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 27th of October to 3rd of November. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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 ٢٧ أكتوبر إلى ٣ نوفمبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **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**

- **عالي جدًا: النتيجة الأساسية لـ CVSS 9.0-10.0**
- **عالي: النتيجة الأساسية لـ CVSS 7.0-8.9**
- **متوسط: النتيجة الأساسية لـ CVSS 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-2024-45656	ibm - Flexible Service Processor	IBM Flexible Service Processor (FSP) FW860.00 through FW860.B3, FW950.00 through FW950.C0, FW1030.00 through FW1030.61, FW1050.00 through FW1050.21, and FW1060.00 through FW1060.10 has static credentials which may allow network users to gain service privileges to the FSP.	2024-10-29	9.8	Critical
CVE-2024-51252	draytek - vigor3900 _firmware	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the restore function.	2024-11-01	9.8	Critical
CVE-2024-40867	apple - multiple products	A custom URL scheme handling issue was addressed with improved input validation. This issue is fixed in iOS 18.1 and iPadOS 18.1. A remote attacker may be able to break out of Web Content sandbox.	2024-10-28	9.6	Critical
CVE-2024-44256	apple - multiple products	The issue was addressed with improved input sanitization. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to break out of its sandbox.	2024-10-28	9.3	Critical
CVE-2024-44217	apple - iOS and iPadOS	A permissions issue was addressed by removing vulnerable code and adding additional checks. This issue is fixed in iOS 18 and iPadOS 18. Password	2024-10-28	9.1	Critical

		autofill may fill in passwords after failing authentication.			
CVE-2024-44122	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sequoia 15, macOS Sonoma 14.7.1. An application may be able to break out of its sandbox.	2024-10-28	8.8	High
CVE-2024-44259	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in iOS 17.7.1 and iPadOS 17.7.1, visionOS 2.1, iOS 18.1 and iPadOS 18.1, macOS Sequoia 15.1, Safari 18.1. An attacker may be able to misuse a trust relationship to download malicious content.	2024-10-28	8.8	High
CVE-2024-10467	mozilla - multiple products	Memory safety bugs present in Firefox 131, Firefox ESR 128.3, and Thunderbird 128.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	2024-10-29	8.8	High
CVE-2024-10487	google - Chrome	Out of bounds write in Dawn in Google Chrome prior to 130.0.6723.92 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Critical)	2024-10-29	8.8	High
CVE-2024-10488	google - Chrome	Use after free in WebRTC in Google Chrome prior to 130.0.6723.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-10-29	8.8	High
CVE-2024-51244	draytek - vigor3900 _firmware	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the doIPSec function.	2024-11-01	8.8	High
CVE-2024-51245	draytek - vigor3900 _firmware	In DrayTek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the rename_table function.	2024-11-01	8.8	High
CVE-2024-51247	draytek - vigor3900 _firmware	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the doPPPo function.	2024-11-01	8.8	High
CVE-2024-51248	draytek - vigor3900 _firmware	In Draytek Vigor3900 1.5.1.3, attackers can inject malicious commands into mainfunction.cgi and execute arbitrary commands by calling the modifyrow function.	2024-11-01	8.8	High
CVE-2024-44270	apple - multiple products	A logic issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A sandboxed process may be able to circumvent sandbox restrictions.	2024-10-28	8.6	High
CVE-2024-43383	apache software foundation - Apache	Deserialization of Untrusted Data vulnerability in Apache Lucene.Net.Replicator. This issue affects Apache Lucene.NET's Replicator library: from 4.8.0-beta00005 through 4.8.0-beta00016. An attacker that	2024-10-31	8	High

	Lucene.Net.Replicator	can intercept traffic between a replication client and server, or control the target replication node URL, can provide a specially-crafted JSON response that is deserialized as an attacker-provided exception type. This can result in remote code execution or other potential unauthorized access. Users are recommended to upgrade to version 4.8.0-beta00017, which fixes the issue.			
CVE-2024-50067	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: uprobe: avoid out-of-bounds memory access of fetching args Uprobe needs to fetch args into a percpu buffer, and then copy to ring buffer to avoid non-atomic context problem. Sometimes user-space strings, arrays can be very large, but the size of percpu buffer is only page size. And store_trace_args() won't check whether these data exceeds a single page or not, caused out-of-bounds memory access. It could be reproduced by following steps: 1. build kernel with CONFIG_KASAN enabled 2. save follow program as test.c ``` \#include <stdio.h> \#include <stdlib.h> \#include <string.h> // If string length large than MAX_STRING_SIZE, the fetch_store_strlen() // will return 0, cause __get_data_size() return shorter size, and // store_trace_args() will not trigger out-of-bounds access. // So make string length less than 4096. \#define STRLEN 4093 void generate_string(char *str, int n) { int i; for (i = 0; i < n; ++i) { char c = i % 26 + 'a'; str[i] = c; } str[n-1] = '\0'; } void print_string(char *str) { printf("%s\n", str); } int main() { char tmp[STRLEN];	2024-10-28	7.8	High

		generate_string(tmp, STRLEN); print_string(tmp); return 0; } ``` 3. compile program `gcc -o test test.c` 4. get the offset of `print_string()` ``` objdump -t test | grep -w print_string 0000000000401199 g F .text 000000000000001b print_string ``` 5. configure uprobe with offset 0x1199 ``` off=0x1199 cd /sys/kernel/debug/tracing/ echo "p /root/test:${off} arg1=+0(%di):ustring arg2=\$comm arg3=+0(%di):ustring" > uprobe_events echo 1 > events/uprobes/enable echo 1 > tracing_on ``` 6. run `test`, and kasan will report error. ========== BUG: KASAN: use-after-free in strncpy_from_user+0x1d6/0x1f0 Write of size 8 at addr ffff88812311c004 by task test/499CPU: 0 UID: 0 PID: 499 Comm: test Not tainted 6.12.0-rc3+ #18 Hardware name: Red Hat KVM, BIOS 1.16.0-4.al8 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0x55/0x70 print_address_description.constprop.0+0x27/0x310 kasan_report+0x10f/0x120 ? strncpy_from_user+0x1d6/0x1f0 strncpy_from_user+0x1d6/0x1f0 ? rmqueue.constprop.0+0x70d/0x2ad0 process_fetch_insn+0xb26/0x1470 ? __pfx_process_fetch_insn+0x10/0x10 ? _raw_spin_lock+0x85/0xe0 ? __pfx__raw_spin_lock+0x10/0x10 ? __pte_offset_map+0x1f/0x2d0 ? unwind_next_frame+0xc5f/0x1f80 ? arch_stack_walk+0x68/0xf0 ? is_bpf_text_address+0x23/0x30			

		? kernel_text_address.part.0+0xbb/0xd0 ? __kernel_text_address+0x66/0xb0 ? unwind_get_return_address+0x5e/0xa0 ? __pfx_stack_trace_consume_entry+0x10/0x10 ? arch_stack_walk+0xa2/0xf0 ? _raw_spin_lock_irqsave+0x8b/0xf0 ? __pfx__raw_spin_lock_irqsave+0x10/0x10 ? depot_alloc_stack+0x4c/0x1f0 ? _raw_spin_unlock_irqrestore+0xe/0x30 ? stack_depot_save_flags+0x35d/0x4f0 ? kasan_save_stack+0x34/0x50 ? kasan_save_stack+0x24/0x50 ? mutex_lock+0x91/0xe0 ? __pfx_mutex_lock+0x10/0x10 prepare_uprobe_buffer.part.0+0x2cd/0x500 uprobe_dispatcher+0x2c3/0x6a0 ? __pfx_uprobe_dispatcher+0x10/0x10 ? __kasan_slab_alloc+0x4d/0x90 handler_chain+0xdd/0x3e0 handle_swbp+0x26e/0x3d0 ? __pfx_handle_swbp+0x10/0x10 ? uprobe_pre_sstep_notifier+0x151/0x1b0 irqentry_exit_to_user_mode+0xe2/0x1b0 asm_exc_int3+0x39/0x40 RIP: 0033:0x401199 Code: 01 c2 0f b6 45 fb 88 02 83 45 fc 01 8b 45 fc 3b 45 e4 7c b7 8b 45 e4 48 98 48 8d 50 ff 48 8b 45 e8 48 01 d0 ce RSP: 002b:00007ffdf00576a8 EFLAGS: 00000206 RAX: 00007ffdf00576b0 RBX: 0000000000000000 RCX: 0000000000000ff2 RDX: 0000000000000ffc RSI: 0000000000000ffd RDI: 00007ffdf00576b0 RBP: 00007ffdf00586b0 R08: 00007feb2f9c0d20 R09: 00007feb2f9c0d20 R10: 0000000000000001 R11: 0000000000000202 R12: 0000000000401040 R13: 00007ffdf0058780 R14: 0000000000000000 R15: 0000000000000000 </TASK> This commit enforces the buffer's maxlen less than a page-size to avoid store_trace_args() out-of-memory access.			
CVE-2024-44126	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sequoia 15, iOS 17.7 and iPadOS 17.7, macOS Sonoma 14.7, visionOS 2, iOS 18 and iPadOS 18. Processing a maliciously crafted file may lead to heap corruption.	2024-10-28	7.8	High

CVE-2024-44218	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in iOS 17.7.1 and iPadOS 17.7.1, macOS Sonoma 14.7.1, iOS 18.1 and iPadOS 18.1. Processing a maliciously crafted file may lead to heap corruption.	2024-10-28	7.8	High
CVE-2024-44255	apple - multiple products	A path handling issue was addressed with improved logic. This issue is fixed in visionOS 2.1, iOS 18.1 and iPadOS 18.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, tvOS 18.1. A malicious app may be able to run arbitrary shortcuts without user consent.	2024-10-28	7.8	High
CVE-2024-44285	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 18.1 and iPadOS 18.1, watchOS 11.1, visionOS 2.1, tvOS 18.1. An app may be able to cause unexpected system termination or corrupt kernel memory.	2024-10-28	7.8	High
CVE-2024-50071	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: pinctrl: nuvoton: fix a double free in ma35_pinctrl_dt_node_to_map_func() 'new_map' is allocated using devm_* which takes care of freeing the allocated data on device removal, call to .dt_free_map = pinconf_generic_dt_free_map double frees the map as pinconf_generic_dt_free_map() calls pinctrl_utils_free_map(). Fix this by using kcalloc() instead of auto-managed devm_kcalloc().	2024-10-29	7.8	High
CVE-2024-50073	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: tty: n_gsm: Fix use-after-free in gsm_cleanup_mux BUG: KASAN: slab-use-after-free in gsm_cleanup_mux+0x77b/0x7b0 drivers/tty/n_gsm.c:3160 [n_gsm] Read of size 8 at addr ffff88815fe99c00 by task poc/3379 CPU: 0 UID: 0 PID: 3379 Comm: poc Not tainted 6.11.0+ #56 Hardware name: VMware, Inc. VMware Virtual Platform/440BX Desktop Reference Platform, BIOS 6.00 11/12/2020 Call Trace: <TASK> gsm_cleanup_mux+0x77b/0x7b0 drivers/tty/n_gsm.c:3160 [n_gsm] __pfx_gsm_cleanup_mux+0x10/0x10 drivers/tty/n_gsm.c:3124 [n_gsm] __pfx_sched_clock_cpu+0x10/0x10 kernel/sched/clock.c:389 update_load_avg+0x1c1/0x27b0 kernel/sched/fair.c:4500 __pfx_min_vruntime_cb_rotate+0x10/0x10 kernel/sched/fair.c:846 __rb_insert_augmented+0x492/0xbf0	2024-10-29	7.8	High

		lib/rbtree.c:161 gsmld_ioctl+0x395/0x1450 drivers/tty/n_gsm.c:3408 [n_gsm] _raw_spin_lock_irqsave+0x92/0xf0 arch/x86/include/asm/atomic.h:107 __pfx_gsmld_ioctl+0x10/0x10 drivers/tty/n_gsm.c:3822 [n_gsm] ktime_get+0x5e/0x140 kernel/time/timekeeping.c:195 ldsem_down_read+0x94/0x4e0 arch/x86/include/asm/atomic64_64.h:79 __pfx_ldsem_down_read+0x10/0x10 drivers/tty/tty_ldsem.c:338 __pfx_do_vfs_ioctl+0x10/0x10 fs/ioctl.c:805 tty_ioctl+0x643/0x1100 drivers/tty/tty_io.c:2818 Allocated by task 65: gsm_data_alloc.constprop.0+0x27/0x190 drivers/tty/n_gsm.c:926 [n_gsm] gsm_send+0x2c/0x580 drivers/tty/n_gsm.c:819 [n_gsm] gsm1_receive+0x547/0xad0 drivers/tty/n_gsm.c:3038 [n_gsm] gsmld_receive_buf+0x176/0x280 drivers/tty/n_gsm.c:3609 [n_gsm] tty_ldisc_receive_buf+0x101/0x1e0 drivers/tty/tty_buffer.c:391 tty_port_default_receive_buf+0x61/0xa0 drivers/tty/tty_port.c:39 flush_to_ldisc+0x1b0/0x750 drivers/tty/tty_buffer.c:445 process_scheduled_works+0x2b0/0x10d0 kernel/workqueue.c:3229 worker_thread+0x3dc/0x950 kernel/workqueue.c:3391 kthread+0x2a3/0x370 kernel/kthread.c:389 ret_from_fork+0x2d/0x70 arch/x86/kernel/process.c:147 ret_from_fork_asm+0x1a/0x30 arch/x86/entry/entry_64.S:257 Freed by task 3367: kfree+0x126/0x420 mm/slub.c:4580 gsm_cleanup_mux+0x36c/0x7b0 drivers/tty/n_gsm.c:3160 [n_gsm] gsmld_ioctl+0x395/0x1450 drivers/tty/n_gsm.c:3408 [n_gsm] tty_ioctl+0x643/0x1100 drivers/tty/tty_io.c:2818 [Analysis] gsm_msg on the tx_ctrl_list or tx_data_list of gsm_mux can be freed by multi threads through ioctl,which leads to the occurrence of uaf. Protect it by gsm tx lock.			

CVE-2024-50074	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: parport: Proper fix for array out-of-bounds access The recent fix for array out-of-bounds accesses replaced sprintf() calls blindly with snprintf(). However, since snprintf() returns the would-be-printed size, not the actually output size, the length calculation can still go over the given limit. Use scnprintf() instead of snprintf(), which returns the actually output letters, for addressing the potential out-of-bounds access properly.	2024-10-29	7.8	High
CVE-2024-50088	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix uninitialized pointer free in add_inode_ref() The add_inode_ref() function does not initialize the "name" struct when it is declared. If any of the following calls to "read_one_inode() returns NULL, dir = read_one_inode(root, parent_objectid); if (!dir) { ret = -ENOENT; goto out; } inode = read_one_inode(root, inode_objectid); if (!inode) { ret = -EIO; goto out; } then "name.name" would be freed on "out" before being initialized. out: ... kfree(name.name); This issue was reported by Coverity with CID 1526744.	2024-10-29	7.8	High
CVE-2024-9632	red hat - multiple products	A flaw was found in the X.org server. Due to improperly tracked allocation size in _XkbSetCompatMap, a local attacker may be able to trigger a buffer overflow condition via a specially crafted payload, leading to denial of service or local privilege escalation in distributions where the X.org server is run with root privileges.	2024-10-30	7.8	High
CVE-2024-44277	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 18.1 and iPadOS 18.1, visionOS 2.1, tvOS 18.1. An app may be able to cause unexpected system termination or corrupt kernel memory.	2024-10-28	7.7	High
CVE-2024-44280	apple - multiple products	A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to modify protected parts of the file system.	2024-10-28	7.7	High

CVE-2024-44295	apple - multiple products	This issue was addressed with additional entitlement checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to modify protected parts of the file system.	2024-10-28	7.7	High
CVE-2024-44196	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to modify protected parts of the file system.	2024-10-28	7.5	High
CVE-2024-44203	apple - macos	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.	2024-10-28	7.5	High
CVE-2024-44208	apple - macos	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15. An app may be able to bypass certain Privacy preferences.	2024-10-28	7.5	High
CVE-2024-44228	apple - xcode	This issue was addressed with improved permissions checking. This issue is fixed in Xcode 16. An app may be able to inherit Xcode permissions and access user data.	2024-10-28	7.5	High
CVE-2024-44289	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to read sensitive location information.	2024-10-28	7.5	High
CVE-2024-50083	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: tcp: fix mptcp DSS corruption due to large pmtu xmit Syzkaller was able to trigger a DSS corruption: TCP: request_sock_subflow_v4: Possible SYN flooding on port [::]:20002. Sending cookies. ------------[cut here]------------ WARNING: CPU: 0 PID: 5227 at net/mptcp/protocol.c:695 __mptcp_move_skbs_from_subflow+0x20a9/0x21f0 net/mptcp/protocol.c:695 Modules linked in: CPU: 0 UID: 0 PID: 5227 Comm: syz-executor350 Not tainted 6.11.0-syzkaller-08829-gaf9c191ac2a0 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024 RIP: 0010:__mptcp_move_skbs_from_subflow+0x20a9/0x21f0 net/mptcp/protocol.c:695 Code: 0f b6 dc 31 ff 89 de e8 b5 dd ea f5 89 d8 48 81 c4 50 01 00 00 5b 41 5c 41 5d 41 5e 41 5f 5d c3 cc cc cc cc e8 98 da ea f5 90 <0f> 0b 90 e9 47 ff ff ff e8 8a da ea f5 90 0f 0b 90 e9 99 e0 ff ff RSP: 0018:ffffc90000006db8 EFLAGS: 00010246 RAX: ffffffff8ba9df18 RBX: 00000000000055f0 RCX: ffff888030023c00	2024-10-29	7.5	High

		RDX: 0000000000000100 RSI: 00000000000081e5 RDI: 00000000000055f0 RBP: 1ffff110062bf1ae R08: ffffffff8ba9cf12 R09: 1ffff110062bf1b8 R10: dfffc0000000000 R11: ffffed10062bf1b9 R12: 0000000000000000 R13: dfffc0000000000 R14: 00000000700cec61 R15: 00000000000081e5 FS: 000055556679c380(0000) GS:ffff8880b8600000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000020287000 CR3: 0000000077892000 CR4: 00000000003506f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <IRQ> move_skbs_to_msk net/mptcp/protocol.c:811 [inline] mptcp_data_ready+0x29c/0xa90 net/mptcp/protocol.c:854 subflow_data_ready+0x34a/0x920 net/mptcp/subflow.c:1490 tcp_data_queue+0x20fd/0x76c0 net/ipv4/tcp_input.c:5283 tcp_rcv_established+0xfba/0x2020 net/ipv4/tcp_input.c:6237 tcp_v4_do_rcv+0x96d/0xc70 net/ipv4/tcp_ipv4.c:1915 tcp_v4_rcv+0x2dc0/0x37f0 net/ipv4/tcp_ipv4.c:2350 ip_protocol_deliver_rcu+0x22e/0x440 net/ipv4/ip_input.c:205 ip_local_deliver_finish+0x341/0x5f0 net/ipv4/ip_input.c:233 NF_HOOK+0x3a4/0x450 include/linux/netfilter.h:314 NF_HOOK+0x3a4/0x450 include/linux/netfilter.h:314 __netif_receive_skb_one_core net/core/dev.c:5662 [inline] __netif_receive_skb+0x2bf/0x650 net/core/dev.c:5775 process_backlog+0x662/0x15b0 net/core/dev.c:6107 __napi_poll+0xcb/0x490 net/core/dev.c:6771 napi_poll net/core/dev.c:6840 [inline]			

		net_rx_action+0x89b/0x1240 net/core/dev.c:6962 handle_softirqs+0x2c5/0x980 kernel/softirq.c:554 do_softirq+0x11b/0x1e0 kernel/softirq.c:455 </IRQ> <TASK> __local_bh_enable_ip+0x1bb/0x200 kernel/softirq.c:382 local_bh_enable include/linux/bottom_half.h:33 [inline] rcu_read_unlock_bh include/linux/rcupdate.h:919 [inline] __dev_queue_xmit+0x1764/0x3e80 net/core/dev.c:4451 dev_queue_xmit include/linux/netdevice.h:3094 [inline] neigh_hh_output include/net/neighbour.h:526 [inline] neigh_output include/net/neighbour.h:540 [inline] ip_finish_output2+0xd41/0x1390 net/ipv4/ip_output.c:236 ip_local_out net/ipv4/ip_output.c:130 [inline] __ip_queue_xmit+0x118c/0x1b80 net/ipv4/ip_output.c:536 __tcp_transmit_skb+0x2544/0x3b30 net/ipv4/tcp_output.c:1466 tcp_transmit_skb net/ipv4/tcp_output.c:1484 [inline] tcp_mtu_probe net/ipv4/tcp_output.c:2547 [inline] tcp_write_xmit+0x641d/0x6bf0 net/ipv4/tcp_output.c:2752 __tcp_push_pending_frames+0x9b/0x360 net/ipv4/tcp_output.c:3015 tcp_push_pending_frames include/net/tcp.h:2107 [inline] tcp_data_snd_check net/ipv4/tcp_input.c:5714 [inline] tcp_rcv_established+0x1026/0x2020 net/ipv4/tcp_input.c:6239 tcp_v4_do_rcv+0x96d/0xc70 net/ipv4/tcp_ipv4.c:1915 sk_backlog_rcv include/net/sock.h:1113 [inline] __release_sock+0x214/0x350 net/core/sock.c:3072 release_sock+0x61/0x1f0 net/core/sock.c:3626 mptcp_push_ ---truncated---			
CVE-2024-10458	mozilla - multiple products	A permission leak could have occurred from a trusted site to an untrusted site via `embed` or `object` elements. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Firefox ESR < 115.17, Thunderbird < 128.4, and Thunderbird < 132.	2024-10-29	7.5	High

CVE-2024-10459	mozilla - multiple products	An attacker could have caused a use-after-free when accessibility was enabled, leading to a potentially exploitable crash. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Firefox ESR < 115.17, Thunderbird < 128.4, and Thunderbird < 132.	2024-10-29	7.5	High
CVE-2024-10466	mozilla - multiple products	By sending a specially crafted push message, a remote server could have hung the parent process, causing the browser to become unresponsive. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	2024-10-29	7.5	High
CVE-2024-22733	tp-link - mr200_firmware	TP Link MR200 V4 Firmware version 210201 was discovered to contain a null-pointer-dereference in the web administration panel on /cgi/login via the sign, Action or LoginStatus query parameters which could lead to a denial of service by a local or remote unauthenticated attacker.	2024-11-01	7.5	High
CVE-2024-44156	apple - multiple products	A path deletion vulnerability was addressed by preventing vulnerable code from running with privileges. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to bypass Privacy preferences.	2024-10-28	7.1	High
CVE-2024-44159	apple - multiple products	A path deletion vulnerability was addressed by preventing vulnerable code from running with privileges. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to bypass Privacy preferences.	2024-10-28	7.1	High
CVE-2024-44252	apple - multiple products	A logic issue was addressed with improved file handling. This issue is fixed in iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, visionOS 2.1, tvOS 18.1. Restoring a maliciously crafted backup file may lead to modification of protected system files.	2024-10-28	7.1	High
CVE-2024-44258	apple - multiple products	This issue was addressed with improved handling of symlinks. This issue is fixed in iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, visionOS 2.1, tvOS 18.1. Restoring a maliciously crafted backup file may lead to modification of protected system files.	2024-10-28	7.1	High
CVE-2024-50086	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix user-after-free from session log off There is racy issue between smb2 session log off and smb2 session setup. It will cause user-after-free from session log off. This add session_lock when setting SMB2_SESSION_EXPIRED and referece count to session struct not to free session while it is being used.	2024-10-29	7	High
CVE-2024-44260	apple - multiple products	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious app with root privileges may be able to modify the contents of system files.	2024-10-28	6.7	Medium

CVE-2024-10573	red hat - multiple products	An out-of-bounds write flaw was found in mpg123 when handling crafted streams. When decoding PCM, the libmpg123 may write past the end of a heap-located buffer. Consequently, heap corruption may happen, and arbitrary code execution is not discarded. The complexity required to exploit this flaw is considered high as the payload must be validated by the MPEG decoder and the PCM synth before execution. Additionally, to successfully execute the attack, the user must scan through the stream, making web live stream content (such as web radios) a very unlikely attack vector.	2024-10-31	6.7	Medium
CVE-2024-44155	apple - multiple products	A custom URL scheme handling issue was addressed with improved input validation. This issue is fixed in Safari 18, iOS 17.7.1 and iPadOS 17.7.1, macOS Sequoia 15, watchOS 11, iOS 18 and iPadOS 18. Maliciously crafted web content may violate iframe sandboxing policy.	2024-10-28	6.5	Medium
CVE-2024-44279	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. Parsing a file may lead to disclosure of user information.	2024-10-28	6.5	Medium
CVE-2024-44294	apple - multiple products	A path deletion vulnerability was addressed by preventing vulnerable code from running with privileges. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An attacker with root privileges may be able to delete protected system files.	2024-10-28	6.5	Medium
CVE-2024-44297	apple - multiple products	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. Processing a maliciously crafted message may lead to a denial-of-service.	2024-10-28	6.5	Medium
CVE-2024-44237	apple - multiple products	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. Processing a maliciously crafted file may lead to unexpected app termination.	2024-10-28	6.5	Medium
CVE-2024-44240	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. Processing a maliciously crafted font may result in the disclosure of process memory.	2024-10-28	6.5	Medium
CVE-2024-44283	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. Parsing a maliciously crafted file may lead to an unexpected app termination.	2024-10-28	6.5	Medium

CVE-2024-50076	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: vt: prevent kernel-infoleak in con_font_get() font.data may not initialize all memory spaces depending on the implementation of vc->vc_sw->con_font_get. This may cause info-leak, so to prevent this, it is safest to modify it to initialize the allocated memory space to 0, and it generally does not affect the overall performance of the system.	2024-10-29	6.5	Medium
CVE-2024-10462	mozilla - multiple products	Truncation of a long URL could have allowed origin spoofing in a permission prompt. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	2024-10-29	6.5	Medium
CVE-2024-10463	mozilla - multiple products	Video frames could have been leaked between origins in some situations. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Firefox ESR < 115.17, Thunderbird < 128.4, and Thunderbird < 132.	2024-10-29	6.5	Medium
CVE-2024-10464	mozilla - multiple products	Repeated writes to history interface attributes could have been used to cause a Denial of Service condition in the browser. This was addressed by introducing rate-limiting to this API. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	2024-10-29	6.5	Medium
CVE-2024-10465	mozilla - multiple products	A clipboard "paste" button could persist across tabs which allowed a spoofing attack. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	2024-10-29	6.5	Medium
CVE-2024-10474	mozilla - firefox_focus	Focus was incorrectly allowing internal links to utilize the app scheme used for deeplinking, which could result in links potentially circumventing some URL safety checks This vulnerability affects Focus for iOS < 132.	2024-10-29	6.5	Medium
CVE-2024-41744	ibm - CICS TX Standard	IBM CICS TX Standard 11.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	2024-11-01	6.5	Medium
CVE-2024-8553	red hat - multiple products	A vulnerability was found in Foreman's loader macros introduced with report templates. These macros may allow an authenticated user with permissions to view and create templates to read any field from Foreman's database. By using specific strings in the loader macros, users can bypass permissions and access sensitive information.	2024-10-31	6.3	Medium
CVE-2024-44261	apple - multiple products	This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 17.7.1 and iPadOS 17.7.1, iOS 18.1 and iPadOS 18.1. An attacker may be able to view restricted content from the lock screen.	2024-10-28	6.2	Medium

CVE-2024-44216	apple - multiple products	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to access user-sensitive data.	2024-10-28	6.2	Medium
CVE-2024-44257	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to access sensitive user data.	2024-10-28	6.2	Medium
CVE-2024-10461	mozilla - multiple products	In multipart/x-mixed-replace responses, `Content-Disposition: attachment` in the response header was not respected and did not force a download, which could allow XSS attacks. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	2024-10-29	6.1	Medium
CVE-2024-41745	ibm - CICS TX Standard	IBM CICS TX Standard is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2024-11-01	6.1	Medium
CVE-2024-44213	apple - multiple products	An issue existed in the parsing of URLs. This issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An attacker in a privileged network position may be able to leak sensitive user information.	2024-10-28	5.9	Medium
CVE-2024-41738	ibm - TXSeries for Multiplatforms	IBM TXSeries for Multiplatforms 10.1 could allow an attacker to obtain sensitive information from the query string of an HTTP GET method to process a request which could be obtained using man in the middle techniques.	2024-11-01	5.9	Medium
CVE-2024-44145	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15, iOS 18 and iPadOS 18. An attacker with physical access to a macOS device with Sidecar enabled may be able to bypass the Lock Screen.	2024-10-28	5.7	Medium
CVE-2024-40855	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sequoia 15, macOS Sonoma 14.7.1. A sandboxed app may be able to access sensitive user data.	2024-10-28	5.5	Medium
CVE-2024-44144	apple - multiple products	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 17.7.1 and iPadOS 17.7.1, macOS Sequoia 15, macOS Sonoma 14.7.1, tvOS 18, watchOS 11, visionOS 2, iOS 18 and iPadOS 18. Processing a maliciously crafted file may lead to unexpected app termination.	2024-10-28	5.5	Medium
CVE-2024-44174	apple - macos	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15. An attacker may be able to view restricted content from the lock screen.	2024-10-28	5.5	Medium
CVE-2024-44175	apple - macos	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Sequoia 15,	2024-10-28	5.5	Medium

		macOS Sonoma 14.7.1. An app may be able to access sensitive user data.			
CVE-2024-44194	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 11.1, visionOS 2.1, iOS 18.1 and iPadOS 18.1. An app may be able to access sensitive user data.	2024-10-28	5.5	Medium
CVE-2024-44215	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. Processing an image may result in disclosure of process memory.	2024-10-28	5.5	Medium
CVE-2024-44236	apple - multiple products	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. Processing a maliciously crafted file may lead to unexpected app termination.	2024-10-28	5.5	Medium
CVE-2024-44239	apple - multiple products	An information disclosure issue was addressed with improved private data redaction for log entries. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. An app may be able to leak sensitive kernel state.	2024-10-28	5.5	Medium
CVE-2024-44247	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious application may be able to modify protected parts of the file system.	2024-10-28	5.5	Medium
CVE-2024-44253	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to modify protected parts of the file system.	2024-10-28	5.5	Medium
CVE-2024-44254	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in watchOS 11.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, iOS 18.1 and iPadOS 18.1. An app may be able to access sensitive user data.	2024-10-28	5.5	Medium
CVE-2024-44262	apple - visionos	This issue was addressed with improved redaction of sensitive information. This issue is fixed in visionOS 2.1. A user may be able to view sensitive user information.	2024-10-28	5.5	Medium
CVE-2024-44264	apple - multiple products	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious app may be able to create symlinks to protected regions of the disk.	2024-10-28	5.5	Medium
CVE-2024-44267	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious application may be able to modify protected parts of the file system.	2024-10-28	5.5	Medium
CVE-2024-44269	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1,	2024-10-28	5.5	Medium

		macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. A malicious app may use shortcuts to access restricted files.			
CVE-2024-44273	apple - multiple products	This issue was addressed with improved handling of symlinks. This issue is fixed in iOS 18.1 and iPadOS 18.1, visionOS 2.1, macOS Sonoma 14.7.1, watchOS 11.1, tvOS 18.1. A malicious app may be able to access private information.	2024-10-28	5.5	Medium
CVE-2024-44278	apple - multiple products	An information disclosure issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. A sandboxed app may be able to access sensitive user data in system logs.	2024-10-28	5.5	Medium
CVE-2024-44281	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. Parsing a file may lead to disclosure of user information.	2024-10-28	5.5	Medium
CVE-2024-44282	apple - multiple products	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. Parsing a file may lead to disclosure of user information.	2024-10-28	5.5	Medium
CVE-2024-44284	apple - multiple products	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. Parsing a maliciously crafted file may lead to an unexpected app termination.	2024-10-28	5.5	Medium
CVE-2024-44287	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious application may be able to modify protected parts of the file system.	2024-10-28	5.5	Medium
CVE-2024-44301	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious application may be able to modify protected parts of the file system.	2024-10-28	5.5	Medium
CVE-2024-44302	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, macOS Ventura 13.7.1, macOS Sonoma 14.7.1, watchOS 11.1, visionOS 2.1. Processing a maliciously crafted font may result in the disclosure of process memory.	2024-10-28	5.5	Medium
CVE-2024-50068	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mm/damon/tests/sysfs-kunit.h: fix memory leak in damon_sysfs_test_add_targets() The sysfs_target->regions allocated in damon_sysfs_regions_alloc() is not freed in damon_sysfs_test_add_targets(), which	2024-10-29	5.5	Medium

		cause the following memory leak, free it to fix it. unreferenced object 0xffffff80c2a8db80 (size 96): comm "kunit_try_catch", pid 187, jiffies 4294894363 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..... backtrace (crc 0): [<0000000001e3714d>] kmemleak_alloc+0x34/0x40 [<000000008e6835c1>] __kmalloc_cache_noprof+0x26c/0x2f4 [<000000001286d9f8>] damon_sysfs_test_add_targets+0x1cc/0x738 [<0000000032ef8f77>] kunit_try_run_case+0x13c/0x3ac [<00000000f3edea23>] kunit_generic_run_threadfn_adapter+0x80/0xec [<00000000adf936cf>] kthread+0x2e8/0x374 [<0000000041bb1628>] ret_from_fork+0x10/0x20			
CVE-2024-50069	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: pinctrl: apple: check devm_kasprintf() returned value devm_kasprintf() can return a NULL pointer on failure but this returned value is not checked. Fix this lack and check the returned value. Found by code review.	2024-10-29	5.5	Medium
CVE-2024-50070	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: pinctrl: stm32: check devm_kasprintf() returned value devm_kasprintf() can return a NULL pointer on failure but this returned value is not checked. Fix this lack and check the returned value. Found by code review.	2024-10-29	5.5	Medium
CVE-2024-50072	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: x86/bugs: Use code segment selector for VERW operand Robert Gill reported below #GP in 32-bit mode when dosemu software was executing vm86() system call: general protection fault: 0000 [#1] PREEMPT SMP CPU: 4 PID: 4610 Comm: dosemu.bin Not tainted 6.6.21-gentoo-x86 #1 Hardware name: Dell Inc. PowerEdge 1950/0H723K, BIOS 2.7.0 10/30/2010 EIP: restore_all_switch_stack+0xbe/0xcf EAX: 00000000 EBX: 00000000 ECX: 00000000 EDX: 00000000 ESI: 00000000 EDI: 00000000 EBP: 00000000 ESP:	2024-10-29	5.5	Medium

		ff8affdc DS: 0000 ES: 0000 FS: 0000 GS: 0033 SS: 0068 EFLAGS: 00010046 CR0: 80050033 CR2: 00c2101c CR3: 04b6d000 CR4: 000406d0 Call Trace: show_regs+0x70/0x78 die_addr+0x29/0x70 exc_general_protection+0x13c/0x348 exc_bounds+0x98/0x98 handle_exception+0x14d/0x14d exc_bounds+0x98/0x98 restore_all_switch_stack+0xbe/0xcf exc_bounds+0x98/0x98 restore_all_switch_stack+0xbe/0xcf This only happens in 32-bit mode when VERW based mitigations like MDS/RFDS are enabled. This is because segment registers with an arbitrary user value can result in #GP when executing VERW. Intel SDM vol. 2C documents the following behavior for VERW instruction: #GP(0) - If a memory operand effective address is outside the CS, DS, ES, FS, or GS segment limit. CLEAR_CPU_BUFFERS macro executes VERW instruction before returning to user space. Use %cs selector to reference VERW operand. This ensures VERW will not #GP for an arbitrary user %ds. [mingo: Fixed the SOB chain.]			
CVE-2024-50075	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: xhci: tegra: fix checked USB2 port number If USB virtualizatoin is enabled, USB2 ports are shared between all Virtual Functions. The USB2 port number owned by an USB2 root hub in a Virtual Function may be less than total USB2 phy number supported by the Tegra XUSB controller. Using total USB2 phy number as port number to check all PORTSC values would cause invalid memory access. [116.923438] Unable to handle kernel paging request at virtual address 006c622f7665642f ... [117.213640] Call trace: [117.216783] tegra_xusb_enter_elpg+0x23c/0x658 [117.222021] tegra_xusb_runtime_suspend+0x40/0x68 [117.227260] pm_generic_runtime_suspend+0x30/0x50 [117.232847] __rpm_callback+0x84/0x3c0	2024-10-29	5.5	Medium

		[117.237038] rpm_suspend+0x2dc/0x740 [117.241229] pm_runtime_work+0xa0/0xb8 [117.245769] process_scheduled_works+0x24c/0x478 [117.251007] worker_thread+0x23c/0x328 [117.255547] kthread+0x104/0x1b0 [117.259389] ret_from_fork+0x10/0x20 [117.263582] Code: 54000222 f9461ae8 f8747908 b4ffff48 (f9400100)			
CVE-2024-50077	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: ISO: Fix multiple init when debugfs is disabled If bt_debugfs is not created successfully, which happens if either CONFIG_DEBUG_FS or CONFIG_DEBUG_FS_ALLOW_ALL is unset, then iso_init() returns early and does not set iso_inited to true. This means that a subsequent call to iso_init() will result in duplicate calls to proto_register(), bt_sock_register(), etc. With CONFIG_LIST_HARDENED and CONFIG_BUG_ON_DATA_CORRUPTION enabled, the duplicate call to proto_register() triggers this BUG(): list_add double add: new=ffffffffc0b280d0, prev=ffffffffbab56250, next=ffffffffc0b280d0. ----------[cut here]---------- kernel BUG at lib/list_debug.c:35! Oops: invalid opcode: 0000 [#1] PREEMPT SMP PTI CPU: 2 PID: 887 Comm: bluetoothd Not tainted 6.10.11-1-ao-desktop #1 RIP: 0010:__list_add_valid_or_report+0x9a/0xa0 ... __list_add_valid_or_report+0x9a/0xa0 proto_register+0x2b5/0x340 iso_init+0x23/0x150 [bluetooth] set_iso_socket_func+0x68/0x1b0 [bluetooth] kmem_cache_free+0x308/0x330 hci_sock_sendmsg+0x990/0x9e0 [bluetooth] __sock_sendmsg+0x7b/0x80 sock_write_iter+0x9a/0x110 do_iter_readv_writev+0x11d/0x220 vfs_writev+0x180/0x3e0 do_writev+0xca/0x100 ... This change removes the early return. The check for iso_debugfs being NULL was unnecessary, it is always NULL when iso_inited is false.	2024-10-29	5.5	Medium
CVE-2024-50078	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: Call iso_exit() on module unload	2024-10-29	5.5	Medium

		If iso_init() has been called, iso_exit() must be called on module unload. Without that, the struct proto that iso_init() registered with proto_register() becomes invalid, which could cause unpredictable problems later. In my case, with CONFIG_LIST_HARDENED and CONFIG_BUG_ON_DATA_CORRUPTION enabled, loading the module again usually triggers this BUG(): list_add corruption. next->prev should be prev (ffffffffb5355fd0), but was 0000000000000068. (next=ffffffffc0a010d0). ------------[cut here]------------ kernel BUG at lib/list_debug.c:29! Oops: invalid opcode: 0000 [#1] PREEMPT SMP PTI CPU: 1 PID: 4159 Comm: modprobe Not tainted 6.10.11-4+bt2-ao-desktop #1 RIP: 0010:__list_add_valid_or_report+0x61/0xa0 ... __list_add_valid_or_report+0x61/0xa0 proto_register+0x299/0x320 hci_sock_init+0x16/0xc0 [bluetooth] bt_init+0x68/0xd0 [bluetooth] __pfx_bt_init+0x10/0x10 [bluetooth] do_one_initcall+0x80/0x2f0 do_init_module+0x8b/0x230 __do_sys_init_module+0x15f/0x190 do_syscall_64+0x68/0x110 ...			
CVE-2024-50079	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved:io_uring/sqpoll: ensure task state is TASK_RUNNING when running task_workWhen the sqpoll is exiting and cancels pending work items, it may needto run task_work. If this happens from within io_uring_cancel_generic(),then it may be under waiting for the io_uring_task waitqueue. Thisresults in the below splat from the scheduler, as the ring mutex may beattempted grabbed while in a TASK_INTERRUPTIBLE state.Ensure that the task state is set appropriately for that, just like whatis done for the other cases in io_run_task_work().do not call blocking ops when !TASK_RUNNING; state=1 set at [<0000000029387fd2>] prepare_to_wait+0x88/0x2fcWARNING: CPU: 6 PID: 59939 at kernel/sched/core.c:8561 __might_sleep+0xf4/0x140Modules linked in:CPU: 6 UID: 0 PID: 59939 Comm: iou-sqp-59938 Not tainted 6.12.0-rc3-00113-g8d020023b155 #7456Hardware	2024-10-29	5.5	Medium

		name: linux,dummy-virt (DT)pstate: 61400005 (nZCv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=--)pc : __might_sleep+0xf4/0x140lr : __might_sleep+0xf4/0x140sp : ffff80008c5e7830x29: ffff80008c5e7830 x28: ffff0000d93088c0 x27: ffff60001c2d7230x26: dfff800000000000 x25: ffff0000e16b9180 x24: ffff80008c5e7a50x23: 1ffff000118bcf4a x22: ffff0000e16b9180 x21: ffff0000e16b9180x20: 000000000000011b x19: ffff80008310fac0 x18: 1ffff000118bcd90x17: 30303c5b20746120 x16: 74657320313d6574 x15: 0720072007200720x14: 0720072007200720 x13: 0720072007200720 x12: ffff600036c64f0bx11: 1fffe00036c64f0a x10: ffff600036c64f0a x9 : dfff800000000000x8 : 00009fffc939b0f6 x7 : ffff0001b6327853 x6 : 0000000000000001x5 : ffff0001b6327850 x4 : ffff600036c64f0b x3 : ffff8000803c35bcx2 : 0000000000000000 x1 : 0000000000000000 x0 : ffff0000e16b9180Call trace: __might_sleep+0xf4/0x140 mutex_lock+0x84/0x124 io_handle_tw_list+0xf4/0x260 tctx_task_work_run+0x94/0x340 io_run_task_work+0x1ec/0x3c0 io_uring_cancel_generic+0x364/0x524 io_sq_thread+0x820/0x124c ret_from_fork+0x10/0x20			
CVE-2024-50080	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ublk: don't allow user copy for unprivileged device UBLK_F_USER_COPY requires userspace to call write() on ublk char device for filling request buffer, and unprivileged device can't be trusted. So don't allow user copy for unprivileged device.	2024-10-29	5.5	Medium
CVE-2024-50081	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: blk-mq: setup queue ->tag_set before initializing hctx Commit 7b815817aa58 ("blk-mq: add helper for checking if one CPU is mapped to specified hctx") needs to check queue mapping via tag set in hctx's cpuhp handler. However, q->tag_set may not be setup yet when the cpuhp handler is enabled, then kernel oops is triggered. Fix the issue by setup queue tag_set before initializing hctx.	2024-10-29	5.5	Medium
CVE-2024-50084	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: microchip: vcap api: Fix memory leaks in vcap_api_encode_rule_test() Commit a3c1e45156ad ("net: microchip: vcap: Fix use-after-free error in kunit test") fixed the use-after-	2024-10-29	5.5	Medium

		free error, but introduced below memory leaks by removing necessary vcap_free_rule(), add it to fix it. unreferenced object 0xffffff80ca58b700 (size 192): comm "kunit_try_catch", pid 1215, jiffies 4294898264 hex dump (first 32 bytes): 00 12 7a 00 05 00 00 00 0a 00 00 00 64 00 00 00 ..z.....d... 00 00 00 00 00 00 00 00 00 00 04 0b cc 80 ff ff ff ..... backtrace (crc 9c09c3fe): [<0000000052a0be73>] kmemleak_alloc+0x34/0x40 [<0000000043605459>] __kmalloc_cache_noprof+0x26c/0x2f4 [<0000000040a01b8d>] vcap_alloc_rule+0x3cc/0x9c4 [<000000003fe86110>] vcap_api_encode_rule_test+0x1ac/0x16b0 [<00000000b3595fc4>] kunit_try_run_case+0x13c/0x3ac [<0000000010f5d2bf>] kunit_generic_run_threadfn_adapter+0x80/0xec [<00000000c5d82c9a>] kthread+0x2e8/0x374 [<00000000f4287308>] ret_from_fork+0x10/0x20 unreferenced object 0xffffff80cc0b0400 (size 64): comm "kunit_try_catch", pid 1215, jiffies 4294898265 hex dump (first 32 bytes): 80 04 0b cc 80 ff ff ff 18 b7 58 ca 80 ff ff ff .....X..... 39 00 00 00 02 00 00 00 06 05 04 03 02 01 ff ff 9..... backtrace (crc daf014e9): [<0000000052a0be73>] kmemleak_alloc+0x34/0x40 [<0000000043605459>] __kmalloc_cache_noprof+0x26c/0x2f4 [<000000000ff63fd4>] vcap_rule_add_key+0x2cc/0x528 [<00000000dfdb1e81>] vcap_api_encode_rule_test+0x224/0x16b0 [<00000000b3595fc4>] kunit_try_run_case+0x13c/0x3ac [<0000000010f5d2bf>] kunit_generic_run_threadfn_adapter+0x80/0xec [<00000000c5d82c9a>] kthread+0x2e8/0x374 [<00000000f4287308>] ret_from_fork+0x10/0x20 unreferenced object 0xffffff80cc0b0700 (size 64): comm "kunit_try_catch", pid 1215, jiffies 4294898265			

		hex dump (first 32 bytes): 80 07 0b cc 80 ff ff ff 28 b7 58 ca 80 ff ff ff ....(.X..... 3c 00 00 00 00 00 00 00 01 2f 03 b3 ec ff ff ff <......../..... backtrace (crc 8d877792): [<0000000052a0be73>] kmemleak_alloc+0x34/0x40 [<0000000043605459>] __kmalloc_cache_noprof+0x26c/0x2f4 [<000000006eadfab7>] vcap_rule_add_action+0x2d0/0x52c [<00000000323475d1>] vcap_api_encode_rule_test+0x4d4/0x16b0 [<00000000b3595fc4>] kunit_try_run_case+0x13c/0x3ac [<0000000010f5d2bf>] kunit_generic_run_threadfn_adapter+0x80/0xec [<00000000c5d82c9a>] kthread+0x2e8/0x374 [<00000000f4287308>] ret_from_fork+0x10/0x20 unreferenced object 0xffffff80cc0b0900 (size 64): comm "kunit_try_catch", pid 1215, jiffies 4294898266 hex dump (first 32 bytes): 80 09 0b cc 80 ff ff ff 80 06 0b cc 80 ff ff ff ..... 7d 00 00 00 01 00 00 00 00 00 00 00 ff 00 00 00 }..... backtrace (crc 34181e56): [<0000000052a0be73>] kmemleak_alloc+0x34/0x40 [<0000000043605459>] __kmalloc_cache_noprof+0x26c/0x2f4 [<000000000ff63fd4>] vcap_rule_add_key+0x2cc/0x528 [<00000000991e3564>] vcap_val_rule+0xcf0/0x13e8 [<00000000fc9868e5>] vcap_api_encode_rule_test+0x678/0x16b0 [<00000000b3595fc4>] kunit_try_run_case+0x13c/0x3ac [<0000000010f5d2bf>] kunit_generic_run_threadfn_adapter+0x80/0xec [<00000000c5d82c9a>] kthread+0x2e8/0x374 [<00000000f4287308>] ret_from_fork+0x10/0x20 unreferenced object 0xffffff80cc0b0980 (size 64): comm "kunit_try_catch", pid 1215, jiffies 4294898266 hex dump (first 32 bytes): 18 b7 58 ca 80 ff ff ff 00 09 0b cc 80 ff ff ff ..X.....			

		67 00 00 00 00 00 00 00 01 01 74 88 c0 ff ff ff g.....t..... backtrace (crc 275fd9be): [<0000000052a0be73>] kmemleak_alloc+0x34/0x40 [<0000000043605459>] __kmalloc_cache_noprof+0x26c/0x2f4 [<000000000ff63fd4>] vcap_rule_add_key+0x2cc/0x528 [<000000001396a1a2>] test_add_de ---truncated---			
CVE-2024-50085	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: fix UaF read in mptcp_pm_nl_rm_addr_or_subflow Syzkaller reported this splat: ========== BUG: KASAN: slab-use-after-free in mptcp_pm_nl_rm_addr_or_subflow+0xb44/0xcc0 net/mptcp/pm_netlink.c:881 Read of size 4 at addr ffff8880569ac858 by task syz.1.2799/14662 CPU: 0 UID: 0 PID: 14662 Comm: syz.1.2799 Not tainted 6.12.0-rc2-syzkaller-00307-g36c254515dc6 #0 Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2~bpo12+1 04/01/2014 Call Trace: <TASK> __dump_stack lib/dump_stack.c:94 [inline] dump_stack_lvl+0x116/0x1f0 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:377 [inline] print_report+0xc3/0x620 mm/kasan/report.c:488 kasan_report+0xd9/0x110 mm/kasan/report.c:601 mptcp_pm_nl_rm_addr_or_subflow+0xb44/0xcc0 net/mptcp/pm_netlink.c:881 mptcp_pm_nl_rm_subflow_received net/mptcp/pm_netlink.c:914 [inline] mptcp_nl_remove_id_zero_address+0x305/0x4a0 net/mptcp/pm_netlink.c:1572 mptcp_pm_nl_del_addr_doit+0x5c9/0x770 net/mptcp/pm_netlink.c:1603 genl_family_rcv_msg_doit+0x202/0x2f0 net/netlink/genetlink.c:1115 genl_family_rcv_msg net/netlink/genetlink.c:1195 [inline] genl_rcv_msg+0x565/0x800 net/netlink/genetlink.c:1210 netlink_rcv_skb+0x165/0x410 net/netlink/af_netlink.c:2551	2024-10-29	5.5	Medium

		genl_rcv+0x28/0x40 net/netlink/genetlink.c:1219 netlink_unicast_kernel net/netlink/af_netlink.c:1331 [inline] netlink_unicast+0x53c/0x7f0 net/netlink/af_netlink.c:1357 netlink_sendmsg+0x8b8/0xd70 net/netlink/af_netlink.c:1901 sock_sendmsg_nosec net/socket.c:729 [inline] __sock_sendmsg net/socket.c:744 [inline] ____sys_sendmsg+0x9ae/0xb40 net/socket.c:2607 ___sys_sendmsg+0x135/0x1e0 net/socket.c:2661 __sys_sendmsg+0x117/0x1f0 net/socket.c:2690 do_syscall_32_irqs_on arch/x86/entry/common.c:165 [inline] __do_fast_syscall_32+0x73/0x120 arch/x86/entry/common.c:386 do_fast_syscall_32+0x32/0x80 arch/x86/entry/common.c:411 entry_SYSENTER_compat_after_hwframe+0x84/0x8e RIP: 0023:0xf7fe4579 Code: b8 01 10 06 03 74 b4 01 10 07 03 74 b0 01 10 08 03 74 d8 01 00 00 00 00 00 00 00 00 00 00 00 00 51 52 55 89 e5 0f 34 cd 80 <5d> 5a 59 c3 90 90 90 8d b4 26 00 00 00 00 8d b4 26 00 00 00 00 RSP: 002b:00000000f574556c EFLAGS: 00000296 ORIG_RAX: 0000000000000172 RAX: ffffffffffffffda RBX: 000000000000000b RCX: 0000000020000140 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: 0000000000000000 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000296 R12: 0000000000000000 R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 </TASK> Allocated by task 5387: kasan_save_stack+0x33/0x60 mm/kasan/common.c:47 kasan_save_track+0x14/0x30 mm/kasan/common.c:68 poison_kmalloc_redzone mm/kasan/common.c:377 [inline] __kasan_kmalloc+0xaa/0xb0 mm/kasan/common.c:394 kmalloc_noprof include/linux/slab.h:878 [inline] kzalloc_noprof include/linux/slab.h:1014 [inline] subflow_create_ctx+0x87/0x2a0 net/mptcp/subflow.c:1803 subflow_ulp_init+0xc3/0x4d0			

		net/mptcp/subflow.c:1956 __tcp_set_ulp net/ipv4/tcp_ulp.c:146 [inline] tcp_set_ulp+0x326/0x7f0 net/ipv4/tcp_ulp.c:167 mptcp_subflow_create_socket+0x4ae/0x10a0 net/mptcp/subflow.c:1764 __mptcp_subflow_connect+0x3cc/0x1490 net/mptcp/subflow.c:1592 mptcp_pm_create_subflow_or_signal_addr+0xbda/0x23a0 net/mptcp/pm_netlink.c:642 mptcp_pm_nl_fully_established net/mptcp/pm_netlink.c:650 [inline] mptcp_pm_nl_work+0x3a1/0x4f0 net/mptcp/pm_netlink.c:943 mptcp_worker+0x15a/0x1240 net/mptcp/protocol.c:2777 process_one_work+0x958/0x1b30 kernel/workqueue.c:3229 process_scheduled_works kernel/workqueue.c:3310 [inline] worker_thread+0x6c8/0xf00 kernel/workqueue.c:3391 kthread+0x2c1/0x3a0 kernel/kthread.c:389 ret_from_fork+0x45/0x80 arch/x86/ke ---truncated---			
CVE-2024-50087	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix uninitialized pointer free on read_alloc_one_name() error The function read_alloc_one_name() does not initialize the name field of the passed fscrypt_str struct if kmalloc fails to allocate the corresponding buffer. Thus, it is not guaranteed that fscrypt_str.name is initialized when freeing it. This is a follow-up to the linked patch that fixes the remaining instances of the bug introduced by commit e43eec81c516 ("btrfs: use struct qstr instead of name and namelen pairs").	2024-10-29	5.5	Medium
CVE-2024-44232	apple - multiple products	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14.7.1, macOS Ventura 13.7.1, visionOS 2.1, watchOS 11.1, tvOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, iOS 18.1 and iPadOS 18.1. Parsing a maliciously crafted video file may lead to unexpected system termination.	2024-11-01	5.5	Medium
CVE-2024-44233	apple - multiple products	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14.7.1, macOS Ventura 13.7.1, visionOS 2.1, watchOS 11.1, tvOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, iOS 18.1 and iPadOS 18.1. Parsing a maliciously crafted video file may lead to unexpected system termination.	2024-11-01	5.5	Medium

CVE-2024-44234	apple - multiple products	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sonoma 14.7.1, macOS Ventura 13.7.1, visionOS 2.1, watchOS 11.1, tvOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, iOS 18.1 and iPadOS 18.1. Parsing a maliciously crafted video file may lead to unexpected system termination.	2024-11-01	5.5	Medium
CVE-2024-44296	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in tvOS 18.1, iOS 18.1 and iPadOS 18.1, iOS 17.7.1 and iPadOS 17.7.1, watchOS 11.1, visionOS 2.1, macOS Sequoia 15.1, Safari 18.1. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.	2024-10-28	5.4	Medium
CVE-2024-44229	apple - multiple products	An information leakage was addressed with additional validation. This issue is fixed in visionOS 2.1, iOS 18.1 and iPadOS 18.1, macOS Sequoia 15.1, Safari 18.1. Private browsing may leak some browsing history.	2024-10-28	5.3	Medium
CVE-2024-10460	mozilla - multiple products	The origin of an external protocol handler prompt could have been obscured using a data: URL within an `iframe`. This vulnerability affects Firefox < 132, Firefox ESR < 128.4, Thunderbird < 128.4, and Thunderbird < 132.	2024-10-29	5.3	Medium
CVE-2024-10468	mozilla - multiple products	Potential race conditions in IndexedDB could have caused memory corruption, leading to a potentially exploitable crash. This vulnerability affects Firefox < 132 and Thunderbird < 132.	2024-10-29	5.3	Medium
CVE-2024-41741	ibm - TXSeries for Multiplatforms	IBM TXSeries for Multiplatforms 10.1 could allow an attacker to determine valid usernames due to an observable timing discrepancy which could be used in further attacks against the system.	2024-11-01	5.3	Medium
CVE-2024-50082	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: blk-rq-qos: fix crash on rq_qos_wait vs. rq_qos_wake_function race We're seeing crashes from rq_qos_wake_function that look like this: BUG: unable to handle page fault for address: ffffafe180a40084 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 100000067 P4D 100000067 PUD 10027c067 PMD 10115d067 PTE 0 Oops: Oops: 0002 [#1] PREEMPT SMP PTI CPU: 17 UID: 0 PID: 0 Comm: swapper/17 Not tainted 6.12.0-rc3-00013-geca631b8fe80 #11 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.0-0-gd239552ce722-prebuilt.qemu.org 04/01/2014 RIP: 0010:_raw_spin_lock_irqsave+0x1d/0x40 Code: 90 90 90 90 90 90 90 90 90 90 90 90 f3 0f	2024-10-29	4.7	Medium

		1e fa 0f 1f 44 00 00 41 54 9c 41 5c fa 65 ff 05 62 97 30 4c 31 c0 ba 01 00 00 00 <f0> 0f b1 17 75 0a 4c 89 e0 41 5c c3 cc cc cc cc 89 c6 e8 2c 0b 00 RSP: 0018:ffffafe180580ca0 EFLAGS: 00010046 RAX: 0000000000000000 RBX: ffffafe180a3f7a8 RCX: 0000000000000011 RDX: 0000000000000001 RSI: 0000000000000003 RDI: ffffafe180a40084 RBP: 0000000000000000 R08: 00000000001e7240 R09: 0000000000000011 R10: 0000000000000028 R11: 0000000000000888 R12: 0000000000000002 R13: ffffafe180a40084 R14: 0000000000000000 R15: 0000000000000003 FS: 0000000000000000(0000) GS:ffff9aaf1f280000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: ffffafe180a40084 CR3: 000000010e428002 CR4: 0000000000770ef0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 PKRU: 55555554 Call Trace: <IRQ> try_to_wake_up+0x5a/0x6a0 rq_qos_wake_function+0x71/0x80 __wake_up_common+0x75/0xa0 __wake_up+0x36/0x60 scale_up.part.0+0x50/0x110 wb_timer_fn+0x227/0x450 ... So rq_qos_wake_function() calls wake_up_process(data->task), which calls try_to_wake_up(), which faults in raw_spin_lock_irqsave(&p->pi_lock). p comes from data->task, and data comes from the waitqueue entry, which is stored on the waiter's stack in rq_qos_wait(). Analyzing the core dump with drgn, I found that the waiter had already woken up and moved on to a completely unrelated code path, clobbering what was previously data->task. Meanwhile, the waker was passing the clobbered garbage in data->task to wake_up_process(), leading to the crash. What's happening is that in between rq_qos_wake_function() deleting the waitqueue			

		entry and calling wake_up_process(), rq_qos_wait() is finding that it already got a token and returning. The race looks like this: rq_qos_wait() rq_qos_wake_function() ========== prepare_to_wait_exclusive() data->got_token = true; list_del_init(&curr->entry); if (data.got_token) break; finish_wait(&rqw->wait, &data.wq); ^- returns immediately because list_empty_careful(&wq_entry->entry) is true ... return, go do something else ... wake_up_process(data->task) (NO LONGER VALID!)-^ Normally, finish_wait() is supposed to synchronize against the waker. But, as noted above, it is returning immediately because the waitqueue entry has already been removed from the waitqueue. The bug is that rq_qos_wake_function() is accessing the waitqueue entry AFTER deleting it. Note that autoremove_wake_function() wakes the waiter and THEN deletes the waitqueue entry, which is the proper order. Fix it by swapping the order. We also need to use list_del_init_careful() to match the list_empty_careful() in finish_wait().			
CVE-2024-44137	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sequoia 15, macOS Sonoma 14.7.1. An attacker with physical access may be able to share items from the lock screen.	2024-10-28	4.6	Medium
CVE-2024-44235	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 18.1 and iPadOS 18.1. An attacker may be able to view restricted content from the lock screen.	2024-10-28	4.6	Medium
CVE-2024-44274	apple - multiple products	The issue was addressed with improved authentication. This issue is fixed in iOS 17.7.1 and iPadOS 17.7.1, watchOS 11.1, iOS 18.1 and iPadOS 18.1. An attacker with physical access to a locked device may be able to view sensitive user information.	2024-10-28	4.6	Medium
CVE-2024-45477	apache - multiple products	Apache NiFi 1.10.0 through 1.27.0 and 2.0.0-M1 through 2.0.0-M3 support a description field for Parameters in a Parameter Context configuration that is vulnerable to cross-site scripting. An authenticated user, authorized to configure a Parameter Context, can enter arbitrary JavaScript code, which the client browser will execute within the session context of the	2024-10-29	4.6	Medium

		authenticated user. Upgrading to Apache NiFi 1.28.0 or 2.0.0-M4 is the recommended mitigation.			
CVE-2024-44244	apple - multiple products	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 18.1 and iPadOS 18.1, watchOS 11.1, visionOS 2.1, tvOS 18.1, macOS Sequoia 15.1, Safari 18.1. Processing maliciously crafted web content may lead to an unexpected process crash.	2024-10-28	4.3	Medium
CVE-2024-44263	apple - iOS and iPadOS	A logic issue was addressed with improved state management. This issue is fixed in iOS 18.1 and iPadOS 18.1. An app may be able to access user-sensitive data.	2024-10-28	4	Medium
CVE-2024-8013	mongodb - multiple products	A bug in query analysis of certain complex self-referential $lookup subpipelines may result in literal values in expressions for encrypted fields to be sent to the server as plaintext instead of ciphertext. Should this occur, no documents would be returned or written. This issue affects mongocryptd binary (v5.0 versions prior to 5.0.29, v6.0 versions prior to 6.0.17, v7.0 versions prior to 7.0.12 and v7.3 versions prior to 7.3.4) and mongo_crypt_v1.so shared libraries (v6.0 versions prior to 6.0.17, v7.0 versions prior to 7.0.12 and v7.3 versions prior to 7.3.4) released alongside MongoDB Enterprise Server versions.	2024-10-28	3.3	Low
CVE-2024-27849	apple - macos	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 read sensitive location information.	2024-10-28	3.3	Low
CVE-2024-40792	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15. A malicious app may be able to change network settings.	2024-10-28	3.3	Low
CVE-2024-40853	apple - multiple products	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 use Siri to enable Auto-Answer Calls.	2024-10-28	3.3	Low
CVE-2024-44222	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An app may be able to read sensitive location information.	2024-10-28	3.3	Low
CVE-2024-44275	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious application may be able to modify protected parts of the file system.	2024-10-28	3.3	Low
CVE-2024-44197	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. A malicious app may be able to cause a denial-of-service.	2024-10-28	2.7	Low
CVE-2024-10452	grafana - grafana	Organization admins can delete pending invites created in an organization they are not part of.	2024-10-29	2.7	Low

CVE-2024-40851	apple - multiple products	This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 18.1 and iPadOS 18.1. An attacker with physical access may be able to access contact photos from the lock screen.	2024-10-28	2.4	Low
CVE-2024-44251	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in iOS 18.1 and iPadOS 18.1. An attacker may be able to view restricted content from the lock screen.	2024-10-28	2.4	Low
CVE-2024-44265	apple - multiple products	The issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Ventura 13.7.1, macOS Sonoma 14.7.1. An attacker with physical access can input Game Controller events to apps running on a locked device.	2024-10-28	2.4	Low
CVE-2024-44123	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15, iOS 18 and iPadOS 18. A malicious app with root privileges may be able to access keyboard input and location information without user consent.	2024-10-28	2.3	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.