clears hext_stream->link_substream, and then hda_ipc4_post_trigger() is called with a NULL snd_pcm_substream pointer.			
CVE-2024-41038	Linux	In the Linux kernel, the following vulnerability has been resolved: firmware: cs_dsp: Prevent buffer overrun when processing V2 alg headers Check that all fields of a V2 algorithm header fit into the available firmware data buffer. The wmfw V2 format introduced variable-length strings in the algorithm block header. This means the overall header length is variable, and the position of most fields varies depending on the length of the string fields. Each field must be checked to ensure that it does not overflow the firmware data buffer. As this ia bugfix patch, the fixes avoid making any significant change to the existing code. This makes it easier to review and less likely to introduce new bugs.	2024-07-29	5.5	Medium
CVE-2024-41089	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau/dispnv04: fix null pointer dereference in nv17_tv_get_hd_modes In nv17_tv_get_hd_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a possible NULL pointer dereference on failure of drm_mode_duplicate(). The same applies to drm_cvt_mode(). Add a check to avoid null pointer dereference.	2024-07-29	5.5	Medium
CVE-2024-41093	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: avoid using null object of framebuffer Instead of using state->fb->obj[0] directly, get object from framebuffer by calling drm_gem_fb_get_obj() and return error code when object is null to avoid using null object of framebuffer.	2024-07-29	5.5	Medium
CVE-2024-41095	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau/dispnv04: fix null pointer dereference in nv17_tv_get_ld_modes In nv17_tv_get_ld_modes(), the return value of drm_mode_duplicate() is assigned to mode, which will lead to a possible NULL pointer dereference on failure of drm_mode_duplicate(). Add a check to avoid npd.	2024-07-29	5.5	Medium
CVE-2024-41098	Linux	In the Linux kernel, the following vulnerability has been resolved: ata: libata-core: Fix null pointer dereference on error If the ata_port_alloc() call in ata_host_alloc() fails, ata_host_release() will get called. However, the code in ata_host_release() tries to free ata_port struct members unconditionally, which can lead to the following: BUG: unable to handle page fault for address: 0000000000003990 PGD 0 P4D 0 Oops: Oops: 0000 [#1] PREEMPT SMP NOPTI CPU: 10 PID: 594 Comm: (udev-worker) Not tainted 6.10.0-rc5 #44 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-2.fc40 04/01/2014 RIP: 0010:ata_host_release.cold+0x2f/0x6e [libata] Code: e4 4d 63 f4 44 89 e2 48 c7 c6 90 ad 32 c0 48 c7 c7 d0 70 33 c0 49 83 c6 0e 41 RSP: 0018:ffffc90000ebb968 EFLAGS: 00010246 RAX: 0000000000000041 RBX: ffff88810fb52e78 RCX:	2024-07-29	5.5	Medium

		0000000000000000 RDX: 0000000000000000 RSI: ffff88813b3218c0 RDI: ffff88813b3218c0 RBP: ffff88810fb52e40 R08: 0000000000000000 R09: 6c65725f74736f68 R10: ffffc90000ebb738 R11: 73692033203a746e R12: 0000000000000004 R13: 0000000000000000 R14: 0000000000000011 R15: 0000000000000006 FS: 00007f6cc55b9980(0000) GS:ffff88813b300000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000003990 CR3: 00000001122a2000 CR4: 0000000000750ef0 PKRU: 55555554 Call Trace: <TASK> ? __die_body.cold+0x19/0x27 ? page_fault_oops+0x15a/0x2f0 ? exc_page_fault+0x7e/0x180 ? asm_exc_page_fault+0x26/0x30 ? ata_host_release.cold+0x2f/0x6e [libata] ? ata_host_release.cold+0x2f/0x6e [libata] release_nodes+0x35/0xb0 devres_release_group+0x113/0x140 ata_host_alloc+0xed/0x120 [libata] ata_host_alloc_pinfo+0x14/0xa0 [libata] ahci_init_one+0x6c9/0xd20 [ahci] Do not access ata_port struct members unconditionally.			
CVE-2024-42064	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Skip pipe if the pipe idx not set properly [why] Driver crashes when pipe idx not set properly [how] Add code to skip the pipe that idx not set properly	2024-07-29	5.5	Medium
CVE-2024-42065	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Add a NULL check in xe_ttm_stolen_mgr_init Add an explicit check to ensure that the mgr is not NULL.	2024-07-29	5.5	Medium
CVE-2024-42066	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Fix potential integer overflow in page size calculation Explicitly cast tbo->page_alignment to u64 before bit-shifting to prevent overflow when assigning to min_page_size.	2024-07-29	5.5	Medium
CVE-2024-42067	Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_rox() into account with bpf_jit_binary_lock_ro() set_memory_rox() can fail, leaving memory unprotected. Check return and bail out when bpf_jit_binary_lock_ro() returns an error.	2024-07-29	5.5	Medium
CVE-2024-42068	Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Take return from set_memory_ro() into account with bpf_prog_lock_ro() set_memory_ro() can fail, leaving memory unprotected. Check its return and take it into account as an error.	2024-07-29	5.5	Medium
CVE-2024-42069	Linux	In the Linux kernel, the following vulnerability has been resolved: net: mana: Fix possible double free in error handling path When auxiliary_device_add() returns error and then calls auxiliary_device_uninit(), callback function adev_release calls kfree(madev). We shouldn't call kfree(madev) again in the error handling path. Set 'madev' to NULL.	2024-07-29	5.5	Medium
CVE-2024-42070	Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fully validate NFT_DATA_VALUE on store to data registers	2024-07-29	5.5	Medium

		register store validation for NFT_DATA_VALUE is conditional, however, the datatype is always either NFT_DATA_VALUE or NFT_DATA_VERDICT. This only requires a new helper function to infer the register type from the set datatype so this conditional check can be removed. Otherwise, pointer to chain object can be leaked through the registers.			
CVE-2024-42071	Linux	In the Linux kernel, the following vulnerability has been resolved: ionic: use dev_consume_skb_any outside of napi If we're not in a NAPI softirq context, we need to be careful about how we call napi_consume_skb(), specifically we need to call it with budget==0 to signal to it that we're not in a safe context. This was found while running some configuration stress testing of traffic and a change queue config loop running, and this curious note popped out: [4371.402645] BUG: using smp_processor_id() in preemptible [00000000] code: ethtool/20545 [4371.402897] caller is napi_skb_cache_put+0x16/0x80 [4371.403120] CPU: 25 PID: 20545 Comm: ethtool Kdump: loaded Tainted: G OE 6.10.0-rc3-netnext+ #8 [4371.403302] Hardware name: HPE ProLiant DL360 Gen10/ProLiant DL360 Gen10, BIOS U32 01/23/2021 [4371.403460] Call Trace: [4371.403613] <TASK> [4371.403758] dump_stack_lvl+0x4f/0x70 [4371.403904] check_preemption_disabled+0xc1/0xe0 [4371.404051] napi_skb_cache_put+0x16/0x80 [4371.404199] ionic_tx_clean+0x18a/0x240 [ionic] [4371.404354] ionic_tx_cq_service+0xc4/0x200 [ionic] [4371.404505] ionic_tx_flush+0x15/0x70 [ionic] [4371.404653] ? ionic_lif_qcq_deinit.isra.23+0x5b/0x70 [ionic] [4371.404805] ionic_txrx_deinit+0x71/0x190 [ionic] [4371.404956] ionic_reconfigure_queues+0x5f5/0xff0 [ionic] [4371.405111] ionic_set_ringparam+0x2e8/0x3e0 [ionic] [4371.405265] ethnl_set_rings+0x1f1/0x300 [4371.405418] ethnl_default_set_doit+0xbb/0x160 [4371.405571] genl_family_rcv_msg_doit+0xff/0x130 [...] I found that ionic_tx_clean() calls napi_consume_skb() which calls napi_skb_cache_put(), but before that last call is the note /* Zero budget indicate non-NAPI context called us, like netpoll */ and DEBUG_NET_WARN_ON_ONCE(!in_softirq()); Those are pretty big hints that we're doing it wrong. We can pass a context hint down through the calls to let ionic_tx_clean() know what we're doing so it can call napi_consume_skb() correctly.	2024-07-29	5.5	Medium
CVE-2024-42073	Linux	In the Linux kernel, the following vulnerability has been resolved: mlxsw: spectrum_buffers: Fix memory corruptions on Spectrum-4 systems The following two shared buffer operations make use of the Shared Buffer Status Register (SBSR): # devlink sb occupancy snapshot pci/0000:01:00.0 # devlink sb occupancy clearmax pci/0000:01:00.0 The register has two masks of 256 bits to denote on which ingress / egress ports the register should operate on. Spectrum-4 has more than 256 ports, so the register was extended by cited commit with a new 'port_page' field. However, when filling the register's payload, the driver specifies the ports as absolute numbers and not relative to the first port of the	2024-07-29	5.5	Medium

		port page, resulting in memory corruptions [1]. Fix by specifying the ports relative to the first port of the port page. [1] BUG: KASAN: slab-use-after-free in mlxsw_sp_sb_occ_snapshot+0xb6d/0xbc0 Read of size 1 at addr ffff8881068cb00f by task devlink/1566 [...] Call Trace: <TASK> dump_stack_lvl+0xc6/0x120 print_report+0xce/0x670 kasan_report+0xd7/0x110 mlxsw_sp_sb_occ_snapshot+0xb6d/0xbc0 mlxsw_devlink_sb_occ_snapshot+0x75/0xb0 devlink_nl_sb_occ_snapshot_doit+0x1f9/0x2a0 genl_family_rcv_msg_doit+0x20c/0x300 genl_rcv_msg+0x567/0x800 netlink_rcv_skb+0x170/0x450 genl_rcv+0x2d/0x40 netlink_unicast+0x547/0x830 netlink_sendmsg+0x8d4/0xdb0 __sys_sendto+0x49b/0x510 __x64_sys_sendto+0xe5/0x1c0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f [...] Allocated by task 1: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 __kasan_kmalloc+0x8f/0xa0 copy_verifier_state+0xbc2/0xfb0 do_check_common+0x2c51/0xc7e0 bpf_check+0x5107/0x9960 bpf_prog_load+0xf0e/0x2690 __sys_bpf+0x1a61/0x49d0 __x64_sys_bpf+0x7d/0xc0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 1: kasan_save_stack+0x33/0x60 kasan_save_track+0x14/0x30 kasan_save_free_info+0x3b/0x60 poison_slab_object+0x109/0x170 __kasan_slab_free+0x14/0x30 kfree+0xca/0x2b0 free_verifier_state+0xce/0x270 do_check_common+0x4828/0xc7e0 bpf_check+0x5107/0x9960 bpf_prog_load+0xf0e/0x2690 __sys_bpf+0x1a61/0x49d0 __x64_sys_bpf+0x7d/0xc0 do_syscall_64+0xc1/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f			
CVE-2024-42074	Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: amd: acp: add a null check for chip_pdev structure When acp platform device creation is skipped, chip->chip_pdev value will remain NULL. Add NULL check for chip->chip_pdev structure in snd_acp_resume() function to avoid null pointer dereference.	2024-07-29	5.5	Medium
CVE-2024-42075	Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix remap of arena. The bpf arena logic didn't account for mremap operation. Add a refcnt for multiple mmap events to prevent use-after-free in arena_vm_close.	2024-07-29	5.5	Medium
CVE-2024-42076	Linux	In the Linux kernel, the following vulnerability has been resolved: net: can: j1939: Initialize unused data in j1939_send_one() syzbot reported kernel-infoleak in raw_recvmsg() [1]. j1939_send_one()	2024-07-29	5.5	Medium

		creates full frame including unused data, but it doesn't initialize it. This causes the kernel-infoleak issue. Fix this by initializing unused data. [1] BUG: KMSAN: kernel-infoleak in instrument_copy_to_user include/linux/instrumented.h:114 [inline] BUG: KMSAN: kernel-infoleak in copy_to_user_iter lib/iov_iter.c:24 [inline] BUG: KMSAN: kernel-infoleak in iterate_ubuf include/linux/iov_iter.h:29 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance2 include/linux/iov_iter.h:245 [inline] BUG: KMSAN: kernel-infoleak in iterate_and_advance include/linux/iov_iter.h:271 [inline] BUG: KMSAN: kernel-infoleak in _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 instrument_copy_to_user include/linux/instrumented.h:114 [inline] copy_to_user_iter lib/iov_iter.c:24 [inline] iterate_ubuf include/linux/iov_iter.h:29 [inline] iterate_and_advance2 include/linux/iov_iter.h:245 [inline] iterate_and_advance include/linux/iov_iter.h:271 [inline] _copy_to_iter+0x366/0x2520 lib/iov_iter.c:185 copy_to_iter include/linux/uio.h:196 [inline] memcpy_to_msg include/linux/skbuff.h:4113 [inline] raw_recvmsg+0x2b8/0x9e0 net/can/raw.c:1008 sock_recvmsg_nosec net/socket.c:1046 [inline] sock_recvmsg+0x2c4/0x340 net/socket.c:1068 ____sys_recvmsg+0x18a/0x620 net/socket.c:2803 ___sys_recvmsg+0x223/0x840 net/socket.c:2845 do_recvmmsg+0x4fc/0xfd0 net/socket.c:2939 __sys_recvmmsg net/socket.c:3018 [inline] __do_sys_recvmmsg net/socket.c:3041 [inline] __se_sys_recvmmsg net/socket.c:3034 [inline] __x64_sys_recvmmsg+0x397/0x490 net/socket.c:3034 x64_sys_call+0xf6c/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:300 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at: slab_post_alloc_hook mm/slub.c:3804 [inline] slab_alloc_node mm/slub.c:3845 [inline] kmem_cache_alloc_node+0x613/0xc50 mm/slub.c:3888 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:577 __alloc_skb+0x35b/0x7a0 net/core/skbuff.c:668 alloc_skb include/linux/skbuff.h:1313 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6504 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2795 sock_alloc_send_skb include/net/sock.h:1842 [inline] j1939_sk_alloc_skb net/can/j1939/socket.c:878 [inline] j1939_sk_send_loop net/can/j1939/socket.c:1142 [inline] j1939_sk_sendmsg+0xc0a/0x2730 net/can/j1939/socket.c:1277 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 ____sys_sendmsg+0x877/0xb60 net/socket.c:2584 ___sys_sendmsg+0x28d/0x3c0 net/socket.c:2638 __sys_sendmsg net/socket.c:2667 [inline] __do_sys_sendmsg net/socket.c:2676 [inline] __se_sys_sendmsg net/socket.c:2674 [inline] __x64_sys_sendmsg+0x307/0x4a0 net/socket.c:2674 x64_sys_call+0xc4b/0x3b50 arch/x86/include/generated/asm/syscalls_64.h:47 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcf/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Bytes 12-15 of 16 are uninitialized Memory access of size 16 starts at ffff888120969690 Data copied to user address 00000000200017c0 CPU: 1 PID: 5050 Comm: syz-executor198 Not tainted 6.9.0-rc5-syzkaller-00031-g71b1543c83d6 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024			
CVE-2024-42077	Linux	In the Linux kernel, the following vulnerability has been resolved: ocfs2: fix DIO failure due to insufficient transaction credits	2024-07-29	5.5	Medium

		The code in ocfs2_dio_end_io_write() estimates number of necessary transaction credits using ocfs2_calc_extend_credits(). This however does not take into account that the IO could be arbitrarily large and can contain arbitrary number of extents. Extent tree manipulations do often extend the current transaction but not in all of the cases. For example if we have only single block extents in the tree, ocfs2_mark_extent_written() will end up calling ocfs2_replace_extent_rec() all the time and we will never extend the current transaction and eventually exhaust all the transaction credits if the IO contains many single block extents. Once that happens a WARN_ON(jbd2_handle_buffer_credits(handle) <= 0) is triggered in jbd2_journal_dirty_metadata() and subsequently OCFS2 aborts in response to this error. This was actually triggered by one of our customers on a heavily fragmented OCFS2 filesystem. To fix the issue make sure the transaction always has enough credits for one extent insert before each call of ocfs2_mark_extent_written(). Heming Zhao said: ------ PANIC: "Kernel panic - not syncing: OCFS2: (device dm-1): panic forced after error" PID: xxx TASK: xxxx CPU: 5 COMMAND: "SubmitThread-CA" #0 machine_kexec at ffffffff8c069932 #1 __crash_kexec at ffffffff8c1338fa #2 panic at ffffffff8c1d69b9 #3 ocfs2_handle_error at ffffffffc0c86c0c [ocfs2] #4 __ocfs2_abort at ffffffffc0c88387 [ocfs2] #5 ocfs2_journal_dirty at ffffffffc0c51e98 [ocfs2] #6 ocfs2_split_extent at ffffffffc0c27ea3 [ocfs2] #7 ocfs2_change_extent_flag at ffffffffc0c28053 [ocfs2] #8 ocfs2_mark_extent_written at ffffffffc0c28347 [ocfs2] #9 ocfs2_dio_end_io_write at ffffffffc0c2bef9 [ocfs2] #10 ocfs2_dio_end_io at ffffffffc0c2c0f5 [ocfs2] #11 dio_complete at ffffffff8c2b9fa7 #12 do_blockdev_direct_IO at ffffffff8c2bc09f #13 ocfs2_direct_IO at ffffffffc0c2b653 [ocfs2] #14 generic_file_direct_write at ffffffff8c1dcf14 #15 __generic_file_write_iter at ffffffff8c1dd07b #16 ocfs2_file_write_iter at ffffffffc0c49f1f [ocfs2] #17 aio_write at ffffffff8c2cc72e #18 kmem_cache_alloc at ffffffff8c248dde #19 do_io_submit at ffffffff8c2ccada #20 do_syscall_64 at ffffffff8c004984 #21 entry_SYSCALL_64_after_hwframe at ffffffff8c8000ba			
CVE-2024-42078	Linux	In the Linux kernel, the following vulnerability has been resolved: nfsd: initialise nfsd_info.mutex early. nfsd_info.mutex can be dereferenced by svc_pool_stats_start() immediately after the new netns is created. Currently this can trigger an oops. Move the initialisation earlier before it can possibly be dereferenced.	2024-07-29	5.5	Medium
CVE-2024-42079	Linux	In the Linux kernel, the following vulnerability has been resolved: gfs2: Fix NULL pointer dereference in gfs2_log_flush In gfs2_jindex_free(), set sdp->sd_jdesc to NULL under the log flush lock to provide exclusion against gfs2_log_flush(). In gfs2_log_flush(), check if sdp->sd_jdesc is non-NULL before dereferencing it. Otherwise, we could run into a NULL pointer dereference when outstanding glock work races with an unmount	2024-07-29	5.5	Medium

		(glock_work_func -> run_queue -> do_xmote -> inode_go_sync -> gfs2_log_flush).			
CVE-2024-42080	Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/restrack: Fix potential invalid address access struct rdma_restrack_entry's kern_name was set to KBUILD_MODNAME in ib_create_cq(), while if the module exited but forgot del this rdma_restrack_entry, it would cause a invalid address access in rdma_restrack_clean() when print the owner of this rdma_restrack_entry. These code is used to help find one forgotten PD release in one of the ULPs. But it is not needed anymore, so delete them.	2024-07-29	5.5	Medium
CVE-2024-42081	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/xe_devcoredump: Check NULL before assignments Assign 'xe_devcoredump_snapshot *' and 'xe_device *' only if 'coredump' is not NULL. v2 - Fix commit messages. v3 - Define variables before code.(Ashutosh/Jose) v4 - Drop return check for coredump_to_xe. (Jose/Rodrigo) v5 - Modify misleading commit message. (Matt)	2024-07-29	5.5	Medium
CVE-2024-42082	Linux	In the Linux kernel, the following vulnerability has been resolved: xdp: Remove WARN() from __xdp_reg_mem_model() syzkaller reports a warning in __xdp_reg_mem_model(). The warning occurs only if __mem_id_init_hash_table() returns an error. It returns the error in two cases: 1. memory allocation fails; 2. rhashtable_init() fails when some fields of rhashtable_params struct are not initialized properly. The second case cannot happen since there is a static const rhashtable_params struct with valid fields. So, warning is only triggered when there is a problem with memory allocation. Thus, there is no sense in using WARN() to handle this error and it can be safely removed. WARNING: CPU: 0 PID: 5065 at net/core/xdp.c:299 __xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 CPU: 0 PID: 5065 Comm: syz-executor883 Not tainted 6.8.0-syzkaller-05271-gf99c5f563c17 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 03/27/2024 RIP: 0010:__xdp_reg_mem_model+0x2d9/0x650 net/core/xdp.c:299 Call Trace: xdp_reg_mem_model+0x22/0x40 net/core/xdp.c:344 xdp_test_run_setup net/bpf/test_run.c:188 [inline] bpf_test_run_xdp_live+0x365/0x1e90 net/bpf/test_run.c:377 bpf_prog_test_run_xdp+0x813/0x11b0 net/bpf/test_run.c:1267 bpf_prog_test_run+0x33a/0x3b0 kernel/bpf/syscall.c:4240 __sys_bpf+0x48d/0x810 kernel/bpf/syscall.c:5649 __do_sys_bpf kernel/bpf/syscall.c:5738 [inline] __se_sys_bpf kernel/bpf/syscall.c:5736 [inline] __x64_sys_bpf+0x7c/0x90 kernel/bpf/syscall.c:5736 do_syscall_64+0xfb/0x240 entry_SYSCALL_64_after_hwframe+0x6d/0x75	2024-07-29	5.5	Medium

		Found by Linux Verification Center (linuxtesting.org) with syzkaller.			
CVE-2024-42083	Linux	In the Linux kernel, the following vulnerability has been resolved: ionic: fix kernel panic due to multi-buffer handling Currently, the ionic_run_xdp() doesn't handle multi-buffer packets properly for XDP_TX and XDP_REDIRECT. When a jumbo frame is received, the ionic_run_xdp() first makes xdp frame with all necessary pages in the rx descriptor. And if the action is either XDP_TX or XDP_REDIRECT, it should unmap dma-mapping and reset page pointer to NULL for all pages, not only the first page. But it doesn't for SG pages. So, SG pages unexpectedly will be reused. It eventually causes kernel panic. Oops: general protection fault, probably for non-canonical address 0x504f4e4dbebc64ff: 0000 [#1] PREEMPT SMP NOPTI CPU: 3 PID: 0 Comm: swapper/3 Not tainted 6.10.0-rc3+ #25 RIP: 0010:xdp_return_frame+0x42/0x90 Code: 01 75 12 5b 4c 89 e6 5d 31 c9 41 5c 31 d2 41 5d e9 73 fd ff ff 44 8b 6b 20 0f b7 43 0a 49 81 ed 68 01 00 00 49 29 c5 49 01 fd <41> 80 7d0 RSP: 0018:ffff99d00122ce08 EFLAGS: 00010202 RAX: 0000000000005453 RBX: ffff8d325f904000 RCX: 0000000000000001 RDX: 00000000670e1000 RSI: 000000011f90d000 RDI: 504f4e4d4c4b4a49 RBP: ffff99d003907740 R08: 0000000000000000 R09: 0000000000000000 R10: 000000011f90d000 R11: 0000000000000000 R12: ffff8d325f904010 R13: 504f4e4dbebc64fd R14: ffff8d3242b070c8 R15: ffff99d0039077c0 FS: 0000000000000000(0000) GS:ffff8d399f780000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007f41f6c85e38 CR3: 000000037ac30000 CR4: 00000000007506f0 PKRU: 55555554 Call Trace: <IRQ> ? die_addr+0x33/0x90 ? exc_general_protection+0x251/0x2f0 ? asm_exc_general_protection+0x22/0x30 ? xdp_return_frame+0x42/0x90 ionic_tx_clean+0x211/0x280 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] ionic_tx_cq_service+0xd3/0x210 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] ionic_txrx_napi+0x41/0x1b0 [ionic 15881354510e6a9c655c59c54812b319ed2cd015] __napi_poll.constprop.0+0x29/0x1b0 net_rx_action+0x2c4/0x350 handle_softirqs+0xf4/0x320 irq_exit_rcu+0x78/0xa0 common_interrupt+0x77/0x90	2024-07-29	5.5	Medium
CVE-2024-42153	Linux	In the Linux kernel, the following vulnerability has been resolved: i2c: pnx: Fix potential deadlock warning from del_timer_sync() call in isr When del_timer_sync() is called in an interrupt context it throws a warning because of potential deadlock. The timer is used only to exit from wait_for_completion() after a timeout so replacing the call with wait_for_completion_timeout() allows to remove the problematic timer and its related functions altogether.	2024-07-30	5.5	Medium
CVE-2024-42223	Linux	In the Linux kernel, the following vulnerability has been resolved: media: dvb-frontends: tda10048: Fix integer overflow state->xtal_hz can be up to 16M, so it can overflow a 32 bit integer when multiplied by pll_mfactor.	2024-07-30	5.5	Medium

		Create a new 64 bit variable to hold the calculations.			
CVE-2024-42231	Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: zoned: fix calc_available_free_space() for zoned mode calc_available_free_space() returns the total size of metadata (or system) block groups, which can be allocated from unallocated disk space. The logic is wrong on zoned mode in two places. First, the calculation of data_chunk_size is wrong. We always allocate one zone as one chunk, and no partial allocation of a zone. So, we should use zone_size (= data_sinfo->chunk_size) as it is. Second, the result "avail" may not be zone aligned. Since we always allocate one zone as one chunk on zoned mode, returning non-zone size aligned bytes will result in less pressure on the async metadata reclaim process. This is serious for the nearly full state with a large zone size device. Allowing over-commit too much will result in less async reclaim work and end up in ENOSPC. We can align down to the zone size to avoid that.	2024-07-30	5.5	Medium
CVE-2023-26288	IBM	IBM Aspera Orchestrator 4.0.1 does not invalidate session after a password change which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 248477.	2024-07-30	5.5	Medium
CVE-2024-39379	Adobe	Acrobat for Edge versions 126.0.2592.81 and earlier are affected by an out-of-bounds read vulnerability that could lead to arbitrary file system read access. An attacker could exploit this vulnerability to read contents from a location in memory past the buffer boundary, potentially leading to sensitive information disclosure. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-07-31	5.5	Medium
CVE-2017-3772	Lenovo	A vulnerability was reported in Lenovo PC Manager versions prior to 2.6.40.3154 that could allow an attacker to cause a system reboot.	2024-07-31	5.5	Medium
CVE-2024-39396	Adobe	InDesign Desktop versions ID18.5.2, ID19.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-08-02	5.5	Medium
CVE-2023-26289	IBM	IBM Aspera Orchestrator 4.0.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking. IBM X-Force ID: 248478.	2024-07-30	5.4	Medium
CVE-2024-27862	Apple	A logic issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.6. Enabling Lockdown Mode while setting up a Mac may cause FileVault to become unexpectedly disabled.	2024-07-29	5.3	Medium
CVE-2024-7357	D-Link	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DIR-600 up to 2.18. It has been rated as critical. This issue affects the function soapcgi_main of the file /soap.cgi. The manipulation of the argument service leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273329 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	2024-08-01	5.3	Medium
CVE-2024-38321	IBM	IBM Business Automation Workflow 22.0.2, 23.0.1, 23.0.2, and 24.0.0 stores potentially sensitive information in log files under certain situations that could be read by an authenticated user. IBM X-Force ID: 284868.	2024-08-03	5.3	Medium
CVE-2024-7436	D-Link	A vulnerability, which was classified as critical, has been found in D-Link DI-8100 16.07. This issue affects the function msp_info_htm of the file msp_info.htm. The manipulation of the argument cmd leads to command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-273521 was assigned to this vulnerability.	2024-08-03	5.3	Medium

CVE-2024-42152	Linux	In the Linux kernel, the following vulnerability has been resolved: nvmet: fix a possible leak when destroy a ctrl during qp establishment In nvmet_sq_destroy we capture sq->ctrl early and if it is non-NULL we know that a ctrl was allocated (in the admin connect request handler) and we need to release pending AERs, clear ctrl->sqs and sq->ctrl (for nvme-loop primarily), and drop the final reference on the ctrl. However, a small window is possible where nvmet_sq_destroy starts (as a result of the client giving up and disconnecting) concurrently with the nvme admin connect cmd (which may be in an early stage). But *before* kill_and_confirm of sq->ref (i.e. the admin connect managed to get an sq live reference). In this case, sq->ctrl was allocated however after it was captured in a local variable in nvmet_sq_destroy. This prevented the final reference drop on the ctrl. Solve this by re-capturing the sq->ctrl after all inflight request has completed, where for sure sq->ctrl reference is final, and move forward based on that. This issue was observed in an environment with many hosts connecting multiple ctrls simoutanuosly, creating a delay in allocating a ctrl leading up to this race window.	2024-07-30	4.7	Medium
CVE-2024-42227	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix overlapping copy within dml_core_mode_programming [WHY] &mode_lib->mp.Watermark and &locals->Watermark are the same address. memcpy may lead to unexpected behavior. [HOW] memmove should be used.	2024-07-30	4.7	Medium
CVE-2024-5678	ManageEngine	Zohocorp ManageEngine Applications Manager versions 170900 and below are vulnerable to the authenticated admin-only SQL Injection in the Create Monitor feature.	2024-08-01	4.7	Medium
CVE-2024-42226	Linux	In the Linux kernel, the following vulnerability has been resolved: usb: xhci: prevent potential failure in handle_tx_event() for Transfer events without TRB Some transfer events don't always point to a TRB, and consequently don't have a endpoint ring. In these cases, function handle_tx_event() should not proceed, because if 'ep->skip' is set, the pointer to the endpoint ring is used. To prevent a potential failure and make the code logical, return after checking the completion code for a Transfer event without TRBs.	2024-07-30	4.6	Medium
CVE-2024-42230	Linux	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: Fix scv instruction crash with kexec kexec on pseries disables AIL (reloc_on_exc), required for scv instruction support, before other CPUs have been shut down. This means they can execute scv instructions after AIL is disabled, which causes an interrupt at an unexpected entry location that crashes the kernel. Change the kexec sequence to disable AIL after other CPUs have been brought down. As a refresher, the real-mode scv interrupt vector is 0x17000, and	2024-07-30	4.4	Medium

		the fixed-location head code probably couldn't easily deal with implementing such high addresses so it was just decided not to support that interrupt at all.			
CVE-2024-25947	Dell	Dell iDRAC Service Module version 5.3.0.0 and prior, contain an Out of bound Read Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event.	2024-08-01	4.4	Medium
CVE-2024-25948	Dell	Dell iDRAC Service Module version 5.3.0.0 and prior, contain a Out of bound Write Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event.	2024-08-01	4.4	Medium
CVE-2024-38481	Dell	Dell iDRAC Service Module version 5.3.0.0 and prior, contain a Out of bound Read Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event.	2024-08-01	4.4	Medium
CVE-2024-38489	Dell	Dell iDRAC Service Module version 5.3.0.0 and prior contains Out of bound write Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service (partial) event.	2024-08-01	4.4	Medium
CVE-2024-38490	Dell	Dell iDRAC Service Module version 5.3.0.0 and prior, contain a Out of bound Write Vulnerability. A privileged local attacker could execute arbitrary code potentially resulting in a denial of service event.	2024-08-01	4.4	Medium
CVE-2024-42156	Linux	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Wipe copies of clear-key structures on failure Wipe all sensitive data from stack for all IOCTLs, which convert a clear-key into a protected- or secure-key.	2024-07-30	4.1	Medium
CVE-2024-42157	Linux	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Wipe sensitive data on failure Wipe sensitive data from stack also if the copy_to_user() fails.	2024-07-30	4.1	Medium
CVE-2024-42158	Linux	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Use kfree_sensitive() to fix Coccinelle warnings Replace memzero_explicit() and kfree() with kfree_sensitive() to fix warnings reported by Coccinelle: WARNING opportunity for kfree_sensitive/kvfree_sensitive (line 1506) WARNING opportunity for kfree_sensitive/kvfree_sensitive (line 1643) WARNING opportunity for kfree_sensitive/kvfree_sensitive (line 1770)	2024-07-30	4.1	Medium
CVE-2024-42229	Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: aead,cipher - zeroize key buffer after use I.G 9.7.B for FIPS 140-3 specifies that variables temporarily holding cryptographic information should be zeroized once they are no longer needed. Accomplish this by using kfree_sensitive for buffers that previously held the private key.	2024-07-30	4.1	Medium
CVE-2022-33167	IBM	IBM Security Directory Integrator 7.2.0 and IBM Security Verify Directory Integrator 10.0.0 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie. IBM X-Force ID: 228587.	2024-07-30	3.7	Low
CVE-2024-40777	Apple	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in iOS 17.6 and iPadOS 17.6, watchOS 10.6, tvOS 17.6, visionOS 1.3, macOS Sonoma 14.6. Processing a maliciously crafted file may lead to unexpected app termination.	2024-07-29	3.3	Low
CVE-2024-37135	Dell	DM5500 5.16.0.0, contains an information disclosure vulnerability. A local attacker with high privileges could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	2024-07-31	3.3	Low
CVE-2024-42155	Linux	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Wipe copies of protected- and secure-keys	2024-07-30	1.9	Low

		Although the clear-key of neither protected- nor secure-keys is accessible, this key material should only be visible to the calling process. So wipe all copies of protected- or secure-keys from stack, even in case of an error.			

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى
مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.