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 15th of September to 21st of September. 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 ١٥ سبتمبر إلى ٢١ سبتمبر. 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-2024-8963	Ivanti	Path Traversal in the Ivanti CSA before 4.6 Patch 519 allows a remote unauthenticated attacker to access restricted functionality.	2024-09-19	9.1	Critical
CVE-2024-45696	D-Link	Certain models of D-Link wireless routers contain hidden functionality. By sending specific packets to the web service, the attacker can forcibly enable the telnet service and log in using hard-coded credentials. The telnet service enabled through this method can only be accessed from within the same local network as the device.	2024-09-16	8.8	High
CVE-2024-38183	Microsoft	An improper access control vulnerability in GroupMe allows an a unauthenticated attacker to elevate privileges over a network by convincing a user to click on a malicious link.	2024-09-17	8.8	High
CVE-2024-43460	Microsoft	Improper authorization in Dynamics 365 Business Central resulted in a vulnerability that allows an authenticated attacker to elevate privileges over a network.	2024-09-17	8.8	High
CVE-2024-8904	Google	Type Confusion in V8 in Google Chrome prior to 129.0.6668.58 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-09-17	8.8	High
CVE-2024-8905	Google	Inappropriate implementation in V8 in Google Chrome prior to 129.0.6668.58 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page. (Chromium security severity: Medium)	2024-09-17	8.8	High
CVE-2024-43489	Microsoft	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-09-19	8.8	High
CVE-2024-43496	Microsoft	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-09-19	8.8	High
CVE-2024-7254	Google	Any project that parses untrusted Protocol Buffers data containing an arbitrary number of nested groups / series of SGROUP tags can corrupted by exceeding the stack limit i.e. StackOverflow. Parsing nested groups as unknown fields with DiscardUnknownFieldsParser or Java Protobuf Lite parser, or against Protobuf map fields, creates unbounded recursions that can be abused by an attacker.	2024-09-19	8.7	High
CVE-2024-44132	Apple	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sequoia 15. An app may be able to break out of its sandbox.	2024-09-17	8.4	High
CVE-2024-27876	Apple	A race condition was addressed with improved locking. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, iOS 18 and iPadOS 18, macOS Sonoma 14.7, macOS Sequoia 15. Unpacking a maliciously crafted archive may allow an attacker to write arbitrary files.	2024-09-17	8.1	High
CVE-2024-44167	Apple	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.7, visionOS 2, iOS 18 and iPadOS 18, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to overwrite arbitrary files.	2024-09-17	8.1	High
CVE-2024-44169	Apple	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18,	2024-09-17	8.1	High

		macOS Sonoma 14.7, tvOS 18. An app may be able to cause unexpected system termination.			
CVE-2024-40841	Apple	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted video file may lead to unexpected app termination.	2024-09-17	7.8	High
CVE-2024-40861	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15. An app may be able to gain root privileges.	2024-09-17	7.8	High
CVE-2024-44160	Apple	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted texture may lead to unexpected app termination.	2024-09-17	7.8	High
CVE-2024-44162	Apple	This issue was addressed by enabling hardened runtime. This issue is fixed in Xcode 16. A malicious application may gain access to a user's Keychain items.	2024-09-17	7.8	High
CVE-2024-46725	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix out-of-bounds write warning Check the ring type value to fix the out-of-bounds write warning	2024-09-18	7.8	High
CVE-2024-46738	Linux	In the Linux kernel, the following vulnerability has been resolved: VMCI: Fix use-after-free when removing resource in vmci_resource_remove() When removing a resource from vmci_resource_table in vmci_resource_remove(), the search is performed using the resource handle by comparing context and resource fields. It is possible though to create two resources with different types but same handle (same context and resource fields). When trying to remove one of the resources, vmci_resource_remove() may not remove the intended one, but the object will still be freed as in the case of the datagram type in vmci_datagram_destroy_handle(). vmci_resource_table will still hold a pointer to this freed resource leading to a use-after-free vulnerability. BUG: KASAN: use-after-free in vmci_handle_is_equal include/linux/vmw_vmci_defs.h:142 [inline] BUG: KASAN: use-after-free in vmci_resource_remove+0x3a1/0x410 drivers/misc/vmw_vmci/vmci_resource.c:147 Read of size 4 at addr ffff88801c16d800 by task syz-executor197/1592 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0x82/0xa9 lib/dump_stack.c:106 print_address_description.constprop.0+0x21/0x366 mm/kasan/report.c:239 __kasan_report.cold+0x7f/0x132 mm/kasan/report.c:425 kasan_report+0x38/0x51 mm/kasan/report.c:442 vmci_handle_is_equal include/linux/vmw_vmci_defs.h:142 [inline] vmci_resource_remove+0x3a1/0x410 drivers/misc/vmw_vmci/vmci_resource.c:147 vmci_qp_broker_detach+0x89a/0x11b9 drivers/misc/vmw_vmci/vmci_queue_pair.c:2182 ctx_free_ctx+0x473/0xbe1 drivers/misc/vmw_vmci/vmci_context.c:444 kref_put include/linux/kref.h:65 [inline] vmci_ctx_put drivers/misc/vmw_vmci/vmci_context.c:497 [inline] vmci_ctx_destroy+0x170/0x1d6 drivers/misc/vmw_vmci/vmci_context.c:195 vmci_host_close+0x125/0x1ac drivers/misc/vmw_vmci/vmci_host.c:143 __fput+0x261/0xa34 fs/file_table.c:282 task_work_run+0xf0/0x194 kernel/task_work.c:164 tracehook_notify_resume include/linux/tracehook.h:189 [inline] exit_to_user_mode_loop+0x184/0x189 kernel/entry/common.c:187 exit_to_user_mode_prepare+0x11b/0x123 kernel/entry/common.c:220 __syscall_exit_to_user_mode_work kernel/entry/common.c:302 [inline]	2024-09-18	7.8	High

		syscall_exit_to_user_mode+0x18/0x42 kernel/entry/common.c:313 do_syscall_64+0x41/0x85 arch/x86/entry/common.c:86 entry_SYSCALL_64_after_hwframe+0x6e/0x0 This change ensures the type is also checked when removing the resource from vmci_resource_table in vmci_resource_remove().			
CVE-2024-46740	Linux	In the Linux kernel, the following vulnerability has been resolved: binder: fix UAF caused by offsets overwrite Binder objects are processed and copied individually into the target buffer during transactions. Any raw data in-between these objects is copied as well. However, this raw data copy lacks an out-of-bounds check. If the raw data exceeds the data section size then the copy overwrites the offsets section. This eventually triggers an error that attempts to unwind the processed objects. However, at this point the offsets used to index these objects are now corrupted. Unwinding with corrupted offsets can result in decrements of arbitrary nodes and lead to their premature release. Other users of such nodes are left with a dangling pointer triggering a use-after-free. This issue is made evident by the following KASAN report (trimmed): == BUG: KASAN: slab-use-after-free in _raw_spin_lock+0xe4/0x19c Write of size 4 at addr ffff47fc91598f04 by task binder-util/743 CPU: 9 UID: 0 PID: 743 Comm: binder-util Not tainted 6.11.0-rc4 #1 Hardware name: linux,dummy-virt (DT) Call trace: _raw_spin_lock+0xe4/0x19c binder_free_buf+0x128/0x434 binder_thread_write+0x8a4/0x3260 binder_ioctl+0x18f0/0x258c [...] Allocated by task 743: __kmalloc_cache_noprof+0x110/0x270 binder_new_node+0x50/0x700 binder_transaction+0x413c/0x6da8 binder_thread_write+0x978/0x3260 binder_ioctl+0x18f0/0x258c [...] Freed by task 745: kfree+0xbc/0x208 binder_thread_read+0x1c5c/0x37d4 binder_ioctl+0x16d8/0x258c [...] == To avoid this issue, let's check that the raw data copy is within the boundaries of the data section.	2024-09-18	7.8	High
CVE-2024-46741	Linux	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: Fix double free of 'buf' in error path smatch warning: drivers/misc/fastrpc.c:1926 fastrpc_req_mmap() error: double free of 'buf' In fastrpc_req_mmap() error path, the fastrpc buffer is freed in fastrpc_req_munmap_impl() if unmap is successful. But in the end, there is an unconditional call to fastrpc_buf_free(). So the above case triggers the double free of fastrpc buf.	2024-09-18	7.8	High

CVE-2024-46746	Linux	In the Linux kernel, the following vulnerability has been resolved: HID: amd_sfh: free driver_data after destroying hid device HID driver callbacks aren't called anymore once hid_destroy_device() has been called. Hence, hid driver_data should be freed only after the hid_destroy_device() function returned as driver_data is used in several callbacks. I observed a crash with kernel 6.10.0 on my T14s Gen 3, after enabling KASAN to debug memory allocation, I got this output: [13.050438] == [13.054060] BUG: KASAN: slab-use-after-free in amd_sfh_get_report+0x3ec/0x530 [amd_sfh] [13.054809] psmouse serio1: trackpoint: Synaptics TrackPoint firmware: 0x02, buttons: 3/3 [13.056432] Read of size 8 at addr ffff88813152f408 by task (udev-worker)/479 [13.060970] CPU: 5 PID: 479 Comm: (udev-worker) Not tainted 6.10.0-arch1-2 #1 893bb55d7f0073f25c46adbb49eb3785fefd74b0 [13.063978] Hardware name: LENOVO 21CQCTO1WW/21CQCTO1WW, BIOS R22ET70W (1.40) 03/21/2024 [13.067860] Call Trace: [13.069383] input: TPPS/2 Synaptics TrackPoint as /devices/platform/i8042/serio1/input/input8 [13.071486] <TASK> [13.071492] dump_stack_lvl+0x5d/0x80 [13.074870] snd_hda_intel 0000:33:00.6: enabling device (0000 -> 0002) [13.078296] ? amd_sfh_get_report+0x3ec/0x530 [amd_sfh 05f43221435b5205f734cd9da29399130f398a38] [13.082199] print_report+0x174/0x505 [13.085776] ? __pfx__raw_spin_lock_irqsave+0x10/0x10 [13.089367] ? srso_alias_return_thunk+0x5/0xfbef5 [13.093255] ? amd_sfh_get_report+0x3ec/0x530 [amd_sfh 05f43221435b5205f734cd9da29399130f398a38] [13.097464] kasan_report+0xc8/0x150 [13.101461] ? amd_sfh_get_report+0x3ec/0x530 [amd_sfh 05f43221435b5205f734cd9da29399130f398a38] [13.105802] amd_sfh_get_report+0x3ec/0x530 [amd_sfh 05f43221435b5205f734cd9da29399130f398a38] [13.110303] amdtp_hid_request+0xb8/0x110 [amd_sfh 05f43221435b5205f734cd9da29399130f398a38] [13.114879] ? srso_alias_return_thunk+0x5/0xfbef5 [13.119450] sensor_hub_get_feature+0x1d3/0x540 [hid_sensor_hub 3f13be3016ff415bea03008d45d99da837ee3082] [13.124097] hid_sensor_parse_common_attributes+0x4d0/0xad0 [hid_sensor_iio_common c3a5cbe93969c28b122609768bbe23efe52eb8f5] [13.127404] ? srso_alias_return_thunk+0x5/0xfbef5 [13.131925] ? __pfx_hid_sensor_parse_common_attributes+0x10/0x10 [hid_sensor_iio_common c3a5cbe93969c28b122609768bbe23efe52eb8f5] [13.136455] ? _raw_spin_lock_irqsave+0x96/0xf0 [13.140197] ? __pfx__raw_spin_lock_irqsave+0x10/0x10 [13.143602] ? devm_iio_device_alloc+0x34/0x50 [industrialio 3d261d5e5765625d2b052be40e526d62b1d2123b] [13.147234] ? srso_alias_return_thunk+0x5/0xfbef5 [13.150446] ? __devm_add_action+0x167/0x1d0 [13.155061] hid_gyro_3d_probe+0x120/0x7f0 [hid_sensor_gyro_3d 63da36a143b775846ab2dbb86c343b401b5e3172] [13.158581] ? srso_alias_return_thunk+0x5/0xfbef5 [13.161814] platform_probe+0xa2/0x150 [13.165029] really_probe+0x1e3/0x8a0 [13.168243] __driver_probe_device+0x18c/0x370 [13.171500] driver_probe_device+0x4a/0x120 [13.175000] __driver_attach+0x190/0x4a0 [13.178521] ? __pfx___driver_attach+0x10/0x10 [13.181771] bus_for_each_dev+0x106/0x180	2024-09-18	7.8	High

		[13.185033] ? __pfx__raw_spin_lock+0x10/0x10 [13.188229] ? __pfx_bus_for_each_dev+0x10/0x10 [13.191446] ? srso_alias_return_thunk+0x5/0xfbef5 [13.194382] bus_add_driver+0x29e/0x4d0 [13.197328] driver_register+0x1a5/0x360 [13.200283] ? __pfx_hid_gyro_3d_platform_driver_init+0x10/0x10 [hid_sensor_gyro_3d 63da36a143b775846ab2dbb86c343b401b5e3172] [13.203362] do_one_initcall+0xa7/0x380 [13.206432] ? __pfx_do_one_initcall+0x10/0x10 [13.210175] ? srso_alias_return_thunk+0x5/0xfbef5 [13.213211] ? kasan_unpoison+0x44/0x70 [13.216688] do_init_module+0x238/0x750 [13.2196 ---truncated---			
CVE-2024-46756	Linux	In the Linux kernel, the following vulnerability has been resolved: hwmon: (w83627ehf) Fix underflows seen when writing limit attributes DIV_ROUND_CLOSEST() after kstrtol() results in an underflow if a large negative number such as -9223372036854775808 is provided by the user. Fix it by reordering clamp_val() and DIV_ROUND_CLOSEST() operations.	2024-09-18	7.8	High
CVE-2024-46757	Linux	In the Linux kernel, the following vulnerability has been resolved: hwmon: (nct6775-core) Fix underflows seen when writing limit attributes DIV_ROUND_CLOSEST() after kstrtol() results in an underflow if a large negative number such as -9223372036854775808 is provided by the user. Fix it by reordering clamp_val() and DIV_ROUND_CLOSEST() operations.	2024-09-18	7.8	High
CVE-2024-46758	Linux	In the Linux kernel, the following vulnerability has been resolved: hwmon: (lm95234) Fix underflows seen when writing limit attributes DIV_ROUND_CLOSEST() after kstrtol() results in an underflow if a large negative number such as -9223372036854775808 is provided by the user. Fix it by reordering clamp_val() and DIV_ROUND_CLOSEST() operations.	2024-09-18	7.8	High
CVE-2024-46759	Linux	In the Linux kernel, the following vulnerability has been resolved: hwmon: (adc128d818) Fix underflows seen when writing limit attributes DIV_ROUND_CLOSEST() after kstrtol() results in an underflow if a large negative number such as -9223372036854775808 is provided by the user. Fix it by reordering clamp_val() and DIV_ROUND_CLOSEST() operations.	2024-09-18	7.8	High
CVE-2024-46766	Linux	In the Linux kernel, the following vulnerability has been resolved: ice: move netif_queue_set_napi to rtnl-protected sections Currently, netif_queue_set_napi() is called from ice_vsi_rebuild() that is not rtnl-locked when called from the reset. This creates the need to take the rtnl_lock just for a single function and complicates the synchronization with .ndo_bpf. At the same time, there no actual need to fill napi-to-queue information at this exact point. Fill napi-to-queue information when opening the VSI and clear it when the VSI is being closed. Those routines are already rtnl-locked. Also, rewrite napi-to-queue assignment in a way that prevents inclusion of XDP queues, as this leads to out-of-bounds writes, such as one	2024-09-18	7.8	High

		below. [+0.000004] BUG: KASAN: slab-out-of-bounds in netif_queue_set_napi+0x1c2/0x1e0 [+0.000012] Write of size 8 at addr ffff889881727c80 by task bash/7047 [+0.000006] CPU: 24 PID: 7047 Comm: bash Not tainted 6.10.0-rc2+ #2 [+0.000004] Hardware name: Intel Corporation S2600WFT/S2600WFT, BIOS SE5C620.86B.02.01.0014.082620210524 08/26/2021 [+0.000003] Call Trace: [+0.000003] <TASK> [+0.000002] dump_stack_lvl+0x60/0x80 [+0.000007] print_report+0xce/0x630 [+0.000007] ? __pfx__raw_spin_lock_irqsave+0x10/0x10 [+0.000007] ? __virt_addr_valid+0x1c9/0x2c0 [+0.000005] ? netif_queue_set_napi+0x1c2/0x1e0 [+0.000003] kasan_report+0xe9/0x120 [+0.000004] ? netif_queue_set_napi+0x1c2/0x1e0 [+0.000004] netif_queue_set_napi+0x1c2/0x1e0 [+0.000005] ice_vsi_close+0x161/0x670 [ice] [+0.000114] ice_dis_vsi+0x22f/0x270 [ice] [+0.000095] ice_pf_dis_all_vsi.constprop.0+0xae/0x1c0 [ice] [+0.000086] ice_prepare_for_reset+0x299/0x750 [ice] [+0.000087] pci_dev_save_and_disable+0x82/0xd0 [+0.000006] pci_reset_function+0x12d/0x230 [+0.000004] reset_store+0xa0/0x100 [+0.000006] ? __pfx_reset_store+0x10/0x10 [+0.000002] ? __pfx_mutex_lock+0x10/0x10 [+0.000004] ? __check_object_size+0x4c1/0x640 [+0.000007] kernfs_fop_write_iter+0x30b/0x4a0 [+0.000006] vfs_write+0x5d6/0xdf0 [+0.000005] ? fd_install+0x180/0x350 [+0.000005] ? __pfx_vfs_write+0x10/0xA10 [+0.000004] ? do_fcntl+0x52c/0xcd0 [+0.000004] ? kasan_save_track+0x13/0x60 [+0.000003] ? kasan_save_free_info+0x37/0x60 [+0.000006] ksys_write+0xfa/0x1d0 [+0.000003] ? __pfx_ksys_write+0x10/0x10 [+0.000002] ? __x64_sys_fcntl+0x121/0x180 [+0.000004] ? _raw_spin_lock+0x87/0xe0 [+0.000005] do_syscall_64+0x80/0x170 [+0.000007] ? _raw_spin_lock+0x87/0xe0 [+0.000004] ? __pfx__raw_spin_lock+0x10/0x10 [+0.000003] ? file_close_fd_locked+0x167/0x230 [+0.000005] ? syscall_exit_to_user_mode+0x7d/0x220 [+0.000005] ? do_syscall_64+0x8c/0x170 [+0.000004] ? do_syscall_64+0x8c/0x170 [+0.000003] ? do_syscall_64+0x8c/0x170 [+0.000003] ? fput+0x1a/0x2c0 [+0.000004] ? filp_close+0x19/0x30 [+0.000004] ? do_dup2+0x25a/0x4c0 [+0.000004] ? __x64_sys_dup2+0x6e/0x2e0 [+0.000002] ? syscall_exit_to_user_mode+0x7d/0x220 [+0.000004] ? do_syscall_64+0x8c/0x170 [+0.000003] ? __count_memcg_events+0x113/0x380 [+0.000005] ? handle_mm_fault+0x136/0x820 [+0.000005] ? do_user_addr_fault+0x444/0xa80 [+0.000004] ? clear_bhb_loop+0x25/0x80 [+0.000004] ? clear_bhb_loop+0x25/0x80 [+0.000002] entry_SYSCALL_64_after_hwframe+0x76/0x7e [+0.000005] RIP: 0033:0x7f2033593154			
CVE-2024-46782	Linux	In the Linux kernel, the following vulnerability has been resolved: ila: call nf_unregister_net_hooks() sooner syzbot found an use-after-free Read in ila_nf_input [1] Issue here is that ila_xlat_exit_net() frees the rhashtable, then call nf_unregister_net_hooks(). It should be done in the reverse way, with a synchronize_rcu(). This is a good match for a pre_exit() method. [1] BUG: KASAN: use-after-free in rht_key_hashfn include/linux/rhashtable.h:159 [inline] BUG: KASAN: use-after-free in __rhashtable_lookup	2024-09-18	7.8	High

<table>
<tr><td></td><td></td><td>include/linux/rhashtable.h:604 [inline]
 BUG: KASAN: use-after-free in rhashtable_lookup
include/linux/rhashtable.h:646 [inline]
 BUG: KASAN: use-after-free in
rhashtable_lookup_fast+0x77a/0x9b0
include/linux/rhashtable.h:672
Read of size 4 at addr ffff888064620008 by task ksoftirqd/0/16

CPU: 0 UID: 0 PID: 16 Comm: ksoftirqd/0 Not tainted 6.11.0-rc4-syzkaller-00238-g2ad6d23f465a #0
Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024
Call Trace:
 <TASK>
  __dump_stack lib/dump_stack.c:93 [inline]
  dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119
  print_address_description mm/kasan/report.c:377 [inline]
  print_report+0x169/0x550 mm/kasan/report.c:488
  kasan_report+0x143/0x180 mm/kasan/report.c:601
  rht_key_hashfn include/linux/rhashtable.h:159 [inline]
  __rhashtable_lookup include/linux/rhashtable.h:604 [inline]
  rhashtable_lookup include/linux/rhashtable.h:646 [inline]
  rhashtable_lookup_fast+0x77a/0x9b0
include/linux/rhashtable.h:672
  ila_lookup_wildcards net/ipv6/ila/ila_xlat.c:132 [inline]
  ila_xlat_addr net/ipv6/ila/ila_xlat.c:652 [inline]
  ila_nf_input+0x1fe/0x3c0 net/ipv6/ila/ila_xlat.c:190
  nf_hook_entry_hookfn include/linux/netfilter.h:154 [inline]
  nf_hook_slow+0xc3/0x220 net/netfilter/core.c:626
  nf_hook include/linux/netfilter.h:269 [inline]
  NF_HOOK+0x29e/0x450 include/linux/netfilter.h:312
  __netif_receive_skb_one_core net/core/dev.c:5661 [inline]
  __netif_receive_skb+0x1ea/0x650 net/core/dev.c:5775
  process_backlog+0x662/0x15b0 net/core/dev.c:6108
  __napi_poll+0xcb/0x490 net/core/dev.c:6772
  napi_poll net/core/dev.c:6841 [inline]
  net_rx_action+0x89b/0x1240 net/core/dev.c:6963
  handle_softirqs+0x2c4/0x970 kernel/softirq.c:554
  run_ksoftirqd+0xca/0x130 kernel/softirq.c:928
  smpboot_thread_fn+0x544/0xa30 kernel/smpboot.c:164
  kthread+0x2f0/0x390 kernel/kthread.c:389
  ret_from_fork+0x4b/0x80 arch/x86/kernel/process.c:147
  ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:244
 </TASK>

The buggy address belongs to the physical page:
page: refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x64620
flags: 0xfff00000000000(node=0|zone=1|lastcpupid=0x7ff)
page_type: 0xbfffffff(buddy)
raw: 00fff00000000000 ffffea0000959608 ffffea00019d9408 0000000000000000
raw: 0000000000000000 0000000000000003 00000000bfffffff 0000000000000000
page dumped because: kasan: bad access detected
page_owner tracks the page as freed
page last allocated via order 3, migratetype Unmovable, gfp_mask 0x52dc0(GFP_KERNEL|__GFP_NOWARN|__GFP_NORETRY|__GFP_COMP|__GFP_ZERO), pid 5242, tgid 5242 (syz-executor), ts 73611328570, free_ts 618981657187
  set_page_owner include/linux/page_owner.h:32 [inline]
  post_alloc_hook+0x1f3/0x230 mm/page_alloc.c:1493
  prep_new_page mm/page_alloc.c:1501 [inline]
  get_page_from_freelist+0x2e4c/0x2f10 mm/page_alloc.c:3439
  __alloc_pages_noprof+0x256/0x6c0 mm/page_alloc.c:4695
  __alloc_pages_node_noprof include/linux/gfp.h:269 [inline]
  alloc_pages_node_noprof include/linux/gfp.h:296 [inline]
  ___kmalloc_large_node+0x8b/0x1d0 mm/slub.c:4103
  __kmalloc_large_node_noprof+0x1a/0x80 mm/slub.c:4130
  __do_kmalloc_node mm/slub.c:4146 [inline]
  __kmalloc_node_noprof+0x2d2/0x440 mm/slub.c:4164
  __kvmalloc_node_noprof+0x72/0x190 mm/util.c:650
  bucket_table_alloc lib/rhashtable.c:186 [inline]
  rhashtable_init_noprof+0x534/0xa60 lib/rhashtable.c:1071
  ila_xlat_init_net+0xa0/0x110 net/ipv6/ila/ila_xlat.c:613
  ops_ini
---truncated---</td><td></td><td></td><td></td></tr>
<tr><td>CVE-2024-46786</td><td>Linux</td><td>In the Linux kernel, the following vulnerability has been resolved:

fscache: delete fscache_cookie_lru_timer when fscache exits to</td><td>2024-09-18</td><td>7.8</td><td>High</td></tr>
</table>

		avoid UAF The fscache_cookie_lru_timer is initialized when the fscache module is inserted, but is not deleted when the fscache module is removed. If timer_reduce() is called before removing the fscache module, the fscache_cookie_lru_timer will be added to the timer list of the current cpu. Afterwards, a use-after-free will be triggered in the softIRQ after removing the fscache module, as follows: == BUG: unable to handle page fault for address: fffffbfff803c9e9 PF: supervisor read access in kernel mode PF: error_code(0x0000) - not-present page PGD 21ffea067 P4D 21ffea067 PUD 21ffe6067 PMD 110a7c067 PTE 0 Oops: Oops: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 1 UID: 0 PID: 0 Comm: swapper/1 Tainted: G W 6.11.0-rc3 #855 Tainted: [W]=WARN RIP: 0010:__run_timer_base.part.0+0x254/0x8a0 Call Trace: <IRQ> tmigr_handle_remote_up+0x627/0x810 __walk_groups.isra.0+0x47/0x140 tmigr_handle_remote+0x1fa/0x2f0 handle_softirqs+0x180/0x590 irq_exit_rcu+0x84/0xb0 sysvec_apic_timer_interrupt+0x6e/0x90 </IRQ> <TASK> asm_sysvec_apic_timer_interrupt+0x1a/0x20 RIP: 0010:default_idle+0xf/0x20 default_idle_call+0x38/0x60 do_idle+0x2b5/0x300 cpu_startup_entry+0x54/0x60 start_secondary+0x20d/0x280 common_startup_64+0x13e/0x148 </TASK> Modules linked in: [last unloaded: netfs] == Therefore delete fscache_cookie_lru_timer when removing the fscahe module.			
CVE-2024-46796	Linux	In the Linux kernel, the following vulnerability has been resolved: smb: client: fix double put of @cfile in smb2_set_path_size() If smb2_compound_op() is called with a valid @cfile and returned -EINVAL, we need to call cifs_get_writable_path() before retrying it as the reference of @cfile was already dropped by previous call. This fixes the following KASAN splat when running fstests generic/013 against Windows Server 2022: CIFS: Attempting to mount //w22-fs0/scratch run fstests generic/013 at 2024-09-02 19:48:59 == BUG: KASAN: slab-use-after-free in detach_if_pending+0xab/0x200 Write of size 8 at addr ffff88811f1a3730 by task kworker/3:2/176 CPU: 3 UID: 0 PID: 176 Comm: kworker/3:2 Not tainted 6.11.0-rc6 #2 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 Workqueue: cifsoplockd cifs_oplock_break [cifs] Call Trace: <TASK> dump_stack_lvl+0x5d/0x80 ? detach_if_pending+0xab/0x200 print_report+0x156/0x4d9	2024-09-18	7.8	High

```
 ? detach_if_pending+0xab/0x200
 ? __virt_addr_valid+0x145/0x300
 ? __phys_addr+0x46/0x90
 ? detach_if_pending+0xab/0x200
 kasan_report+0xda/0x110
 ? detach_if_pending+0xab/0x200
 detach_if_pending+0xab/0x200
 timer_delete+0x96/0xe0
 ? __pfx_timer_delete+0x10/0x10
 ? rcu_is_watching+0x20/0x50
 try_to_grab_pending+0x46/0x3b0
 __cancel_work+0x89/0x1b0
 ? __pfx___cancel_work+0x10/0x10
 ? kasan_save_track+0x14/0x30
 cifs_close_deferred_file+0x110/0x2c0 [cifs]
 ? __pfx_cifs_close_deferred_file+0x10/0x10 [cifs]
 ? __pfx_down_read+0x10/0x10
 cifs_oplock_break+0x4c1/0xa50 [cifs]
 ? __pfx_cifs_oplock_break+0x10/0x10 [cifs]
 ? lock_is_held_type+0x85/0xf0
 ? mark_held_locks+0x1a/0x90
 process_one_work+0x4c6/0x9f0
 ? find_held_lock+0x8a/0xa0
 ? __pfx_process_one_work+0x10/0x10
 ? lock_acquired+0x220/0x550
 ? __list_add_valid_or_report+0x37/0x100
 worker_thread+0x2e4/0x570
 ? __kthread_parkme+0xd1/0xf0
 ? __pfx_worker_thread+0x10/0x10
 kthread+0x17f/0x1c0
 ? kthread+0xda/0x1c0
 ? __pfx_kthread+0x10/0x10
 ret_from_fork+0x31/0x60
 ? __pfx_kthread+0x10/0x10
 ret_from_fork_asm+0x1a/0x30
 </TASK>

Allocated by task 1118:
 kasan_save_stack+0x30/0x50
 kasan_save_track+0x14/0x30
 __kasan_kmalloc+0xaa/0xb0
 cifs_new_fileinfo+0xc8/0x9d0 [cifs]
 cifs_atomic_open+0x467/0x770 [cifs]
 lookup_open.isra.0+0x665/0x8b0
 path_openat+0x4c3/0x1380
 do_filp_open+0x167/0x270
 do_sys_openat2+0x129/0x160
 __x64_sys_creat+0xad/0xe0
 do_syscall_64+0xbb/0x1d0
 entry_SYSCALL_64_after_hwframe+0x77/0x7f

Freed by task 83:
 kasan_save_stack+0x30/0x50
 kasan_save_track+0x14/0x30
 kasan_save_free_info+0x3b/0x70
 poison_slab_object+0xe9/0x160
 __kasan_slab_free+0x32/0x50
 kfree+0xf2/0x300
 process_one_work+0x4c6/0x9f0
 worker_thread+0x2e4/0x570
 kthread+0x17f/0x1c0
 ret_from_fork+0x31/0x60
 ret_from_fork_asm+0x1a/0x30

Last potentially related work creation:
 kasan_save_stack+0x30/0x50
 __kasan_record_aux_stack+0xad/0xc0
 insert_work+0x29/0xe0
 __queue_work+0x5ea/0x760
 queue_work_on+0x6d/0x90
 _cifsFileInfo_put+0x3f6/0x770 [cifs]
 smb2_compound_op+0x911/0x3940 [cifs]
 smb2_set_path_size+0x228/0x270 [cifs]
 cifs_set_file_size+0x197/0x460 [cifs]
 cifs_setattr+0xd9c/0x14b0 [cifs]
 notify_change+0x4e3/0x740
 do_truncate+0xfa/0x180
 vfs_truncate+0x195/0x200
 __x64_sys_truncate+0x109/0x150
```

		do_syscall_64+0xbb/0x1d0 entry_SYSCALL_64_after_hwframe+0x77/0x7f			
CVE-2024-46798	Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: dapm: Fix UAF for snd_soc_pcm_runtime object When using kernel with the following extra config, - CONFIG_KASAN=y - CONFIG_KASAN_GENERIC=y - CONFIG_KASAN_INLINE=y - CONFIG_KASAN_VMALLOC=y - CONFIG_FRAME_WARN=4096 kernel detects that snd_pcm_suspend_all() access a freed 'snd_soc_pcm_runtime' object when the system is suspended, which leads to a use-after-free bug: [52.047746] BUG: KASAN: use-after-free in snd_pcm_suspend_all+0x1a8/0x270 [52.047765] Read of size 1 at addr ffff0000b9434d50 by task systemd-sleep/2330 [52.047785] Call trace: [52.047787] dump_backtrace+0x0/0x3c0 [52.047794] show_stack+0x34/0x50 [52.047797] dump_stack_lvl+0x68/0x8c [52.047802] print_address_description.constprop.0+0x74/0x2c0 [52.047809] kasan_report+0x210/0x230 [52.047815] __asan_report_load1_noabort+0x3c/0x50 [52.047820] snd_pcm_suspend_all+0x1a8/0x270 [52.047824] snd_soc_suspend+0x19c/0x4e0 The snd_pcm_sync_stop() has a NULL check on 'substream->runtime' before making any access. So we need to always set 'substream->runtime' to NULL everytime we kfree() it.	2024-09-18	7.8	High
CVE-2024-46800	Linux	In the Linux kernel, the following vulnerability has been resolved: sch/netem: fix use after free in netem_dequeue If netem_dequeue() enqueues packet to inner qdisc and that qdisc returns __NET_XMIT_STOLEN. The packet is dropped but qdisc_tree_reduce_backlog() is not called to update the parent's q.qlen, leading to the similar use-after-free as Commit e04991a48dbaf382 ("netem: fix return value if duplicate enqueue fails") Commands to trigger KASAN UaF: ip link add type dummy ip link set lo up ip link set dummy0 up tc qdisc add dev lo parent root handle 1: drr tc filter add dev lo parent 1: basic classid 1:1 tc class add dev lo classid 1:1 drr tc qdisc add dev lo parent 1:1 handle 2: netem tc qdisc add dev lo parent 2: handle 3: drr tc filter add dev lo parent 3: basic classid 3:1 action mirred egress redirect dev dummy0 tc class add dev lo classid 3:1 drr ping -c1 -W0.01 localhost # Trigger bug tc class del dev lo classid 1:1 tc class add dev lo classid 1:1 drr ping -c1 -W0.01 localhost # UaF	2024-09-18	7.8	High
CVE-2024-38016	Microsoft	Microsoft Office Visio Remote Code Execution Vulnerability	2024-09-19	7.8	High
CVE-2024-44147	Apple	This issue was addressed through improved state management. This issue is fixed in iOS 18 and iPadOS 18. An app may gain unauthorized access to Local Network.	2024-09-17	7.7	High
CVE-2024-27795	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. A camera extension may be able to access the internet.	2024-09-17	7.5	High
CVE-2024-27861	Apple	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15. An application may be able to read restricted memory.	2024-09-17	7.5	High
CVE-2024-27869	Apple	The issue was addressed with improved checks. This issue is fixed in iOS 18 and iPadOS 18, macOS Sequoia 15. An app may be able to record the screen without an indicator.	2024-09-17	7.5	High

CVE-2024-27874	Apple	This issue was addressed through improved state management. This issue is fixed in iOS 18 and iPadOS 18. A remote attacker may be able to cause a denial-of-service.	2024-09-17	7.5	High
CVE-2024-27879	Apple	The issue was addressed with improved bounds checks. This issue is fixed in iOS 17.7 and iPadOS 17.7, iOS 18 and iPadOS 18. An attacker may be able to cause unexpected app termination.	2024-09-17	7.5	High
CVE-2024-40770	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. A non-privileged user may be able to modify restricted network settings.	2024-09-17	7.5	High
CVE-2024-40848	Apple	A downgrade issue was addressed with additional code-signing restrictions. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An attacker may be able to read sensitive information.	2024-09-17	7.5	High
CVE-2024-40852	Apple	This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 18 and iPadOS 18. An attacker may be able to see recent photos without authentication in Assistive Access.	2024-09-17	7.5	High
CVE-2024-40856	Apple	An integrity issue was addressed with Beacon Protection. This issue is fixed in iOS 18 and iPadOS 18, tvOS 18, macOS Sequoia 15. An attacker may be able to force a device to disconnect from a secure network.	2024-09-17	7.5	High
CVE-2024-40862	Apple	A privacy issue was addressed by removing sensitive data. This issue is fixed in Xcode 16. An attacker may be able to determine the Apple ID of the owner of the computer.	2024-09-17	7.5	High
CVE-2024-44149	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access protected user data.	2024-09-17	7.5	High
CVE-2024-44152	Apple	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sequoia 15. An app may be able to access user-sensitive data.	2024-09-17	7.5	High
CVE-2024-44165	Apple	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, iOS 18 and iPadOS 18, macOS Sonoma 14.7, macOS Sequoia 15. Network traffic may leak outside a VPN tunnel.	2024-09-17	7.5	High
CVE-2024-44189	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15. A logic issue existed where a process may be able to capture screen contents without user consent.	2024-09-17	7.5	High
CVE-2024-45601	google	Mesop is a Python-based UI framework designed for rapid web apps development. A vulnerability has been discovered and fixed in Mesop that could potentially allow unauthorized access to files on the server hosting the Mesop application. The vulnerability was related to insufficient input validation in a specific endpoint. This could have allowed an attacker to access files not intended to be served. Users are strongly advised to update to the latest version of Mesop immediately. The latest version includes a fix for this vulnerability. At time of publication 0.12.4 is the most recently available version of Mesop.	2024-09-18	7.5	High
CVE-2024-44164	Apple	This issue was addressed with improved checks. This issue is fixed in iOS 17.7 and iPadOS 17.7, macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to bypass Privacy preferences.	2024-09-17	7.1	High
CVE-2024-46722	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix mc_data out-of-bounds read warning Clear warning that read mc_data[i-1] may out-of-bounds.	2024-09-18	7.1	High
CVE-2024-46723	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix ucode out-of-bounds read warning Clear warning that read ucode[] may out-of-bounds.	2024-09-18	7.1	High
CVE-2024-46724	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix out-of-bounds read of df_v1_7_channel_number Check the fb_channel_number range to avoid the array out-of-bounds read error	2024-09-18	7.1	High
CVE-2024-46731	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: fix the Out-of-bounds read warning using index i - 1U may beyond element index for mc_data[] when i = 0.	2024-09-18	7.1	High
CVE-2024-46743	Linux	In the Linux kernel, the following vulnerability has been resolved: of/irq: Prevent device address out-of-bounds read in interrupt map walk	2024-09-18	7.1	High

		When of_irq_parse_raw() is invoked with a device address smaller than the interrupt parent node (from #address-cells property), KASAN detects the following out-of-bounds read when populating the initial match table (dyndbg="func of_irq_parse_* +p"): OF: of_irq_parse_one: dev=/soc@0/picasso/watchdog, index=0 OF: parent=/soc@0/pci@878000000000/gpio0@17,0, intsize=2 OF: intspec=4 OF: of_irq_parse_raw: ipar=/soc@0/pci@878000000000/gpio0@17,0, size=2 OF: -> addrsize=3 == BUG: KASAN: slab-out-of-bounds in of_irq_parse_raw+0x2b8/0x8d0 Read of size 4 at addr ffffff81beca5608 by task bash/764 CPU: 1 PID: 764 Comm: bash Tainted: G O 6.1.67-484c613561-nokia_sm_arm64 #1 Hardware name: Unknown Unknown Product/Unknown Product, BIOS 2023.01-12.24.03-dirty 01/01/2023 Call trace: dump_backtrace+0xdc/0x130 show_stack+0x1c/0x30 dump_stack_lvl+0x6c/0x84 print_report+0x150/0x448 kasan_report+0x98/0x140 __asan_load4+0x78/0xa0 of_irq_parse_raw+0x2b8/0x8d0 of_irq_parse_one+0x24c/0x270 parse_interrupts+0xc0/0x120 of_fwnode_add_links+0x100/0x2d0 fw_devlink_parse_fwtree+0x64/0xc0 device_add+0xb38/0xc30 of_device_add+0x64/0x90 of_platform_device_create_pdata+0xd0/0x170 of_platform_bus_create+0x244/0x600 of_platform_notify+0x1b0/0x254 blocking_notifier_call_chain+0x9c/0xd0 __of_changeset_entry_notify+0x1b8/0x230 __of_changeset_apply_notify+0x54/0xe4 of_overlay_fdt_apply+0xc04/0xd94 ... The buggy address belongs to the object at ffffff81beca5600 which belongs to the cache kmalloc-128 of size 128 The buggy address is located 8 bytes inside of 128-byte region [ffffff81beca5600, ffffff81beca5680) The buggy address belongs to the physical page: page:00000000230d3d03 refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x1beca4 head:00000000230d3d03 order:1 compound_mapcount:0 compound_pincount:0 flags: 0x8000000000010200(slab|head|zone=2) raw: 8000000000010200 0000000000000000 dead000000000122 ffffff810000c300 raw: 0000000000000000 0000000000200020 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffffff81beca5500: 04 fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ffffff81beca5580: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc >ffffff81beca5600: 00 fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ^ ffffff81beca5680: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc ffffff81beca5700: 00 00 00 00 00 00 fc fc fc fc fc fc fc fc fc fc == OF: -> got it ! Prevent the out-of-bounds read by copying the device address into a buffer of sufficient size.			

CVE-2024-46747	Linux	In the Linux kernel, the following vulnerability has been resolved: HID: cougar: fix slab-out-of-bounds Read in cougar_report_fixup report_fixup for the Cougar 500k Gaming Keyboard was not verifying that the report descriptor size was correct before accessing it	2024-09-18	7.1	High
CVE-2024-38315	IBM	IBM Aspera Shares 1.0 through 1.10.0 PL3 does not invalidate session after a password reset which could allow an authenticated user to impersonate another user on the system.	2024-09-16	6.5	Medium
CVE-2024-40866	Apple	The issue was addressed with improved UI. This issue is fixed in Safari 18, macOS Sequoia 15. Visiting a malicious website may lead to address bar spoofing.	2024-09-17	6.5	Medium
CVE-2024-44124	Apple	This issue was addressed through improved state management. This issue is fixed in iOS 18 and iPadOS 18. A malicious Bluetooth input device may bypass pairing.	2024-09-17	6.5	Medium
CVE-2024-44187	Apple	A cross-origin issue existed with "iframe" elements. This was addressed with improved tracking of security origins. This issue is fixed in Safari 18, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, tvOS 18. A malicious website may exfiltrate data cross-origin.	2024-09-17	6.5	Medium
CVE-2024-40797	Apple	This issue was addressed through improved state management. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. Visiting a malicious website may lead to user interface spoofing.	2024-09-17	6.1	Medium
CVE-2024-40826	Apple	A privacy issue was addressed with improved handling of files. This issue is fixed in iOS 18 and iPadOS 18, macOS Sequoia 15. An unencrypted document may be written to a temporary file when using print preview.	2024-09-17	6.1	Medium
CVE-2024-40857	Apple	This issue was addressed through improved state management. This issue is fixed in Safari 18, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, tvOS 18. Processing maliciously crafted web content may lead to universal cross site scripting.	2024-09-17	6.1	Medium
CVE-2024-8897	Mozilla	Under certain conditions, an attacker with the ability to redirect users to a malicious site via an open redirect on a trusted site, may be able to spoof the address bar contents. This can lead to a malicious site to appear to have the same URL as the trusted site. *This bug only affects Firefox for Android. Other versions of Firefox are unaffected.* This vulnerability affects Firefox for Android < 130.0.1.	2024-09-17	6.1	Medium
CVE-2024-8907	Google	Insufficient data validation in Omnibox in Google Chrome on Android prior to 129.0.6668.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to inject arbitrary scripts or HTML (XSS) via a crafted set of UI gestures. (Chromium security severity: Medium)	2024-09-17	6.1	Medium
CVE-2024-40825	Apple	The issue was addressed with improved checks. This issue is fixed in visionOS 2, macOS Sequoia 15. A malicious app with root privileges may be able to modify the contents of system files.	2024-09-17	6	Medium
CVE-2024-37985	Microsoft	Windows Kernel Information Disclosure Vulnerability	2024-09-17	5.6	Medium
CVE-2024-23237	Apple	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15. An app may be able to cause a denial-of-service.	2024-09-17	5.5	Medium
CVE-2024-27858	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access protected user data.	2024-09-17	5.5	Medium
CVE-2024-27860	Apple	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15. An application may be able to read restricted memory.	2024-09-17	5.5	Medium
CVE-2024-27875	Apple	A logic issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15. Privacy Indicators for microphone or camera access may be attributed incorrectly.	2024-09-17	5.5	Medium
CVE-2024-27880	Apple	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in iOS 17.7 and iPadOS 17.7, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, macOS Sonoma 14.7, tvOS 18. Processing a maliciously crafted file may lead to unexpected app termination.	2024-09-17	5.5	Medium
CVE-2024-40790	Apple	The issue was addressed with improved handling of caches. This issue is fixed in visionOS 2. An app may be able to read sensitive data from the GPU memory.	2024-09-17	5.5	Medium
CVE-2024-40801	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access protected user data.	2024-09-17	5.5	Medium
CVE-2024-40831	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access a user's Photos Library.	2024-09-17	5.5	Medium
CVE-2024-40837	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access protected user data.	2024-09-17	5.5	Medium

CVE-2024-40842	Apple	An issue was addressed with improved validation of environment variables. This issue is fixed in macOS Sequoia 15. An app may be able to access user-sensitive data.	2024-09-17	5.5	Medium
CVE-2024-40843	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15. An app may be able to modify protected parts of the file system.	2024-09-17	5.5	Medium
CVE-2024-40844	Apple	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in iOS 17.7 and iPadOS 17.7, macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to observe data displayed to the user by Shortcuts.	2024-09-17	5.5	Medium
CVE-2024-40845	Apple	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted video file may lead to unexpected app termination.	2024-09-17	5.5	Medium
CVE-2024-40846	Apple	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted video file may lead to unexpected app termination.	2024-09-17	5.5	Medium
CVE-2024-40847	Apple	The issue was addressed with additional code-signing restrictions. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access sensitive user data.	2024-09-17	5.5	Medium
CVE-2024-40850	Apple	A file access issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, macOS Sonoma 14.7, tvOS 18. An app may be able to access user-sensitive data.	2024-09-17	5.5	Medium
CVE-2024-40859	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access user-sensitive data.	2024-09-17	5.5	Medium
CVE-2024-40860	Apple	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to modify protected parts of the file system.	2024-09-17	5.5	Medium
CVE-2024-40863	Apple	This issue was addressed with improved data protection. This issue is fixed in iOS 18 and iPadOS 18. An app may be able to leak sensitive user information.	2024-09-17	5.5	Medium
CVE-2024-44125	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. A malicious application may be able to leak sensitive user information.	2024-09-17	5.5	Medium
CVE-2024-44128	Apple	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An Automator Quick Action workflow may be able to bypass Gatekeeper.	2024-09-17	5.5	Medium
CVE-2024-44129	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7, macOS Sequoia 15. An app may be able to leak sensitive user information.	2024-09-17	5.5	Medium
CVE-2024-44131	Apple	This issue was addressed with improved validation of symlinks. This issue is fixed in iOS 18 and iPadOS 18, macOS Sequoia 15. An app may be able to access sensitive user data.	2024-09-17	5.5	Medium
CVE-2024-44133	Apple	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15. On MDM managed devices, an app may be able to bypass certain Privacy preferences.	2024-09-17	5.5	Medium
CVE-2024-44134	Apple	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sequoia 15. An app may be able to read sensitive location information.	2024-09-17	5.5	Medium
CVE-2024-44135	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access protected files within an App Sandbox container.	2024-09-17	5.5	Medium
CVE-2024-44151	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to modify protected parts of the file system.	2024-09-17	5.5	Medium
CVE-2024-44153	Apple	The issue was addressed with improved permissions logic. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access user-sensitive data.	2024-09-17	5.5	Medium
CVE-2024-44154	Apple	A memory initialization issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted file may lead to unexpected app termination.	2024-09-17	5.5	Medium
CVE-2024-44158	Apple	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 17.7 and iPadOS 17.7, macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. A shortcut may output sensitive user data without consent.	2024-09-17	5.5	Medium
CVE-2024-44161	Apple	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. Processing a maliciously crafted texture may lead to unexpected app termination.	2024-09-17	5.5	Medium

CVE-2024-44163	Apple	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. A malicious application may be able to access private information.	2024-09-17	5.5	Medium
CVE-2024-44166	Apple	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access user-sensitive data.	2024-09-17	5.5	Medium
CVE-2024-44168	Apple	A library injection issue was addressed with additional restrictions. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to modify protected parts of the file system.	2024-09-17	5.5	Medium
CVE-2024-44176	Apple	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, macOS Sonoma 14.7, tvOS 18. Processing an image may lead to a denial-of-service.	2024-09-17	5.5	Medium
CVE-2024-44177	Apple	A privacy issue was addressed by removing sensitive data. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access user-sensitive data.	2024-09-17	5.5	Medium
CVE-2024-44178	Apple	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to modify protected parts of the file system.	2024-09-17	5.5	Medium
CVE-2024-44181	Apple	An issue was addressed with improved handling of temporary files. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to read sensitive location information.	2024-09-17	5.5	Medium
CVE-2024-44182	Apple	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access sensitive data logged when a shortcut fails to launch another app.	2024-09-17	5.5	Medium
CVE-2024-44183	Apple	A logic error was addressed with improved error handling. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, macOS Sonoma 14.7, tvOS 18. An app may be able to cause a denial-of-service.	2024-09-17	5.5	Medium
CVE-2024-44184	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, iOS 18 and iPadOS 18, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access user-sensitive data.	2024-09-17	5.5	Medium
CVE-2024-44186	Apple	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access protected user data.	2024-09-17	5.5	Medium
CVE-2024-44188	Apple	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. An app may be able to access protected user data.	2024-09-17	5.5	Medium
CVE-2024-44190	Apple	A path handling issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.7, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to read arbitrary files.	2024-09-17	5.5	Medium
CVE-2024-44191	Apple	This issue was addressed through improved state management. This issue is fixed in iOS 17.7 and iPadOS 17.7, Xcode 16, visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, tvOS 18. An app may gain unauthorized access to Bluetooth.	2024-09-17	5.5	Medium
CVE-2024-44198	Apple	An integer overflow was addressed through improved input validation. This issue is fixed in visionOS 2, watchOS 11, macOS Sequoia 15, iOS 18 and iPadOS 18, tvOS 18. Processing maliciously crafted web content may lead to an unexpected process crash.	2024-09-17	5.5	Medium
CVE-2024-46719	Linux	In the Linux kernel, the following vulnerability has been resolved: usb: typec: ucsi: Fix null pointer dereference in trace ucsi_register_altmode checks IS_ERR for the alt pointer and treats NULL as valid. When CONFIG_TYPEC_DP_ALTMODE is not enabled, ucsi_register_displayport returns NULL which causes a NULL pointer dereference in trace. Rather than return NULL, call typec_port_register_altmode to register DisplayPort alternate mode as a non-controllable mode when CONFIG_TYPEC_DP_ALTMODE is not enabled.	2024-09-18	5.5	Medium
CVE-2024-46720	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix dereference after null check check the pointer hive before use.	2024-09-18	5.5	Medium
CVE-2024-46721	Linux	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix possible NULL pointer dereference	2024-09-18	5.5	Medium

		profile->parent->dents[AAFS_PROF_DIR] could be NULL only if its parent is made from __create_missing_ancestors(..) and 'ent->old' is NULL in aa_replace_profiles(..). In that case, it must return an error code and the code, -ENOENT represents its state that the path of its parent is not existed yet. BUG: kernel NULL pointer dereference, address: 0000000000000030 PGD 0 P4D 0 PREEMPT SMP PTI CPU: 4 PID: 3362 Comm: apparmor_parser Not tainted 6.8.0-24-generic #24 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.15.0-1 04/01/2014 RIP: 0010:aafs_create.constprop.0+0x7f/0x130 Code: 4c 63 e0 48 83 c4 18 4c 89 e0 5b 41 5c 41 5d 41 5e 41 5f 5d 31 d2 31 c9 31 f6 31 ff 45 31 c0 45 31 c9 45 31 d2 c3 cc cc cc cc <4d> 8b 55 30 4d 8d ba a0 00 00 00 4c 89 55 c0 4c 89 ff e8 7a 6a ae RSP: 0018:ffffc9000b2c7c98 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 00000000000041ed RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffc9000b2c7cd8 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffffffff82baac10 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 FS: 00007be9f22cf740(0000) GS:ffff88817bc00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000030 CR3: 0000000134b08000 CR4: 00000000000006f0 Call Trace: <TASK> ? show_regs+0x6d/0x80 ? __die+0x24/0x80 ? page_fault_oops+0x99/0x1b0 ? kernelmode_fixup_or_oops+0xb2/0x140 ? __bad_area_nosemaphore+0x1a5/0x2c0 ? find_vma+0x34/0x60 ? bad_area_nosemaphore+0x16/0x30 ? do_user_addr_fault+0x2a2/0x6b0 ? exc_page_fault+0x83/0x1b0 ? asm_exc_page_fault+0x27/0x30 ? aafs_create.constprop.0+0x7f/0x130 ? aafs_create.constprop.0+0x51/0x130 __aafs_profile_mkdir+0x3d6/0x480 aa_replace_profiles+0x83f/0x1270 policy_update+0xe3/0x180 profile_load+0xbc/0x150 ? rw_verify_area+0x47/0x140 vfs_write+0x100/0x480 ? __x64_sys_openat+0x55/0xa0 ? syscall_exit_to_user_mode+0x86/0x260 ksys_write+0x73/0x100 __x64_sys_write+0x19/0x30 x64_sys_call+0x7e/0x25c0 do_syscall_64+0x7f/0x180 entry_SYSCALL_64_after_hwframe+0x78/0x80 RIP: 0033:0x7be9f211c574 Code: c7 00 16 00 00 00 b8 ff ff ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 f3 0f 1e fa 80 3d d5 ea 0e 00 00 74 13 b8 01 00 00 00 0f 05 <48> 3d 00 f0 ff ff 77 54 c3 0f 1f 00 55 48 89 e5 48 83 ec 20 48 89 RSP: 002b:00007ffd26f2b8c8 EFLAGS: 00000202 ORIG_RAX: 0000000000000001 RAX: ffffffffffffffda RBX: 00005d504415e200 RCX: 00007be9f211c574 RDX: 0000000000001fc1 RSI: 00005d504418bc80 RDI: 0000000000000004 RBP: 0000000000001fc1 R08: 0000000000001fc1 R09: 0000000080000000 R10: 0000000000000000 R11: 0000000000000202 R12: 00005d504418bc80 R13: 0000000000000004 R14: 00007ffd26f2b9b0 R15: 00007ffd26f2ba30			

		</TASK> Modules linked in: snd_seq_dummy snd_hrtimer qrtr snd_hda_codec_generic snd_hda_intel snd_intel_dspcfg snd_intel_sdw_acpi snd_hda_codec snd_hda_core snd_hwdep snd_pcm snd_seq_midi snd_seq_midi_event snd_rawmidi snd_seq snd_seq_device i2c_i801 snd_timer i2c_smbus qxl snd soundcore drm_ttm_helper lpc_ich ttm joydev input_leds serio_raw mac_hid binfmt_misc msr parport_pc ppdev lp parport efi_pstore nfnetlink dmi_sysfs qemu_fw_cfg ip_tables x_tables autofs4 hid_generic usbhid hid ahci libahci psmouse virtio_rng xhci_pci xhci_pci_renesas CR2: 0000000000000030 ---[end trace 0000000000000000]--- RIP: 0010:aafs_create.constprop.0+0x7f/0x130 Code: 4c 63 e0 48 83 c4 18 4c 89 e0 5b 41 5c 41 5d 41 5e 41 5f 5d 31 d2 31 c9 31 f6 31 ff 45 31 c0 45 31 c9 45 31 d2 c3 cc cc cc cc <4d> 8b 55 30 4d 8d ba a0 00 00 00 4c 89 55 c0 4c 89 ff e8 7a 6a ae RSP: 0018:ffffc9000b2c7c98 EFLAGS: 00010246 RAX: 0000000000000000 RBX: 00000000000041ed RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffffc9000b2c7cd8 R08: 0000000000000000 R09: 0000000000000000 R10: 0000 ---truncated---			
CVE-2024-46726	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Ensure index calculation will not overflow [WHY & HOW] Make sure vmid0p72_idx, vnom0p8_idx and vmax0p9_idx calculation will never overflow and exceess array size. This fixes 3 OVERRUN and 1 INTEGER_OVERFLOW issues reported by Coverity.	2024-09-18	5.5	Medium
CVE-2024-46728	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check index for aux_rd_interval before using aux_rd_interval has size of 7 and should be checked. This fixes 3 OVERRUN and 1 INTEGER_OVERFLOW issues reported by Coverity.	2024-09-18	5.5	Medium
CVE-2024-46732	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Assign linear_pitch_alignment even for VM [Description] Assign linear_pitch_alignment so we don't cause a divide by 0 error in VM environments	2024-09-18	5.5	Medium
CVE-2024-46735	Linux	In the Linux kernel, the following vulnerability has been resolved: ublk_drv: fix NULL pointer dereference in ublk_ctrl_start_recovery() When two UBLK_CMD_START_USER_RECOVERY commands are submitted, the first one sets 'ubq->ubq_daemon' to NULL, and the second one triggers WARN in ublk_queue_reinit() and subsequently a NULL pointer dereference issue. Fix it by adding the check in ublk_ctrl_start_recovery() and return immediately in case of zero 'ub->nr_queues_ready'. BUG: kernel NULL pointer dereference, address: 0000000000000028 RIP: 0010:ublk_ctrl_start_recovery.constprop.0+0x82/0x180 Call Trace: <TASK> ? __die+0x20/0x70 ? page_fault_oops+0x75/0x170 ? exc_page_fault+0x64/0x140 ? asm_exc_page_fault+0x22/0x30 ? ublk_ctrl_start_recovery.constprop.0+0x82/0x180 ublk_ctrl_uring_cmd+0x4f7/0x6c0	2024-09-18	5.5	Medium

		? pick_next_task_idle+0x26/0x40 io_uring_cmd+0x9a/0x1b0 io_issue_sqe+0x193/0x3f0 io_wq_submit_work+0x9b/0x390 io_worker_handle_work+0x165/0x360 io_wq_worker+0xcb/0x2f0 ? finish_task_switch.isra.0+0x203/0x290 ? finish_task_switch.isra.0+0x203/0x290 ? __pfx_io_wq_worker+0x10/0x10 ret_from_fork+0x2d/0x50 ? __pfx_io_wq_worker+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK>			
CVE-2024-46737	Linux	In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: fix kernel crash if commands allocation fails If the commands allocation fails in nvmet_tcp_alloc_cmds() the kernel crashes in nvmet_tcp_release_queue_work() because of a NULL pointer dereference. nvmet: failed to install queue 0 cntlid 1 ret 6 Unable to handle kernel NULL pointer dereference at virtual address 0000000000000008 Fix the bug by setting queue->nr_cmds to zero in case nvmet_tcp_alloc_cmd() fails.	2024-09-18	5.5	Medium
CVE-2024-46739	Linux	In the Linux kernel, the following vulnerability has been resolved: uio_hv_generic: Fix kernel NULL pointer dereference in hv_uio_rescind For primary VM Bus channels, primary_channel pointer is always NULL. This pointer is valid only for the secondary channels. Also, rescind callback is meant for primary channels only. Fix NULL pointer dereference by retrieving the device_obj from the parent for the primary channel.	2024-09-18	5.5	Medium
CVE-2024-46742	Linux	In the Linux kernel, the following vulnerability has been resolved: smb/server: fix potential null-ptr-deref of lease_ctx_info in smb2_open() null-ptr-deref will occur when (req_op_level == SMB2_OPLOCK_LEVEL_LEASE) and parse_lease_state() return NULL. Fix this by check if 'lease_ctx_info' is NULL. Additionally, remove the redundant parentheses in parse_durable_handle_context().	2024-09-18	5.5	Medium
CVE-2024-46749	Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btnxpuart: Fix Null pointer dereference in btnxpuart_flush() This adds a check before freeing the rx->skb in flush and close functions to handle the kernel crash seen while removing driver after FW download fails or before FW download completes. dmesg log: [54.634586] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000080 [54.643398] Mem abort info: [54.646204] ESR = 0x0000000096000004 [54.649964] EC = 0x25: DABT (current EL), IL = 32 bits [54.655286] SET = 0, FnV = 0 [54.658348] EA = 0, S1PTW = 0 [54.661498] FSC = 0x04: level 0 translation fault [54.666391] Data abort info: [54.669273] ISV = 0, ISS = 0x00000004, ISS2 = 0x00000000 [54.674768] CM = 0, WnR = 0, TnD = 0, TagAccess = 0 [54.674771] GCS = 0, Overlay = 0, DirtyBit = 0, Xs = 0 [54.674775] user pgtable: 4k pages, 48-bit VAs, pgdp=0000000048860000	2024-09-18	5.5	Medium

		[54.674780] [0000000000000080] pgd=0000000000000000, p4d=0000000000000000 [54.703880] Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP [54.710152] Modules linked in: btnxpuart(-) overlay fsl_jr_uio caam_jr caamkeyblob_desc caamhash_desc caamalg_desc crypto_engine authenc libdes crct10dif_ce polyval_ce polyval_generic snd_soc_imx_spdif snd_soc_imx_card snd_soc_ak5558 snd_soc_ak4458 caam secvio error snd_soc_fsl_micfil snd_soc_fsl_spdif snd_soc_fsl_sai snd_soc_fsl_utils imx_pcm_dma gpio_ir_recv rc_core sch_fq_codel fuse [54.744357] CPU: 3 PID: 72 Comm: kworker/u9:0 Not tainted 6.6.3-otbr-g128004619037 #2 [54.744364] Hardware name: FSL i.MX8MM EVK board (DT) [54.744368] Workqueue: hci0 hci_power_on [54.757244] pstate: 60000005 (nZCv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) [54.757249] pc : kfree_skb_reason+0x18/0xb0 [54.772299] lr : btnxpuart_flush+0x40/0x58 [btnxpuart] [54.782921] sp : ffff8000805ebca0 [54.782923] x29: ffff8000805ebca0 x28: ffffa5c6cf1869c0 x27: ffffa5c6cf186000 [54.782931] x26: ffff377b84852400 x25: ffff377b848523c0 x24: ffff377b845e7230 [54.782938] x23: ffffa5c6ce8dbe08 x22: ffffa5c6ceb65410 x21: 00000000ffffff92 [54.782945] x20: ffffa5c6ce8dbe98 x19: ffffffffffffffac x18: ffffffffffffffff [54.807651] x17: 0000000000000000 x16: ffffa5c6ce2824ec x15: ffff8001005eb857 [54.821917] x14: 0000000000000000 x13: ffffa5c6cf1a02e0 x12: 0000000000000642 [54.821924] x11: 0000000000000040 x10: ffffa5c6cf19d690 x9 : ffffa5c6cf19d688 [54.821931] x8 : ffff377b86000028 x7 : 0000000000000000 x6 : 0000000000000000 [54.821938] x5 : ffff377b86000000 x4 : 0000000000000000 x3 : 0000000000000000 [54.843331] x2 : 0000000000000000 x1 : 0000000000000002 x0 : ffffffffffffffac [54.857599] Call trace: [54.857601] kfree_skb_reason+0x18/0xb0 [54.863878] btnxpuart_flush+0x40/0x58 [btnxpuart] [54.863888] hci_dev_open_sync+0x3a8/0xa04 [54.872773] hci_power_on+0x54/0x2e4 [54.881832] process_one_work+0x138/0x260 [54.881842] worker_thread+0x32c/0x438 [54.881847] kthread+0x118/0x11c [54.881853] ret_from_fork+0x10/0x20 [54.896406] Code: a9be7bfd 910003fd f9000bf3 aa0003f3 (b940d400) [54.896410] ---[end trace 0000000000000000]---			
CVE-2024-46755	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mwifiex: Do not return unused priv in mwifiex_get_priv_by_id() mwifiex_get_priv_by_id() returns the priv pointer corresponding to the bss_num and bss_type, but without checking if the priv is actually currently in use. Unused priv pointers do not have a wiphy attached to them which can lead to NULL pointer dereferences further down the callstack. Fix this by returning only used priv pointers which have priv->bss_mode set to something else than NL80211_IFTYPE_UNSPECIFIED. Said NULL pointer dereference happened when an Accesspoint was started with wpa_supplicant -i mlan0 with this config: network={ ssid="somessid" mode=2 frequency=2412 key_mgmt=WPA-PSK WPA-PSK-SHA256 proto=RSN	2024-09-18	5.5	Medium

		group=CCMP pairwise=CCMP psk="12345678" } When waiting for the AP to be established, interrupting wpa_supplicant with <ctrl-c> and starting it again this happens: | Unable to handle kernel NULL pointer dereference at virtual address 0000000000000140 | 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 | user pgtable: 4k pages, 48-bit VAs, pgdp=0000000046d96000 | [0000000000000140] pgd=0000000000000000, p4d=0000000000000000 | Internal error: Oops: 0000000096000004 [#1] PREEMPT SMP | Modules linked in: caam_jr caamhash_desc spidev caamalg_desc crypto_engine authenc libdes mwifiex_sdio +mwifiex crct10dif_ce cdc_acm onboard_usb_hub fsl_imx8_ddr_perf imx8m_ddrc rtc_ds1307 lm75 rtc_snvs +imx_sdma caam imx8mm_thermal spi_imx error imx_cpufreq_dt fuse ip_tables x_tables ipv6 | CPU: 0 PID: 8 Comm: kworker/0:1 Not tainted 6.9.0-00007-g937242013fce-dirty #18 | Hardware name: somemachine (DT) | Workqueue: events sdio_irq_work | pstate: 00000005 (nzcv daif -PAN -UAO -TCO -DIT -SSBS BTYPE=--) | pc : mwifiex_get_cfp+0xd8/0x15c [mwifiex] | lr : mwifiex_get_cfp+0x34/0x15c [mwifiex] | sp : ffff8000818b3a70 | x29: ffff8000818b3a70 x28: ffff000006bfd8a5 x27: 0000000000000004 | x26: 000000000000002c x25: 0000000000001511 x24: 0000000002e86bc9 | x23: ffff000006bfd996 x22: 0000000000000004 x21: ffff000007bec000 | x20: 000000000000002c x19: 0000000000000000 x18: 0000000000000000 | x17: 000000040044ffff x16: 00500072b5503510 x15: ccc283740681e517 | x14: 0201000101006d15 x13: 0000000002e8ff43 x12: 002c01000000ffb1 | x11: 0100000000000000 x10: 02e8ff43002c0100 x9 : 0000ffb100100157 | x8 : ffff000003d20000 x7 : 00000000000002f1 x6 : 00000000ffffe124 | x5 : 0000000000000001 x4 : 0000000000000003 x3 : 0000000000000000 | x2 : 0000000000000000 x1 : 0001000000011001 x0 : 0000000000000000 | Call trace: | mwifiex_get_cfp+0xd8/0x15c [mwifiex] | mwifiex_parse_single_response_buf+0x1d0/0x504 [mwifiex] | mwifiex_handle_event_ext_scan_report+0x19c/0x2f8 [mwifiex] | mwifiex_process_sta_event+0x298/0xf0c [mwifiex] | mwifiex_process_event+0x110/0x238 [mwifiex] | mwifiex_main_process+0x428/0xa44 [mwifiex] | mwifiex_sdio_interrupt+0x64/0x12c [mwifiex_sdio] | process_sdio_pending_irqs+0x64/0x1b8 | sdio_irq_work+0x4c/0x7c | process_one_work+0x148/0x2a0 | worker_thread+0x2fc/0x40c | kthread+0x110/0x114 | ret_from_fork+0x10/0x20 | Code: a94153f3 a8c37bfd d50323bf d65f03c0 (f940a000) | ---[end trace 0000000000000000]---			
CVE-2024-46760	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw88: usb: schedule rx work after everything is set up	2024-09-18	5.5	Medium

		Right now it's possible to hit NULL pointer dereference in rtw_rx_fill_rx_status on hw object and/or its fields because initialization routine can start getting USB replies before rtw_dev is fully setup. The stack trace looks like this: rtw_rx_fill_rx_status rtw8821c_query_rx_desc rtw_usb_rx_handler ... queue_work rtw_usb_read_port_complete ... usb_submit_urb rtw_usb_rx_resubmit rtw_usb_init_rx rtw_usb_probe So while we do the async stuff rtw_usb_probe continues and calls rtw_register_hw, which does all kinds of initialization (e.g. via ieee80211_register_hw) that rtw_rx_fill_rx_status relies on. Fix this by moving the first usb_submit_urb after everything is set up. For me, this bug manifested as: [8.893177] rtw_8821cu 1-1:1.2: band wrong, packet dropped [8.910904] rtw_8821cu 1-1:1.2: hw->conf.chandef.chan NULL in rtw_rx_fill_rx_status because I'm using Larry's backport of rtw88 driver with the NULL checks in rtw_rx_fill_rx_status.			
CVE-2024-46761	Linux	In the Linux kernel, the following vulnerability has been resolved: pci/hotplug/pnv_php: Fix hotplug driver crash on Powernv The hotplug driver for powerpc (pci/hotplug/pnv_php.c) causes a kernel crash when we try to hot-unplug/disable the PCIe switch/bridge from the PHB. The crash occurs because although the MSI data structure has been released during disable/hot-unplug path and it has been assigned with NULL, still during unregistration the code was again trying to explicitly disable the MSI which causes the NULL pointer dereference and kernel crash. The patch fixes the check during unregistration path to prevent invoking pci_disable_msi/msix() since its data structure is already freed.	2024-09-18	5.5	Medium
CVE-2024-46762	Linux	In the Linux kernel, the following vulnerability has been resolved: xen: privcmd: Fix possible access to a freed kirqfd instance Nothing prevents simultaneous ioctl calls to privcmd_irqfd_assign() and privcmd_irqfd_deassign(). If that happens, it is possible that a kirqfd created and added to the irqfds_list by privcmd_irqfd_assign() may get removed by another thread executing privcmd_irqfd_deassign(), while the former is still using it after dropping the locks. This can lead to a situation where an already freed kirqfd instance may be accessed and cause kernel oops. Use SRCU locking to prevent the same, as is done for the KVM implementation for irqfds.	2024-09-18	5.5	Medium
CVE-2024-46763	Linux	In the Linux kernel, the following vulnerability has been resolved: fou: Fix null-ptr-deref in GRO. We observed a null-ptr-deref in fou_gro_receive() while shutting down a host. [0]	2024-09-18	5.5	Medium

		The NULL pointer is sk->sk_user_data, and the offset 8 is of protocol in struct fou. When fou_release() is called due to netns dismantle or explicit tunnel teardown, udp_tunnel_sock_release() sets NULL to sk->sk_user_data. Then, the tunnel socket is destroyed after a single RCU grace period. So, in-flight udp4_gro_receive() could find the socket and execute the FOU GRO handler, where sk->sk_user_data could be NULL. Let's use rcu_dereference_sk_user_data() in fou_from_sock() and add NULL checks in FOU GRO handlers. [0]: BUG: kernel NULL pointer dereference, address: 0000000000000008 PF: supervisor read access in kernel mode PF: error_code(0x0000) - not-present page PGD 80000001032f4067 P4D 80000001032f4067 PUD 103240067 PMD 0 SMP PTI CPU: 0 PID: 0 Comm: swapper/0 Not tainted 5.10.216-204.855.amzn2.x86_64 #1 Hardware name: Amazon EC2 c5.large/, BIOS 1.0 10/16/2017 RIP: 0010:fou_gro_receive (net/ipv4/fou.c:233) [fou] Code: 41 5f c3 cc cc cc cc e8 e7 2e 69 f4 0f 1f 80 00 00 00 00 0f 1f 44 00 00 49 89 f8 41 54 48 89 f7 48 89 d6 49 8b 80 88 02 00 00 <0f> b6 48 08 0f b7 42 4a 66 25 fd fd 80 cc 02 66 89 42 4a 0f b6 42 RSP: 0018:ffffa330c0003d08 EFLAGS: 00010297 RAX: 0000000000000000 RBX: ffff93d9e3a6b900 RCX: 0000000000000010 RDX: ffff93d9e3a6b900 RSI: ffff93d9e3a6b900 RDI: ffff93dac2e24d08 RBP: ffff93d9e3a6b900 R08: ffff93dacbce6400 R09: 0000000000000002 R10: 0000000000000000 R11: ffffffffb5f369b0 R12: ffff93dacbce6400 R13: ffff93dac2e24d08 R14: 0000000000000000 R15: ffffffffb4edd1c0 FS: 0000000000000000(0000) GS:ffff93daee800000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000008 CR3: 0000000102140001 CR4: 00000000007706f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <IRQ> ? show_trace_log_lvl (arch/x86/kernel/dumpstack.c:259) ? __die_body.cold (arch/x86/kernel/dumpstack.c:478 arch/x86/kernel/dumpstack.c:420) ? no_context (arch/x86/mm/fault.c:752) ? exc_page_fault (arch/x86/include/asm/irqflags.h:49 arch/x86/include/asm/irqflags.h:89 arch/x86/mm/fault.c:1435 arch/x86/mm/fault.c:1483) ? asm_exc_page_fault (arch/x86/include/asm/idtentry.h:571) ? fou_gro_receive (net/ipv4/fou.c:233) [fou] udp_gro_receive (include/linux/netdevice.h:2552 net/ipv4/udp_offload.c:559) udp4_gro_receive (net/ipv4/udp_offload.c:604) inet_gro_receive (net/ipv4/af_inet.c:1549 (discriminator 7)) dev_gro_receive (net/core/dev.c:6035 (discriminator 4)) napi_gro_receive (net/core/dev.c:6170) ena_clean_rx_irq (drivers/amazon/net/ena/ena_netdev.c:1558) [ena] ena_io_poll (drivers/amazon/net/ena/ena_netdev.c:1742) [ena] napi_poll (net/core/dev.c:6847) net_rx_action (net/core/dev.c:6917) __do_softirq (arch/x86/include/asm/jump_label.h:25 include/linux/jump_label.h:200 include/trace/events/irq.h:142			

		kernel/softirq.c:299) asm_call_irq_on_stack (arch/x86/entry/entry_64.S:809) </IRQ> do_softirq_own_stack (arch/x86/include/asm/irq_stack.h:27 arch/x86/include/asm/irq_stack.h:77 arch/x86/kernel/irq_64.c:77) irq_exit_rcu (kernel/softirq.c:393 kernel/softirq.c:423 kernel/softirq.c:435) common_interrupt (arch/x86/kernel/irq.c:239) asm_common_interrupt (arch/x86/include/asm/idtentry.h:626) RIP: 0010:acpi_idle_do_entry (arch/x86/include/asm/irqflags.h:49 arch/x86/include/asm/irqflags.h:89 drivers/acpi/processor_idle.c:114 drivers/acpi/processor_idle.c:575) Code: 8b 15 d1 3c c4 02 ed c3 cc cc cc cc 65 48 8b 04 25 40 ef 01 00 48 8b 00 a8 08 75 eb 0f 1f 44 00 00 0f 00 2d d5 09 55 00 fb f4 <fa> c3 cc cc cc cc e9 be fc ff ff 66 66 2e 0f 1f 84 00 00 00 00 00 RSP: 0018:ffffffffb5603e58 EFLAGS: 00000246 RAX: 0000000000004000 RBX: ffff93dac0929c00 RCX: ffff93daee833900 RDX: ffff93daee800000 RSI: ffff93d ---truncated---			
CVE-2024-46765	Linux	In the Linux kernel, the following vulnerability has been resolved: ice: protect XDP configuration with a mutex The main threat to data consistency in ice_xdp() is a possible asynchronous PF reset. It can be triggered by a user or by TX timeout handler. XDP setup and PF reset code access the same resources in the following sections: * ice_vsi_close() in ice_prepare_for_reset() - already rtnl-locked * ice_vsi_rebuild() for the PF VSI - not protected * ice_vsi_open() - already rtnl-locked With an unfortunate timing, such accesses can result in a crash such as the one below: [+1.999878] ice 0000:b1:00.0: Registered XDP mem model MEM_TYPE_XSK_BUFF_POOL on Rx ring 14 [+2.002992] ice 0000:b1:00.0: Registered XDP mem model MEM_TYPE_XSK_BUFF_POOL on Rx ring 18 [Mar15 18:17] ice 0000:b1:00.0 ens801f0np0: NETDEV WATCHDOG: CPU: 38: transmit queue 14 timed out 80692736 ms [+0.000093] ice 0000:b1:00.0 ens801f0np0: tx_timeout: VSI_num: 6, Q 14, NTC: 0x0, HW_HEAD: 0x0, NTU: 0x0, INT: 0x4000001 [+0.000012] ice 0000:b1:00.0 ens801f0np0: tx_timeout recovery level 1, txqueue 14 [+0.394718] ice 0000:b1:00.0: PTP reset successful [+0.006184] BUG: kernel NULL pointer dereference, address: 0000000000000098 [+0.000045] #PF: supervisor read access in kernel mode [+0.000023] #PF: error_code(0x0000) - not-present page [+0.000023] PGD 0 P4D 0 [+0.000018] Oops: 0000 [#1] PREEMPT SMP NOPTI [+0.000023] CPU: 38 PID: 7540 Comm: kworker/38:1 Not tainted 6.8.0-rc7 #1 [+0.000031] Hardware name: Intel Corporation S2600WFT/S2600WFT, BIOS SE5C620.86B.02.01.0014.082620210524 08/26/2021 [+0.000036] Workqueue: ice ice_service_task [ice] [+0.000183] RIP: 0010:ice_clean_tx_ring+0xa/0xd0 [ice] [...] [+0.000013] Call Trace: [+0.000016] <TASK> [+0.000014] ? __die+0x1f/0x70 [+0.000029] ? page_fault_oops+0x171/0x4f0 [+0.000029] ? schedule+0x3b/0xd0 [+0.000027] ? exc_page_fault+0x7b/0x180 [+0.000022] ? asm_exc_page_fault+0x22/0x30 [+0.000031] ? ice_clean_tx_ring+0xa/0xd0 [ice] [+0.000194] ice_free_tx_ring+0xe/0x60 [ice] [+0.000186] ice_destroy_xdp_rings+0x157/0x310 [ice] [+0.000151] ice_vsi_decfg+0x53/0xe0 [ice] [+0.000180] ice_vsi_rebuild+0x239/0x540 [ice] [+0.000186] ice_vsi_rebuild_by_type+0x76/0x180 [ice] [+0.000145] ice_rebuild+0x18c/0x840 [ice] [+0.000145] ? delay_tsc+0x4a/0xc0	2024-09-18	5.5	Medium

		[+0.000022] ? delay_tsc+0x92/0xc0 [+0.000020] ice_do_reset+0x140/0x180 [ice] [+0.000886] ice_service_task+0x404/0x1030 [ice] [+0.000824] process_one_work+0x171/0x340 [+0.000685] worker_thread+0x277/0x3a0 [+0.000675] ? preempt_count_add+0x6a/0xa0 [+0.000677] ? _raw_spin_lock_irqsave+0x23/0x50 [+0.000679] ? __pfx_worker_thread+0x10/0x10 [+0.000653] kthread+0xf0/0x120 [+0.000635] ? __pfx_kthread+0x10/0x10 [+0.000616] ret_from_fork+0x2d/0x50 [+0.000612] ? __pfx_kthread+0x10/0x10 [+0.000604] ret_from_fork_asm+0x1b/0x30 [+0.000604] </TASK> The previous way of handling this through returning -EBUSY is not viable, particularly when destroying AF_XDP socket, because the kernel proceeds with removal anyway. There is plenty of code between those calls and there is no need to create a large critical section that covers all of them, same as there is no need to protect ice_vsi_rebuild() with rtnl_lock(). Add xdp_state_lock mutex to protect ice_vsi_rebuild() and ice_xdp(). Leaving unprotected sections in between would result in two states that have to be considered: 1. when the VSI is closed, but not yet rebuild 2. when VSI is already rebuild, but not yet open The latter case is actually already handled through !netif_running() case, we just need to adjust flag checking a little. The former one is not as trivial, because between ice_vsi_close() and ice_vsi_rebuild(), a lot of hardware interaction happens, this can make adding/deleting rings exit with an error. Luckily, VSI rebuild is pending and can apply new configuration for us in a managed fashion. Therefore, add an additional VSI state flag ICE_VSI_REBUILD_PENDING to indicate that ice_x ---truncated---			
CVE-2024-46770	Linux	In the Linux kernel, the following vulnerability has been resolved: ice: Add netif_device_attach/detach into PF reset flow Ethtool callbacks can be executed while reset is in progress and try to access deleted resources, e.g. getting coalesce settings can result in a NULL pointer dereference seen below. Reproduction steps: Once the driver is fully initialized, trigger reset: # echo 1 > /sys/class/net/<interface>/device/reset when reset is in progress try to get coalesce settings using ethtool: # ethtool -c <interface> BUG: kernel NULL pointer dereference, address: 0000000000000020 PGD 0 P4D 0 Oops: Oops: 0000 [#1] PREEMPT SMP PTI CPU: 11 PID: 19713 Comm: ethtool Tainted: G S 6.10.0-rc7+ #7 RIP: 0010:ice_get_q_coalesce+0x2e/0xa0 [ice] RSP: 0018:ffffbab1e9bcf6a8 EFLAGS: 00010206 RAX: 000000000000000c RBX: ffff94512305b028 RCX: 0000000000000000 RDX: 0000000000000000 RSI: ffff9451c3f2e588 RDI: ffff9451c3f2e588 RBP: 0000000000000000 R08: 0000000000000000 R09:	2024-09-18	5.5	Medium

		0000000000000000 R10: ffff9451c3f2e580 R11: 000000000000001f R12: ffff945121fa9000 R13: ffffbab1e9bcf760 R14: 0000000000000013 R15: ffffffff9e65dd40 FS: 00007faee5fbe740(0000) GS:ffff94546fd80000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000020 CR3: 0000000106c2e005 CR4: 00000000001706f0 Call Trace: <TASK> ice_get_coalesce+0x17/0x30 [ice] coalesce_prepare_data+0x61/0x80 ethnl_default_doit+0xde/0x340 genl_family_rcv_msg_doit+0xf2/0x150 genl_rcv_msg+0x1b3/0x2c0 netlink_rcv_skb+0x5b/0x110 genl_rcv+0x28/0x40 netlink_unicast+0x19c/0x290 netlink_sendmsg+0x222/0x490 __sys_sendto+0x1df/0x1f0 __x64_sys_sendto+0x24/0x30 do_syscall_64+0x82/0x160 entry_SYSCALL_64_after_hwframe+0x76/0x7e RIP: 0033:0x7faee60d8e27 Calling netif_device_detach() before reset makes the net core not call the driver when ethtool command is issued, the attempt to execute an ethtool command during reset will result in the following message: netlink error: No such device instead of NULL pointer dereference. Once reset is done and ice_rebuild() is executing, the netif_device_attach() is called to allow for ethtool operations to occur again in a safe manner.			
[CVE-2024-46772]()	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check denominator crb_pipes before used [WHAT & HOW] A denominator cannot be 0, and is checked before used. This fixes 2 DIVIDE_BY_ZERO issues reported by Coverity.	2024-09-18	5.5	Medium
[CVE-2024-46773]()	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check denominator pbn_div before used [WHAT & HOW] A denominator cannot be 0, and is checked before used. This fixes 1 DIVIDE_BY_ZERO issue reported by Coverity.	2024-09-18	5.5	Medium
[CVE-2024-46779]()	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/imagination: Free pvr_vm_gpuva after unlink This caused a measurable memory leak. Although the individual allocations are small, the leaks occurs in a high-usage codepath (remapping or unmapping device memory) so they add up quickly.	2024-09-18	5.5	Medium
[CVE-2024-46781]()	Linux	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix missing cleanup on rollforward recovery error In an error injection test of a routine for mount-time recovery, KASAN found a use-after-free bug. It turned out that if data recovery was performed using partial logs created by dsync writes, but an error occurred before starting the log writer to create a recovered checkpoint, the inodes whose data had been recovered were left in the ns_dirty_files list of the nilfs object and were not freed. Fix this issue by cleaning up inodes that have read the recovery	2024-09-18	5.5	Medium

		data if the recovery routine fails midway before the log writer starts.			
CVE-2024-46784	Linux	In the Linux kernel, the following vulnerability has been resolved: net: mana: Fix error handling in mana_create_txq/rxq's NAPI cleanup Currently napi_disable() gets called during rxq and txq cleanup, even before napi is enabled and hrtimer is initialized. It causes kernel panic. ? page_fault_oops+0x136/0x2b0 ? page_counter_cancel+0x2e/0x80 ? do_user_addr_fault+0x2f2/0x640 ? refill_obj_stock+0xc4/0x110 ? exc_page_fault+0x71/0x160 ? asm_exc_page_fault+0x27/0x30 ? __mmdrop+0x10/0x180 ? __mmdrop+0xec/0x180 ? hrtimer_active+0xd/0x50 hrtimer_try_to_cancel+0x2c/0xf0 hrtimer_cancel+0x15/0x30 napi_disable+0x65/0x90 mana_destroy_rxq+0x4c/0x2f0 mana_create_rxq.isra.0+0x56c/0x6d0 ? mana_uncfg_vport+0x50/0x50 mana_alloc_queues+0x21b/0x320 ? skb_dequeue+0x5f/0x80	2024-09-18	5.5	Medium
CVE-2024-46791	Linux	In the Linux kernel, the following vulnerability has been resolved: can: mcp251x: fix deadlock if an interrupt occurs during mcp251x_open The mcp251x_hw_wake() function is called with the mpc_lock mutex held and disables the interrupt handler so that no interrupts can be processed while waking the device. If an interrupt has already occurred then waiting for the interrupt handler to complete will deadlock because it will be trying to acquire the same mutex. CPU0 CPU1 ---- ---- mcp251x_open() mutex_lock(&priv->mcp_lock) request_threaded_irq() <interrupt> mcp251x_can_ist() mutex_lock(&priv->mcp_lock) mcp251x_hw_wake() disable_irq() <-- deadlock Use disable_irq_nosync() instead because the interrupt handler does everything while holding the mutex so it doesn't matter if it's still running.	2024-09-18	5.5	Medium

CVE-2024-46793	Linux	In the Linux kernel, the following vulnerability has been resolved:
		
		ASoC: Intel: Boards: Fix NULL pointer deref in BYT/CHT boards harder
		
		Since commit 13f58267cda3 ("ASoC: soc.h: don't create dummy Component
		via COMP_DUMMY()") dummy codecs declared like this:
		
		SND_SOC_DAILINK_DEF(dummy,
		DAILINK_COMP_ARRAY(COMP_DUMMY()));
		
		expand to:
		
		static struct snd_soc_dai_link_component dummy[] = {
		};
		
		Which means that dummy is a zero sized array and thus dais[i].codecs should
		not be dereferenced *at all* since it points to the address of the next
		variable stored in the data section as the "dummy" variable has an
			2024-09-18	5.5	Medium

		address but no size, so even dereferencing dais[0] is already an out of bounds array reference. Which means that the if (dais[i].codecs->name) check added in commit 7d99a70b6595 ("ASoC: Intel: Boards: Fix NULL pointer deref in BYT/CHT boards") relies on that the part of the next variable which the name member maps to just happens to be NULL. Which apparently so far it usually is, except when it isn't and then it results in crashes like this one: [28.795659] BUG: unable to handle page fault for address: 0000000000030011 ... [28.795780] Call Trace: [28.795787] <TASK> ... [28.795862] ? strcmp+0x18/0x40 [28.795872] 0xffffffffc150c605 [28.795887] platform_probe+0x40/0xa0 ... [28.795979] ? __pfx_init_module+0x10/0x10 [snd_soc_sst_bytcr_wm5102] Really fix things this time around by checking dais.num_codecs != 0.			
CVE-2024-46795	Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: unset the binding mark of a reused connection Steve French reported null pointer dereference error from sha256 lib. cifs.ko can send session setup requests on reused connection. If reused connection is used for binding session, conn->binding can still remain true and generate_preauth_hash() will not set sess->Preauth_HashValue and it will be NULL. It is used as a material to create an encryption key in ksmbd_gen_smb311_encryptionkey. ->Preauth_HashValue cause null pointer dereference error from crypto_shash_update(). BUG: kernel NULL pointer dereference, address: 0000000000000000 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP PTI CPU: 8 PID: 429254 Comm: kworker/8:39 Hardware name: LENOVO 20MAS08500/20MAS08500, BIOS N2CET69W (1.52) Workqueue: ksmbd-io handle_ksmbd_work [ksmbd] RIP: 0010:lib_sha256_base_do_update.isra.0+0x11e/0x1d0 [sha256_ssse3] <TASK> ? show_regs+0x6d/0x80 ? __die+0x24/0x80 ? page_fault_oops+0x99/0x1b0 ? do_user_addr_fault+0x2ee/0x6b0 ? exc_page_fault+0x83/0x1b0 ? asm_exc_page_fault+0x27/0x30 ? __pfx_sha256_transform_rorx+0x10/0x10 [sha256_ssse3] ? lib_sha256_base_do_update.isra.0+0x11e/0x1d0 [sha256_ssse3] ? __pfx_sha256_transform_rorx+0x10/0x10 [sha256_ssse3] ? __pfx_sha256_transform_rorx+0x10/0x10 [sha256_ssse3] _sha256_update+0x77/0xa0 [sha256_ssse3] sha256_avx2_update+0x15/0x30 [sha256_ssse3] crypto_shash_update+0x1e/0x40 hmac_update+0x12/0x20 crypto_shash_update+0x1e/0x40 generate_key+0x234/0x380 [ksmbd] generate_smb3encryptionkey+0x40/0x1c0 [ksmbd] ksmbd_gen_smb311_encryptionkey+0x72/0xa0 [ksmbd] ntlm_authenticate.isra.0+0x423/0x5d0 [ksmbd] smb2_sess_setup+0x952/0xaa0 [ksmbd] __process_request+0xa3/0x1d0 [ksmbd] __handle_ksmbd_work+0x1c4/0x2f0 [ksmbd]	2024-09-18	5.5	Medium

		handle_ksmbd_work+0x2d/0xa0 [ksmbd] process_one_work+0x16c/0x350 worker_thread+0x306/0x440 ? __pfx_worker_thread+0x10/0x10 kthread+0xef/0x120 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x44/0x70 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1b/0x30 </TASK>			
CVE-2024-46797	Linux	In the Linux kernel, the following vulnerability has been resolved: powerpc/qspinlock: Fix deadlock in MCS queue If an interrupt occurs in queued_spin_lock_slowpath() after we increment qnodesp->count and before node->lock is initialized, another CPU might see stale lock values in get_tail_qnode(). If the stale lock value happens to match the lock on that CPU, then we write to the "next" pointer of the wrong qnode. This causes a deadlock as the former CPU, once it becomes the head of the MCS queue, will spin indefinitely until it's "next" pointer is set by its successor in the queue. Running stress-ng on a 16 core (16EC/16VP) shared LPAR, results in occasional lockups similar to the following: $ stress-ng --all 128 --vm-bytes 80% --aggressive \\ --maximize --oomable --verify --syslog \\ --metrics --times --timeout 5m watchdog: CPU 15 Hard LOCKUP ...... NIP [c0000000000b78f4] queued_spin_lock_slowpath+0x1184/0x1490 LR [c000000001037c5c] _raw_spin_lock+0x6c/0x90 Call Trace: 0xc000002cfffa3bf0 (unreliable) _raw_spin_lock+0x6c/0x90 raw_spin_rq_lock_nested.part.135+0x4c/0xd0 sched_ttwu_pending+0x60/0x1f0 __flush_smp_call_function_queue+0x1dc/0x670 smp_ipi_demux_relaxed+0xa4/0x100 xive_muxed_ipi_action+0x20/0x40 __handle_irq_event_percpu+0x80/0x240 handle_irq_event_percpu+0x2c/0x80 handle_percpu_irq+0x84/0xd0 generic_handle_irq+0x54/0x80 __do_irq+0xac/0x210 __do_IRQ+0x74/0xd0 0x0 do_IRQ+0x8c/0x170 hardware_interrupt_common_virt+0x29c/0x2a0 --- interrupt: 500 at queued_spin_lock_slowpath+0x4b8/0x1490 ...... NIP [c0000000000b6c28] queued_spin_lock_slowpath+0x4b8/0x1490 LR [c000000001037c5c] _raw_spin_lock+0x6c/0x90 --- interrupt: 500 0xc0000029c1a41d00 (unreliable) _raw_spin_lock+0x6c/0x90 futex_wake+0x100/0x260 do_futex+0x21c/0x2a0 sys_futex+0x98/0x270 system_call_exception+0x14c/0x2f0 system_call_vectored_common+0x15c/0x2ec The following code flow illustrates how the deadlock occurs. For the sake of brevity, assume that both locks (A and B) are contended and we call the queued_spin_lock_slowpath() function. CPU0 CPU1 ---- ---- spin_lock_irqsave(A) | spin_unlock_irqrestore(A) |	2024-09-18	5.5	Medium

<table>
<tr><td></td><td></td><td>spin_lock(B) |
	 ?	 id = qnodesp->count++;	 (Note that nodes[0].lock == A)
	 ?	 Interrupt	 (happens before "nodes[0].lock = B")
	 ?	 spin_lock_irqsave(A)
	 ?	 id = qnodesp->count++	 nodes[1].lock = A
	 ?	 Tail of MCS queue
spin_lock_irqsave(A) ?	 Head of MCS queue ? 	CPU0 is previous tail ?	 Spin indefinitely ? (until "nodes[1].next != NULL") prev = get_tail_qnode(A, CPU0) 	 ? prev == &qnodes[CPU0].nodes[0] (as qnodes ---truncated---</td><td></td><td></td><td></td></tr>
<tr><td>CVE-2024-46799</td><td>Linux</td><td>In the Linux kernel, the following vulnerability has been resolved:

net: ethernet: ti: am65-cpsw: Fix NULL dereference on XDP_TX

If number of TX queues are set to 1 we get a NULL pointer dereference during XDP_TX.

~# ethtool -L eth0 tx 1
~# ./xdp-trafficgen udp -A <ipv6-src> -a <ipv6-dst> eth0 -t 2
Transmitting on eth0 (ifindex 2)
[241.135257] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000030

Fix this by using actual TX queues instead of max TX queues when picking the TX channel in am65_cpsw_ndo_xdp_xmit().</td><td>2024-09-18</td><td>5.5</td><td>Medium</td></tr>
<tr><td>CVE-2024-46801</td><td>Linux</td><td>In the Linux kernel, the following vulnerability has been resolved:

libfs: fix get_stashed_dentry()

get_stashed_dentry() tries to optimistically retrieve a stashed dentry
from a provided location. It needs to ensure to hold rcu lock before it
dereference the stashed location to prevent UAF issues. Use rcu_dereference() instead of READ_ONCE() it's effectively equivalent
with some lockdep bells and whistles and it communicates clearly that
this expects rcu protection.</td><td>2024-09-18</td><td>5.5</td><td>Medium</td></tr>
<tr><td>CVE-2024-44127</td><td>Apple</td><td>This issue was addressed through improved state management. This issue is fixed in iOS 17.7 and iPadOS 17.7, iOS 18 and iPadOS 18. Private Browsing tabs may be accessed without authentication.</td><td>2024-09-17</td><td>5.3</td><td>Medium</td></tr>
<tr><td>CVE-2024-44202</td><td>Apple</td><td>An authentication issue was addressed with improved state management. This issue is fixed in iOS 18 and iPadOS 18. Private Browsing tabs may be accessed without authentication.</td><td>2024-09-17</td><td>5.3</td><td>Medium</td></tr>
<tr><td>CVE-2024-9004</td><td>D-Link</td><td>A vulnerability classified as critical has been found in D-Link DAR-7000 up to 20240912. Affected is an unknown function of the file /view/DBManage/Backup_Server_commit.php. The manipulation of the argument host leads to os command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.</td><td>2024-09-19</td><td>5.3</td><td>Medium</td></tr>
<tr><td>CVE-2024-43188</td><td>IBM</td><td>IBM Business Automation Workflow

22.0.2, 23.0.1, 23.0.2, and 24.0.0

could allow a privileged user to perform unauthorized activities due to improper client side validation.</td><td>2024-09-18</td><td>4.9</td><td>Medium</td></tr>
</table>

CVE-2024-40840	Apple	This issue was addressed through improved state management. This issue is fixed in iOS 18 and iPadOS 18. An attacker with physical access may be able to use Siri to access sensitive user data.	2024-09-17	4.6	Medium
CVE-2024-44171	Apple	This issue was addressed through improved state management. This issue is fixed in iOS 17.7 and iPadOS 17.7, iOS 18 and iPadOS 18, watchOS 11. An attacker with physical access to a locked device may be able to Control Nearby Devices via accessibility features.	2024-09-17	4.6	Medium
CVE-2024-44130	Apple	This issue was addressed with improved data protection. This issue is fixed in macOS Sequoia 15. An app with root privileges may be able to access private information.	2024-09-17	4.4	Medium
CVE-2024-8906	Google	Incorrect security UI in Downloads in Google Chrome prior to 129.0.6668.58 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2024-09-17	4.3	Medium
CVE-2024-8908	Google	Inappropriate implementation in Autofill in Google Chrome prior to 129.0.6668.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2024-09-17	4.3	Medium
CVE-2024-8909	Google	Inappropriate implementation in UI in Google Chrome on iOS prior to 129.0.6668.58 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2024-09-17	4.3	Medium
CVE-2024-38221	Microsoft	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-09-19	4.3	Medium
CVE-2024-40791	Apple	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.7, iOS 17.7 and iPadOS 17.7, iOS 18 and iPadOS 18, macOS Sonoma 14.7, macOS Sequoia 15. An app may be able to access information about a user's contacts.	2024-09-17	3.3	Low
CVE-2024-40830	Apple	This issue was addressed with improved data protection. This issue is fixed in iOS 18 and iPadOS 18. An app may be able to enumerate a user's installed apps.	2024-09-17	3.3	Low
CVE-2024-40838	Apple	A privacy issue was addressed by moving sensitive data to a protected location. This issue is fixed in macOS Sequoia 15. A malicious app may be able to access notifications from the user's device.	2024-09-17	3.3	Low
CVE-2024-44139	Apple	The issue was addressed with improved checks. This issue is fixed in iOS 18 and iPadOS 18. An attacker with physical access may be able to access contacts from the lock screen.	2024-09-17	2.4	Low
CVE-2024-44180	Apple	The issue was addressed with improved checks. This issue is fixed in iOS 18 and iPadOS 18. An attacker with physical access may be able to access contacts from the lock screen.	2024-09-17	2.4	Low

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.