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

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ١٨ أغسطس إلى ٢٤ أغسطس. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- 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

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 18th of August to 24th of August. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2024-42361	Apache	Hertzbeat is an open source, real-time monitoring system. Hertzbeat 1.6.0 and earlier declares a /api/monitor/{monitorId}/metric/{metricFull} endpoint to download job metrics. In the process, it executes a SQL query with user-controlled data, allowing for SQL injection.	2024-08-20	9.8	Critical
CVE-2024-38175	Microsoft	An improper access control vulnerability in the Azure Managed Instance for Apache Cassandra allows an authenticated attacker to elevate privileges over a network.	2024-08-20	9.6	Critical
CVE-2024-28987	SolarWinds	The SolarWinds Web Help Desk (WHD) software is affected by a hardcoded credential vulnerability, allowing remote unauthenticated user to access internal functionality and modify data.	2024-08-21	9.1	Critical
CVE-2024-42362	Apache	Hertzbeat is an open source, real-time monitoring system. Hertzbeat has an authenticated (user role) RCE via unsafe deserialization in /api/monitors/import. This vulnerability is fixed in 1.6.0.	2024-08-20	8.8	High
CVE-2024-6813	NETGEAR	NETGEAR ProSAFE Network Management System getSortString SQL Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Authentication is required to exploit this vulnerability. The specific flaw exists within the getSortString method. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-23207.	2024-08-21	8.8	High
CVE-2024-6814	NETGEAR	NETGEAR ProSAFE Network Management System getFilterString SQL Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of NETGEAR ProSAFE Network Management System. Authentication is required to exploit this vulnerability. The specific flaw exists within the getFilterString method. The issue results from the lack of proper validation of a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-23399.	2024-08-21	8.8	High
CVE-2024-7964	Google	Use after free in Passwords in Google Chrome on Android prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-08-21	8.8	High
CVE-2024-7965	Google	Inappropriate implementation in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-08-21	8.8	High
CVE-2024-7966	Google	Out of bounds memory access in Skia in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who had compromised	2024-08-21	8.8	High

		the renderer process to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)			
CVE-2024-7967	Google	Heap buffer overflow in Fonts in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-08-21	8.8	High
CVE-2024-7968	Google	Use after free in Autofill in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who had convinced the user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-08-21	8.8	High
CVE-2024-7969	Google	Type Confusion in V8 in Google Chrome prior to 128.0.6613.113 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-08-21	8.8	High
CVE-2024-7971	Google	Type confusion in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-08-21	8.8	High
CVE-2024-7972	Google	Inappropriate implementation in V8 in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	2024-08-21	8.8	High
CVE-2024-7973	Google	Heap buffer overflow in PDFium in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file. (Chromium security severity: Medium)	2024-08-21	8.8	High
CVE-2024-7974	Google	Insufficient data validation in V8 API in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: Medium)	2024-08-21	8.8	High
CVE-2024-39576	Dell	Dell Power Manager (DPM), versions 3.15.0 and prior, contains an Incorrect Privilege Assignment vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Code execution and Elevation of privileges.	2024-08-22	8.8	High
CVE-2024-36514	ManageEngine	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in file summary option.	2024-08-23	8.8	High
CVE-2024-36515	ManageEngine	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in dashboard. Note: This vulnerability is different from another vulnerability (CVE-2024-36516), both of which have affected ADAudit Plus' dashboard.	2024-08-23	8.8	High
CVE-2024-36516	ManageEngine	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in dashboard. Note: This vulnerability is different from another vulnerability (CVE-2024-36515), both of which have affected ADAudit Plus' dashboard.	2024-08-23	8.8	High
CVE-2024-36517	ManageEngine	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in alerts module.	2024-08-23	8.8	High
CVE-2024-5466	ManageEngine	Zohocorp ManageEngine OpManager and Remote Monitoring and Management versions 128329 and below are vulnerable to the authenticated remote code execution in the deploy agent option.	2024-08-23	8.8	High
CVE-2024-5467	ManageEngine	Zohocorp ManageEngine ADAudit Plus versions below 8121 are vulnerable to the authenticated SQL injection in account lockout report.	2024-08-23	8.8	High
CVE-2024-5490	ManageEngine	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in aggregate reports option.	2024-08-23	8.8	High
CVE-2024-5556	ManageEngine	Zohocorp ManageEngine ADAudit Plus versions below 8000 are vulnerable to the authenticated SQL injection in reports module.	2024-08-23	8.8	High
CVE-2024-5586	ManageEngine	Zohocorp ManageEngine ADAudit Plus versions below 8121 are vulnerable to the authenticated SQL injection in extranet lockouts report option.	2024-08-23	8.8	High
CVE-2024-20375	Cisco	A vulnerability in the SIP call processing function of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper parsing of SIP messages. An attacker could exploit this vulnerability by sending a crafted SIP message to an affected Cisco Unified CM or Cisco Unified CM SME device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition that interrupts the communications of reliant voice and video devices.	2024-08-21	8.6	High
CVE-2022-43915	IBM	IBM App Connect Enterprise Certified Container 5.0, 7.1, 7.2, 8.0, 8.1, 8.2, 9.0, 9.1, 9.2, 10.0, 10.1, 11.0, 11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 12.0, and 12.1 does not limit calls to unshare in running Pods.	2024-08-24	8.1	High

		This can allow a user with access to execute commands in a running Pod to elevate their user privileges.			
CVE-2024-32927	Google	In sendDeviceState_1_6 of RadioExt.cpp, there is a possible use after free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-08-19	7.8	High
CVE-2022-48874	Linux	In the Linux kernel, the following vulnerability has been resolved: misc: fastrpc: Fix use-after-free and race in fastrpc_map_find Currently, there is a race window between the point when the mutex is unlocked in fastrpc_map_lookup and the reference count increasing (fastrpc_map_get) in fastrpc_map_find, which can also lead to use-after-free. So lets merge fastrpc_map_find into fastrpc_map_lookup which allows us to both protect the maps list by also taking the &fl->lock spinlock and the reference count, since the spinlock will be released only after. Add take_ref argument to make this suitable for all callers.	2024-08-21	7.8	High
CVE-2022-48878	Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_qca: Fix driver shutdown on closed serdev The driver shutdown callback (which sends EDL_SOC_RESET to the device over serdev) should not be invoked when HCI device is not open (e.g. if hci_dev_open_sync() failed), because the serdev and its TTY are not open either. Also skip this step if device is powered off (qca_power_shutdown()). The shutdown callback causes use-after-free during system reboot with Qualcomm Atheros Bluetooth: Unable to handle kernel paging request at virtual address 0072662f67726fd7 ... CPU: 6 PID: 1 Comm: systemd-shutdow Tainted: G W 6.1.0-rt5-00325-g8a5f56bcfcca #8 Hardware name: Qualcomm Technologies, Inc. Robotics RB5 (DT) Call trace: tty_driver_flush_buffer+0x4/0x30 serdev_device_write_flush+0x24/0x34 qca_serdev_shutdown+0x80/0x130 [hci_uart] device_shutdown+0x15c/0x260 kernel_restart+0x48/0xac KASAN report: BUG: KASAN: use-after-free in tty_driver_flush_buffer+0x1c/0x50 Read of size 8 at addr ffff16270c2e0018 by task systemd-shutdow/1 CPU: 7 PID: 1 Comm: systemd-shutdow Not tainted 6.1.0-next-20221220-00014-gb85aaf97fb01-dirty #28 Hardware name: Qualcomm Technologies, Inc. Robotics RB5 (DT) Call trace: dump_backtrace.part.0+0xdc/0xf0 show_stack+0x18/0x30 dump_stack_lvl+0x68/0x84 print_report+0x188/0x488 kasan_report+0xa4/0xf0 __asan_load8+0x80/0xac tty_driver_flush_buffer+0x1c/0x50 ttyport_write_flush+0x34/0x44 serdev_device_write_flush+0x48/0x60 qca_serdev_shutdown+0x124/0x274 device_shutdown+0x1e8/0x350 kernel_restart+0x48/0xb0 __do_sys_reboot+0x244/0x2d0 __arm64_sys_reboot+0x54/0x70 invoke_syscall+0x60/0x190 el0_svc_common.constprop.0+0x7c/0x160 do_el0_svc+0x44/0xf0	2024-08-21	7.8	High

		el0_svc+0x2c/0x6c el0t_64_sync_handler+0xbc/0x140 el0t_64_sync+0x190/0x194			
CVE-2022-48892	Linux	In the Linux kernel, the following vulnerability has been resolved: sched/core: Fix use-after-free bug in dup_user_cpus_ptr() Since commit 07ec77a1d4e8 ("sched: Allow task CPU affinity to be restricted on asymmetric systems"), the setting and clearing of user_cpus_ptr are done under pi_lock for arm64 architecture. However, dup_user_cpus_ptr() accesses user_cpus_ptr without any lock protection. Since sched_setaffinity() can be invoked from another process, the process being modified may be undergoing fork() at the same time. When racing with the clearing of user_cpus_ptr in __set_cpus_allowed_ptr_locked(), it can lead to user-after-free and possibly double-free in arm64 kernel. Commit 8f9ea86fdf99 ("sched: Always preserve the user requested cpumask") fixes this problem as user_cpus_ptr, once set, will never be cleared in a task's lifetime. However, this bug was re-introduced in commit 851a723e45d1 ("sched: Always clear user_cpus_ptr in do_set_cpus_allowed()") which allows the clearing of user_cpus_ptr in do_set_cpus_allowed(). This time, it will affect all arches. Fix this bug by always clearing the user_cpus_ptr of the newly cloned/forked task before the copying process starts and check the user_cpus_ptr state of the source task under pi_lock. Note to stable, this patch won't be applicable to stable releases. Just copy the new dup_user_cpus_ptr() function over.	2024-08-21	7.8	High
CVE-2023-22576	Dell	Dell Repository Manager version 3.4.2 and earlier, contain a Local Privilege Escalation Vulnerability in Installation module. A local low privileged attacker may potentially exploit this vulnerability leading to the execution of arbitrary executable on the operating system with high privileges using the existing vulnerability in operating system. Exploitation may lead to unavailability of the service.	2024-08-21	7.8	High
CVE-2024-7977	Google	Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a malicious file. (Chromium security severity: Medium)	2024-08-21	7.8	High
CVE-2024-7979	Google	Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a crafted symbolic link. (Chromium security severity: Medium)	2024-08-21	7.8	High
CVE-2024-7980	Google	Insufficient data validation in Installer in Google Chrome on Windows prior to 128.0.6613.84 allowed a local attacker to perform privilege escalation via a crafted symbolic link. (Chromium security severity: Medium)	2024-08-21	7.8	High
CVE-2022-48912	Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: fix use-after-free in __nf_register_net_hook() We must not dereference @new_hooks after nf_hook_mutex has been released, because other threads might have freed our allocated hooks already. BUG: KASAN: use-after-free in nf_hook_entries_get_hook_ops include/linux/netfilter.h:130 [inline] BUG: KASAN: use-after-free in hooks_validate net/netfilter/core.c:171 [inline] BUG: KASAN: use-after-free in __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 Read of size 2 at addr ffff88801c1a8000 by task syz-executor237/4430 CPU: 1 PID: 4430 Comm: syz-executor237 Not tainted 5.17.0-rc5-syzkaller-00306-g2293be58d6a1 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: <TASK>	2024-08-22	7.8	High

		__dump_stack lib/dump_stack.c:88 [inline] dump_stack_lvl+0xcd/0x134 lib/dump_stack.c:106 print_address_description.constprop.0.cold+0x8d/0x336 mm/kasan/report.c:255 __kasan_report mm/kasan/report.c:442 [inline] kasan_report.cold+0x83/0xdf mm/kasan/report.c:459 nf_hook_entries_get_hook_ops include/linux/netfilter.h:130 [inline] hooks_validate net/netfilter/core.c:171 [inline] __nf_register_net_hook+0x77a/0x820 net/netfilter/core.c:438 nf_register_net_hook+0x114/0x170 net/netfilter/core.c:571 nf_register_net_hooks+0x59/0xc0 net/netfilter/core.c:587 nf_synproxy_ipv6_init+0x85/0xe0 net/netfilter/nf_synproxy_core.c:1218 synproxy_tg6_check+0x30d/0x560 net/ipv6/netfilter/ip6t_SYNPROXY.c:81 xt_check_target+0x26c/0x9e0 net/netfilter/x_tables.c:1038 check_target net/ipv6/netfilter/ip6_tables.c:530 [inline] find_check_entry.constprop.0+0x7f1/0x9e0 net/ipv6/netfilter/ip6_tables.c:573 translate_table+0xc8b/0x1750 net/ipv6/netfilter/ip6_tables.c:735 do_replace net/ipv6/netfilter/ip6_tables.c:1153 [inline] do_ip6t_set_ctl+0x56e/0xb90 net/ipv6/netfilter/ip6_tables.c:1639 nf_setsockopt+0x83/0xe0 net/netfilter/nf_sockopt.c:101 ipv6_setsockopt+0x122/0x180 net/ipv6/ipv6_sockglue.c:1024 rawv6_setsockopt+0xd3/0x6a0 net/ipv6/raw.c:1084 __sys_setsockopt+0x2db/0x610 net/socket.c:2180 __do_sys_setsockopt net/socket.c:2191 [inline] __se_sys_setsockopt net/socket.c:2188 [inline] __x64_sys_setsockopt+0xba/0x150 net/socket.c:2188 do_syscall_x64 arch/x86/entry/common.c:50 [inline] do_syscall_64+0x35/0xb0 arch/x86/entry/common.c:80 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7f65a1ace7d9 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 71 15 00 00 90 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 b8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f65a1a7f308 EFLAGS: 00000246 ORIG_RAX: 0000000000000036 RAX: ffffffffffffffda RBX: 0000000000000006 RCX: 00007f65a1ace7d9 RDX: 0000000000000040 RSI: 0000000000000029 RDI: 0000000000000003 RBP: 00007f65a1b574c8 R08: 0000000000000001 R09: 0000000000000000 R10: 0000000020000000 R11: 0000000000000246 R12: 00007f65a1b55130 R13: 00007f65a1b574c0 R14: 00007f65a1b24090 R15: 0000000000022000 </TASK> The buggy address belongs to the page: page:ffffea0000706a00 refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x1c1a8 flags: 0xfff00000000000(node=0|zone=1|lastcpupid=0x7ff) raw: 00fff00000000000 ffffea0001c1b108 ffffea000046dd08 0000000000000000 raw: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: kasan: bad access detected page_owner tracks the page as freed page last allocated via order 2, migratetype Unmovable, gfp_mask 0x52dc0(GFP_KERNEL|__GFP_NOWARN|__GFP_NORETRY|__GFP _COMP|__GFP_ZERO), pid 4430, ts 1061781545818, free_ts 1061791488993 prep_new_page mm/page_alloc.c:2434 [inline] get_page_from_freelist+0xa72/0x2f50 mm/page_alloc.c:4165 __alloc_pages+0x1b2/0x500 mm/page_alloc.c:5389 __alloc_pages_node include/linux/gfp.h:572 [inline] alloc_pages_node include/linux/gfp.h:595 [inline] kmalloc_large_node+0x62/0x130 mm/slub.c:4438 __kmalloc_node+0x35a/0x4a0 mm/slub. ---truncated---			
CVE-2022-48913	Linux	In the Linux kernel, the following vulnerability has been resolved: blktrace: fix use after free for struct blk_trace When tracing the whole disk, 'dropped' and 'msg' will be created under 'q->debugfs_dir' and 'bt->dir' is NULL, thus blk_trace_free()	2024-08-22	7.8	High

won't remove those files. What's worse, the following UAF can be triggered because of accessing stale 'dropped' and 'msg':

==========
BUG: KASAN: use-after-free in blk_dropped_read+0x89/0x100
Read of size 4 at addr ffff88816912f3d8 by task blktrace/1188

CPU: 27 PID: 1188 Comm: blktrace Not tainted 5.17.0-rc4-next-20220217+ #469
Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS ?-20190727_073836-4
Call Trace:
 <TASK>
 dump_stack_lvl+0x34/0x44
 print_address_description.constprop.0.cold+0xab/0x381
 ? blk_dropped_read+0x89/0x100
 ? blk_dropped_read+0x89/0x100
 kasan_report.cold+0x83/0xdf
 ? blk_dropped_read+0x89/0x100
 kasan_check_range+0x140/0x1b0
 blk_dropped_read+0x89/0x100
 ? blk_create_buf_file_callback+0x20/0x20
 ? kmem_cache_free+0xa1/0x500
 ? do_sys_openat2+0x258/0x460
 full_proxy_read+0x8f/0xc0
 vfs_read+0xc6/0x260
 ksys_read+0xb9/0x150
 ? vfs_write+0x3d0/0x3d0
 ? fpregs_assert_state_consistent+0x55/0x60
 ? exit_to_user_mode_prepare+0x39/0x1e0
 do_syscall_64+0x35/0x80
 entry_SYSCALL_64_after_hwframe+0x44/0xae
RIP: 0033:0x7fbc080d92fd
Code: ce 20 00 00 75 10 b8 00 00 00 00 0f 05 48 3d 01 f0 ff ff 73 31 c3 48 83 1
RSP: 002b:00007fbb95ff9cb0 EFLAGS: 00000293 ORIG_RAX: 0000000000000000
RAX: ffffffffffffffda RBX: 00007fbb95ff9dc0 RCX: 00007fbc080d92fd
RDX: 0000000000000100 RSI: 00007fbb95ff9cc0 RDI: 0000000000000045
RBP: 0000000000000045 R08: 0000000000406299 R09: 00000000ffffffd
R10: 000000000153afa0 R11: 0000000000000293 R12: 00007fbb780008c0
R13: 00007fbb78000938 R14: 0000000000608b30 R15: 00007fbb780029c8
 </TASK>

Allocated by task 1050:
 kasan_save_stack+0x1e/0x40
 __kasan_kmalloc+0x81/0xa0
 do_blk_trace_setup+0xcb/0x410
 __blk_trace_setup+0xac/0x130
 blk_trace_ioctl+0xe9/0x1c0
 blkdev_ioctl+0xf1/0x390
 __x64_sys_ioctl+0xa5/0xe0
 do_syscall_64+0x35/0x80
 entry_SYSCALL_64_after_hwframe+0x44/0xae

Freed by task 1050:
 kasan_save_stack+0x1e/0x40
 kasan_set_track+0x21/0x30
 kasan_set_free_info+0x20/0x30
 __kasan_slab_free+0x103/0x180
 kfree+0x9a/0x4c0
 __blk_trace_remove+0x53/0x70
 blk_trace_ioctl+0x199/0x1c0
 blkdev_common_ioctl+0x5e9/0xb30
 blkdev_ioctl+0x1a5/0x390
 __x64_sys_ioctl+0xa5/0xe0
 do_syscall_64+0x35/0x80
 entry_SYSCALL_64_after_hwframe+0x44/0xae

The buggy address belongs to the object at ffff88816912f380
 which belongs to the cache kmalloc-96 of size 96
The buggy address is located 88 bytes inside of
 96-byte region [ffff88816912f380, ffff88816912f3e0)
The buggy address belongs to the page:
page:000000009a1b4e7c refcount:1 mapcount:0

		mapping:0000000000000000 index:0x0f flags: 0x17ffffc0000200(slab|node=0|zone=2|lastcpupid=0x1fffff) raw: 0017ffffc0000200 ffffea00044f1100 dead000000000002 ffff88810004c780 raw: 0000000000000000 0000000000200020 00000001ffffffff 0000000000000000 page dumped because: kasan: bad access detected Memory state around the buggy address: ffff88816912f280: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ffff88816912f300: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc >ffff88816912f380: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ^ ffff88816912f400: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ffff88816912f480: fa fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ========== ==========			
CVE-2022-48919	Linux	In the Linux kernel, the following vulnerability has been resolved: cifs: fix double free race when mount fails in cifs_get_root() When cifs_get_root() fails during cifs_smb3_do_mount() we call deactivate_locked_super() which eventually will call delayed_free() which will free the context. In this situation we should not proceed to enter the out: section in cifs_smb3_do_mount() and free the same resources a second time. [Thu Feb 10 12:59:06 2022] BUG: KASAN: use-after-free in rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] Read of size 8 at addr ffff888364f4d110 by task swapper/1/0 [Thu Feb 10 12:59:06 2022] CPU: 1 PID: 0 Comm: swapper/1 Tainted: G OE 5.17.0-rc3+ #4 [Thu Feb 10 12:59:06 2022] Hardware name: Microsoft Corporation Virtual Machine/Virtual Machine, BIOS Hyper-V UEFI Release v4.0 12/17/2019 [Thu Feb 10 12:59:06 2022] Call Trace: [Thu Feb 10 12:59:06 2022] <IRQ> [Thu Feb 10 12:59:06 2022] dump_stack_lvl+0x5d/0x78 [Thu Feb 10 12:59:06 2022] print_address_description.constprop.0+0x24/0x150 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] kasan_report.cold+0x7d/0x117 [Thu Feb 10 12:59:06 2022] ? rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] __asan_load8+0x86/0xa0 [Thu Feb 10 12:59:06 2022] rcu_cblist_dequeue+0x32/0x60 [Thu Feb 10 12:59:06 2022] rcu_core+0x547/0xca0 [Thu Feb 10 12:59:06 2022] ? call_rcu+0x3c0/0x3c0 [Thu Feb 10 12:59:06 2022] ? __this_cpu_preempt_check+0x13/0x20 [Thu Feb 10 12:59:06 2022] ? lock_is_held_type+0xea/0x140 [Thu Feb 10 12:59:06 2022] rcu_core_si+0xe/0x10 [Thu Feb 10 12:59:06 2022] __do_softirq+0x1d4/0x67b [Thu Feb 10 12:59:06 2022] __irq_exit_rcu+0x100/0x150 [Thu Feb 10 12:59:06 2022] irq_exit_rcu+0xe/0x30 [Thu Feb 10 12:59:06 2022] sysvec_hyperv_stimer0+0x9d/0xc0 ... [Thu Feb 10 12:59:07 2022] Freed by task 58179: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50 [Thu Feb 10 12:59:07 2022] kasan_set_track+0x25/0x30 [Thu Feb 10 12:59:07 2022] kasan_set_free_info+0x24/0x40 [Thu Feb 10 12:59:07 2022] ____kasan_slab_free+0x137/0x170 [Thu Feb 10 12:59:07 2022] __kasan_slab_free+0x12/0x20 [Thu Feb 10 12:59:07 2022] slab_free_freelist_hook+0xb3/0x1d0 [Thu Feb 10 12:59:07 2022] kfree+0xcd/0x520 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0x149/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae [Thu Feb 10 12:59:07 2022] Last potentially related work creation: [Thu Feb 10 12:59:07 2022] kasan_save_stack+0x26/0x50	2024-08-22	7.8	High

		[Thu Feb 10 12:59:07 2022] __kasan_record_aux_stack+0xb6/0xc0 [Thu Feb 10 12:59:07 2022] kasan_record_aux_stack_noalloc+0xb/0x10 [Thu Feb 10 12:59:07 2022] call_rcu+0x76/0x3c0 [Thu Feb 10 12:59:07 2022] cifs_umount+0xce/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] cifs_kill_sb+0xc8/0xe0 [cifs] [Thu Feb 10 12:59:07 2022] deactivate_locked_super+0x5d/0xd0 [Thu Feb 10 12:59:07 2022] cifs_smb3_do_mount+0xab9/0xbe0 [cifs] [Thu Feb 10 12:59:07 2022] smb3_get_tree+0x1a0/0x2e0 [cifs] [Thu Feb 10 12:59:07 2022] vfs_get_tree+0x52/0x140 [Thu Feb 10 12:59:07 2022] path_mount+0x635/0x10c0 [Thu Feb 10 12:59:07 2022] __x64_sys_mount+0x1bf/0x210 [Thu Feb 10 12:59:07 2022] do_syscall_64+0x5c/0xc0 [Thu Feb 10 12:59:07 2022] entry_SYSCALL_64_after_hwframe+0x44/0xae			
[CVE-2022-48925](#)	Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/cma: Do not change route.addr.src_addr outside state checks If the state is not idle then resolve_prepare_src() should immediately fail and no change to global state should happen. However, it unconditionally overwrites the src_addr trying to build a temporary any address. For instance if the state is already RDMA_CM_LISTEN then this will corrupt the src_addr and would cause the test in cma_cancel_operation(): if (cma_any_addr(cma_src_addr(id_priv)) && !id_priv->cma_dev) Which would manifest as this trace from syzkaller: BUG: KASAN: use-after-free in __list_add_valid+0x93/0xa0 lib/list_debug.c:26 Read of size 8 at addr ffff8881546491e0 by task syz-executor.1/32204 CPU: 1 PID: 32204 Comm: syz-executor.1 Not tainted 5.12.0-rc8-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: __dump_stack lib/dump_stack.c:79 [inline] dump_stack+0x141/0x1d7 lib/dump_stack.c:120 print_address_description.constprop.0.cold+0x5b/0x2f8 mm/kasan/report.c:232 __kasan_report mm/kasan/report.c:399 [inline] kasan_report.cold+0x7c/0xd8 mm/kasan/report.c:416 __list_add_valid+0x93/0xa0 lib/list_debug.c:26 __list_add include/linux/list.h:67 [inline] list_add_tail include/linux/list.h:100 [inline] cma_listen_on_all drivers/infiniband/core/cma.c:2557 [inline] rdma_listen+0x787/0xe00 drivers/infiniband/core/cma.c:3751 ucma_listen+0x16a/0x210 drivers/infiniband/core/ucma.c:1102 ucma_write+0x259/0x350 drivers/infiniband/core/ucma.c:1732 vfs_write+0x28e/0xa30 fs/read_write.c:603 ksys_write+0x1ee/0x250 fs/read_write.c:658 do_syscall_64+0x2d/0x70 arch/x86/entry/common.c:46 entry_SYSCALL_64_after_hwframe+0x44/0xae This is indicating that an rdma_id_private was destroyed without doing cma_cancel_listens(). Instead of trying to re-use the src_addr memory to indirectly create an any address derived from the dst build one explicitly on the stack and bind to that as any other normal flow would do. rdma_bind_addr() will copy it over the src_addr once it knows the state is valid. This is similar to commit bc0bdc5afaa7 ("RDMA/cma: Do not	2024-08-22	7.8	High

		change route.addr.src_addr.ss_family")			
CVE-2022-48926	Linux	In the Linux kernel, the following vulnerability has been resolved: usb: gadget: rndis: add spinlock for rndis response list There's no lock for rndis response list. It could cause list corruption if there're two different list_add at the same time like below. It's better to add in rndis_add_response / rndis_free_response / rndis_get_next_response to prevent any race condition on response list. [361.894299] [1: irq/191-dwc3:16979] list_add corruption. next->prev should be prev (ffffff80651764d0), but was ffffff883dc36f80. (next=ffffff80651764d0). [361.904380] [1: irq/191-dwc3:16979] Call trace: [361.904391] [1: irq/191-dwc3:16979] __list_add_valid+0x74/0x90 [361.904401] [1: irq/191-dwc3:16979] rndis_msg_parser+0x168/0x8c0 [361.904409] [1: irq/191-dwc3:16979] rndis_command_complete+0x24/0x84 [361.904417] [1: irq/191-dwc3:16979] usb_gadget_giveback_request+0x20/0xe4 [361.904426] [1: irq/191-dwc3:16979] dwc3_gadget_giveback+0x44/0x60 [361.904434] [1: irq/191-dwc3:16979] dwc3_ep0_complete_data+0x1e8/0x3a0 [361.904442] [1: irq/191-dwc3:16979] dwc3_ep0_interrupt+0x29c/0x3dc [361.904450] [1: irq/191-dwc3:16979] dwc3_process_event_entry+0x78/0x6cc [361.904457] [1: irq/191-dwc3:16979] dwc3_process_event_buf+0xa0/0x1ec [361.904465] [1: irq/191-dwc3:16979] dwc3_thread_interrupt+0x34/0x5c	2024-08-22	7.8	High
CVE-2022-48927	Linux	In the Linux kernel, the following vulnerability has been resolved: iio: adc: tsc2046: fix memory corruption by preventing array overflow On one side we have indio_dev->num_channels includes all physical channels + timestamp channel. On other side we have an array allocated only for physical channels. So, fix memory corruption by ARRAY_SIZE() instead of num_channels variable. Note the first case is a cleanup rather than a fix as the software timestamp channel bit in active_scanmask is never set by the IIO core.	2024-08-22	7.8	High
CVE-2022-48943	Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: x86/mmu: make apf token non-zero to fix bug In current async pagefault logic, when a page is ready, KVM relies on kvm_arch_can_dequeue_async_page_present() to determine whether to deliver a READY event to the Guest. This function test token value of struct kvm_vcpu_pv_apf_data, which must be reset to zero by Guest kernel when a READY event is finished by Guest. If value is zero meaning that a READY event is done, so the KVM can deliver another. But the kvm_arch_setup_async_pf() may produce a valid token with zero value, which is confused with previous mention and may lead the loss of this READY event. This bug may cause task blocked forever in Guest: INFO: task stress:7532 blocked for more than 1254 seconds. Not tainted 5.10.0 #16 "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message. task:stress state:D stack: 0 pid: 7532 ppid: 1409	2024-08-22	7.8	High

		flags:0x00000080 Call Trace: __schedule+0x1e7/0x650 schedule+0x46/0xb0 kvm_async_pf_task_wait_schedule+0xad/0xe0 ? exit_to_user_mode_prepare+0x60/0x70 __kvm_handle_async_pf+0x4f/0xb0 ? asm_exc_page_fault+0x8/0x30 exc_page_fault+0x6f/0x110 ? asm_exc_page_fault+0x8/0x30 asm_exc_page_fault+0x1e/0x30 RIP: 0033:0x402d00 RSP: 002b:00007ffd31912500 EFLAGS: 00010206 RAX: 0000000000071000 RBX: ffffffffffffffff RCX: 00000000021a32b0 RDX: 000000000007d011 RSI: 000000000007d000 RDI: 00000000021262b0 RBP: 00000000021262b0 R08: 0000000000000003 R09: 0000000000000086 R10: 00000000000000eb R11: 00007fefbdf2baa0 R12: 0000000000000000 R13: 0000000000000002 R14: 000000000007d000 R15: 0000000000001000			
CVE-2024-38209	Microsoft	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-08-22	7.8	High
CVE-2024-38210	Microsoft	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2024-08-22	7.8	High
CVE-2024-21689	Atlassian	This High severity RCE (Remote Code Execution) vulnerability CVE-2024-21689 was introduced in versions 9.1.0, 9.2.0, 9.3.0, 9.4.0, 9.5.0, and 9.6.0 of Bamboo Data Center and Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 7.6, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires user interaction. Atlassian recommends that Bamboo Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Bamboo Data Center and Server 9.2: Upgrade to a release greater than or equal to 9.2.17 Bamboo Data Center and Server 9.6: Upgrade to a release greater than or equal to 9.6.5 See the release notes ([https://confluence.atlassian.com/bambooreleases/bamboo-release-notes-1189793869.html]). You can download the latest version of Bamboo Data Center and Server from the download center ([https://www.atlassian.com/software/bamboo/download-archives]). This vulnerability was reported via our Bug Bounty program.	2024-08-20	7.6	High
CVE-2024-39745	IBM	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	2024-08-22	7.5	High
CVE-2024-43477	Microsoft	Improper access control in Decentralized Identity Services allows an unauthenticated attacker to disable Verifiable ID's on another tenant.	2024-08-23	7.5	High
CVE-2024-38305	Dell	Dell SupportAssist for Home PCs Installer exe version 4.0.3 contains a privilege escalation vulnerability in the installer. A local low-privileged authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary executables on the operating system with elevated privileges.	2024-08-21	7.3	High
CVE-2022-48881	Linux	In the Linux kernel, the following vulnerability has been resolved: platform/x86/amd: Fix refcount leak in amd_pmc_probe	2024-08-21	7.1	High

		pci_get_domain_bus_and_slot() takes reference, the caller should release the reference by calling pci_dev_put() after use. Call pci_dev_put() in the error path to fix this.			
CVE-2024-21690	Atlassian	This High severity Reflected XSS and CSRF (Cross-Site Request Forgery) vulnerability was introduced in versions 7.19.0, 7.20.0, 8.0.0, 8.1.0, 8.2.0, 8.3.0, 8.4.0, 8.5.0, 8.6.0, 8.7.1, 8.8.0, and 8.9.0 of Confluence Data Center and Server. This Reflected XSS and CSRF (Cross-Site Request Forgery) vulnerability, with a CVSS Score of 7.1, allows an unauthenticated attacker to execute arbitrary HTML or JavaScript code on a victims browser and force a end user to execute unwanted actions on a web application in which they're currently authenticated which has high impact to confidentiality, low impact to integrity, no impact to availability, and requires user interaction. Atlassian recommends that Confluence Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: * Confluence Data Center and Server 7.19: Upgrade to a release greater than or equal to 7.19.26 * Confluence Data Center and Server 8.5: Upgrade to a release greater than or equal to 8.5.14 * Confluence Data Center and Server 9.0: Upgrade to a release greater than or equal to 9.0.1 See the release notes (https://confluence.atlassian.com/doc/confluence-release-notes-327.html). You can download the latest version of Confluence Data Center and Server from the download center (https://www.atlassian.com/software/confluence/download-archives). This vulnerability was reported via our Bug Bounty program.	2024-08-21	7.1	High
CVE-2024-7634	F5	NGINX Agent's "config_dirs" restriction feature allows a highly privileged attacker to gain the ability to write/overwrite files outside of the designated secure directory.	2024-08-22	6.9	Medium
CVE-2024-41773	IBM	IBM Global Configuration Management 7.0.2 and 7.0.3 could allow an authenticated user to archive a global baseline due to improper access controls.	2024-08-20	6.5	Medium
CVE-2024-20417	Cisco	Multiple vulnerabilities in the REST API of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to conduct blind SQL injection attacks. These vulnerabilities are due to insufficient validation of user-supplied input in REST API calls. An attacker could exploit these vulnerabilities by sending crafted input to an affected device. A successful exploit could allow the attacker to view or modify data on the affected device.	2024-08-21	6.5	Medium
CVE-2024-20466	Cisco	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to obtain sensitive information from an affected device. This vulnerability is due to improper enforcement of administrative privilege levels for high-value sensitive data. An attacker with read-only Administrator privileges for the web-based management interface on an affected device could exploit this vulnerability by browsing to a page that contains sensitive data. A successful exploit could allow the attacker to collect sensitive information regarding the configuration of the system.	2024-08-21	6.5	Medium
CVE-2024-20486	Cisco	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack and perform arbitrary actions on an affected device. This vulnerability is due to insufficient CSRF protections for the	2024-08-21	6.5	Medium

		web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on the affected device with the privileges of the targeted user.			
CVE-2024-35151	IBM	IBM OpenPages with Watson 8.3 and 9.0 could allow authenticated users access to sensitive information through improper authorization controls on APIs.	2024-08-22	6.5	Medium
CVE-2024-38207	Microsoft	Microsoft Edge (HTML-based) Memory Corruption Vulnerability	2024-08-23	6.3	Medium
CVE-2024-20488	Cisco	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2024-08-21	6.1	Medium
CVE-2024-38208	Microsoft	Microsoft Edge for Android Spoofing Vulnerability	2024-08-22	6.1	Medium
CVE-2024-41150	ManageEngine	An Stored Cross-site Scripting vulnerability in request module affects Zohocorp ManageEngine ServiceDesk Plus, ServiceDesk Plus MSP and SupportCenter Plus.This issue affects ServiceDesk Plus versions: through 14810; ServiceDesk Plus MSP: through 14800; SupportCenter Plus: through 14800.	2024-08-23	6.1	Medium
CVE-2024-32928	Google	The libcurl CURLOPT_SSL_VERIFYPEER option was disabled on a subset of requests made by Nest production devices which enabled a potential man-in-the-middle attack on requests to Google cloud services by any host the traffic was routed through.	2024-08-19	5.9	Medium
CVE-2024-39746	IBM	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques.	2024-08-22	5.9	Medium
CVE-2022-48876	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix initialization of rx->link and rx->link_sta There are some codepaths that do not initialize rx->link_sta properly. This causes a crash in places which assume that rx->link_sta is valid if rx->sta is valid. One known instance is triggered by __ieee80211_rx_h_amsdu being called from fast-rx. It results in a crash like this one: BUG: kernel NULL pointer dereference, address: 00000000000000a8 #PF: supervisor write access in kernel mode #PF: error_code(0x0002) - not-present page PGD 0 P4D 0 Oops: 0002 [#1] PREEMPT SMP PTI CPU: 1 PID: 506 Comm: mt76-usb-rx phy Tainted: G E 6.1.0-debian64x+1.7 #3 Hardware name: ZOTAC ZBOX-ID92/ZBOX-IQ01/ZBOX-ID92/ZBOX-IQ01, BIOS B220P007 05/21/2014 RIP: 0010:ieee80211_deliver_skb+0x62/0x1f0 [mac80211] Code: 00 48 89 04 24 e8 9e a7 c3 df 89 c0 48 03 1c c5 a0 ea 39 a1 4c 01 6b 08 48 ff 03 48 83 7d 28 00 74 11 48 8b 45 30 48 63 55 44 <48> 83 84 d0 a8 00 00 00 01 41 8b 86 c0 11 00 00 8d 50 fd 83 fa 01 RSP: 0018:ffff999040803b10 EFLAGS: 00010286 RAX: 0000000000000000 RBX: ffffb9903f496480 RCX: 0000000000000000 RDX: 0000000000000000 RSI: 0000000000000000 RDI: 0000000000000000 RBP: ffff999040803ce0 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000000 R12: ffff8d21828ac900 R13: 000000000000004a R14: ffff8d2198ed89c0 R15: ffff8d2198ed8000 FS: 0000000000000000(0000) GS:ffff8d24afe80000(0000) knlGS:0000000000000000	2024-08-21	5.5	Medium

		CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00000000000000a8 CR3: 0000000429810002 CR4: 00000000001706e0 Call Trace: <TASK> __ieee80211_rx_h_amsdu+0x1b5/0x240 [mac80211] ? ieee80211_prepare_and_rx_handle+0xcdd/0x1320 [mac80211] ? __local_bh_enable_ip+0x3b/0xa0 ieee80211_prepare_and_rx_handle+0xcdd/0x1320 [mac80211] ? prepare_transfer+0x109/0x1a0 [xhci_hcd] ieee80211_rx_list+0xa80/0xda0 [mac80211] mt76_rx_complete+0x207/0x2e0 [mt76] mt76_rx_poll_complete+0x357/0x5a0 [mt76] mt76u_rx_worker+0x4f5/0x600 [mt76_usb] ? mt76_get_min_avg_rssi+0x140/0x140 [mt76] __mt76_worker_fn+0x50/0x80 [mt76] kthread+0xed/0x120 ? kthread_complete_and_exit+0x20/0x20 ret_from_fork+0x22/0x30 Since the initialization of rx->link and rx->link_sta is rather convoluted and duplicated in many places, clean it up by using a helper function to set it. [remove unnecessary rx->sta->sta.mlo check]			
CVE-2022-48879	Linux	In the Linux kernel, the following vulnerability has been resolved: efi: fix NULL-deref in init error path In cases where runtime services are not supported or have been disabled, the runtime services workqueue will never have been allocated. Do not try to destroy the workqueue unconditionally in the unlikely event that EFI initialisation fails to avoid dereferencing a NULL pointer.	2024-08-21	5.5	Medium
CVE-2022-48882	Linux	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: Fix macsec possible null dereference when updating MAC security entity (SecY) Upon updating MAC security entity (SecY) in hw offload path, the macsec security association (SA) initialization routine is called. In case of extended packet number (epn) is enabled the salt and ssci attributes are retrieved using the MACsec driver rx_sa context which is unavailable when updating a SecY property such as encoding-sa hence the null dereference. Fix by using the provided SA to set those attributes.	2024-08-21	5.5	Medium
CVE-2022-48888	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/msm/dpu: Fix memory leak in msm_mdss_parse_data_bus_icc_path of_icc_get() alloc resources for path1, we should release it when not need anymore. Early return when IS_ERR_OR_NULL(path0) may leak path1. Defer getting path1 to fix this. Patchwork: https://patchwork.freedesktop.org/patch/514264/	2024-08-21	5.5	Medium
CVE-2022-48915	Linux	In the Linux kernel, the following vulnerability has been resolved: thermal: core: Fix TZ_GET_TRIP NULL pointer dereference Do not call get_trip_hyst() from thermal_genl_cmd_tz_get_trip() if the thermal zone does not define one.	2024-08-22	5.5	Medium
CVE-2022-48918	Linux	In the Linux kernel, the following vulnerability has been resolved: iwlwifi: mvm: check debugfs_dir ptr before use When "debugfs=off" is used on the kernel command line, iwiwifi's mvm module uses an invalid/unchecked debugfs_dir pointer and causes a BUG:	2024-08-22	5.5	Medium

		BUG: kernel NULL pointer dereference, address: 000000000000004f #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] PREEMPT SMP CPU: 1 PID: 503 Comm: modprobe Tainted: G W 5.17.0-rc5 #7 Hardware name: Dell Inc. Inspiron 15 5510/076F7Y, BIOS 2.4.1 11/05/2021 RIP: 0010:iwl_mvm_dbgfs_register+0x692/0x700 [iwlmvm] Code: 69 a0 be 80 01 00 00 48 c7 c7 50 73 6a a0 e8 95 cf ee e0 48 8b 83 b0 1e 00 00 48 c7 c2 54 73 6a a0 be 64 00 00 00 48 8d 7d 8c <48> 8b 48 50 e8 15 22 07 e1 48 8b 43 28 48 8d 55 8c 48 c7 c7 5f 73 RSP: 0018:ffffc90000a0ba68 EFLAGS: 00010246 RAX: ffffffffffffffff RBX: ffff88817d6e3328 RCX: ffff88817d6e3328 RDX: ffffffffa06a7354 RSI: 0000000000000064 RDI: ffffc90000a0ba6c RBP: ffffc90000a0bae0 R08: ffffffff824e4880 R09: ffffffffa069d620 R10: ffffc90000a0ba00 R11: ffffffffffffffff R12: 0000000000000000 R13: ffffc90000a0bb28 R14: ffff88817d6e3328 R15: ffff88817d6e3320 FS: 00007f64dd92d740(0000) GS:ffff88847f640000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 000000000000004f CR3: 000000016fc79001 CR4: 0000000000770ee0 PKRU: 55555554 Call Trace: <TASK> ? iwl_mvm_mac_setup_register+0xbdc/0xda0 [iwlmvm] iwl_mvm_start_post_nvm+0x71/0x100 [iwlmvm] iwl_op_mode_mvm_start+0xab8/0xb30 [iwlmvm] _iwl_op_mode_start+0x6f/0xd0 [iwlwifi] iwl_opmode_register+0x6a/0xe0 [iwlwifi] ? 0xffffffffa0231000 iwl_mvm_init+0x35/0x1000 [iwlmvm] ? 0xffffffffa0231000 do_one_initcall+0x5a/0x1b0 ? kmem_cache_alloc+0x1e5/0x2f0 ? do_init_module+0x1e/0x220 do_init_module+0x48/0x220 load_module+0x2602/0x2bc0 ? __kernel_read+0x145/0x2e0 ? kernel_read_file+0x229/0x290 __do_sys_finit_module+0xc5/0x130 ? __do_sys_finit_module+0xc5/0x130 __x64_sys_finit_module+0x13/0x20 do_syscall_64+0x38/0x90 entry_SYSCALL_64_after_hwframe+0x44/0xae RIP: 0033:0x7f64dda564dd Code: 5b 41 5c c3 66 0f 1f 84 00 00 00 00 00 f3 0f 1e fa 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 1b 29 0f 00 f7 d8 64 89 01 48 RSP: 002b:00007ffdba393f88 EFLAGS: 00000246 ORIG_RAX: 0000000000000139 RAX: ffffffffffffffda RBX: 0000000000000000 RCX: 00007f64dda564dd RDX: 0000000000000000 RSI: 00005575399e2ab2 RDI: 0000000000000001 RBP: 000055753a91c5e0 R08: 0000000000000000 R09: 0000000000000002 R10: 0000000000000001 R11: 0000000000000246 R12: 00005575399e2ab2 R13: 000055753a91ceb0 R14: 0000000000000000 R15: 000055753a923018 </TASK> Modules linked in: btintel(+) btmtk bluetooth vfat snd_hda_codec_hdmi fat snd_hda_codec_realtek snd_hda_codec_generic iwlmvm(+) snd_sof_pci_intel_tgl mac80211 snd_sof_intel_hda_common soundwire_intel soundwire_generic_allocation soundwire_cadence soundwire_bus snd_sof_intel_hda snd_sof_pci snd_sof snd_sof_xtensa_dsp snd_soc_hdac_hda snd_hda_ext_core snd_soc_acpi_intel_match snd_soc_acpi snd_soc_core btrfs snd_compress snd_hda_intel snd_intel_dspcfg snd_intel_sdw_acpi snd_hda_codec raid6_pq iwlwifi snd_hda_core snd_pcm snd_timer snd soundcore cfg80211 intel_ish_ipc(+) thunderbolt rfkill intel_ishtp ucsi_acpi wmi			

		i2c_hid_acpi i2c_hid evdev CR2: 0000000000000004f ---[end trace 0000000000000000]--- Check the debugfs_dir pointer for an error before using it. [change to make both conditional]			
CVE-2022-48924	Linux	In the Linux kernel, the following vulnerability has been resolved: thermal: int340x: fix memory leak in int3400_notify() It is easy to hit the below memory leaks in my TigerLake platform: unreferenced object 0xffff927c8b91dbc0 (size 32): comm "kworker/0:2", pid 112, jiffies 4294893323 (age 83.604s) hex dump (first 32 bytes): 4e 41 4d 45 3d 49 4e 54 33 34 30 30 20 54 68 65 NAME=INT3400 The 72 6d 61 6c 00 6b 6b 6b 6b 6b 6b 6b 6b 6b a5 rmal.kkkkkkkkk. backtrace: [<ffffffff9c502c3e>] __kmalloc_track_caller+0x2fe/0x4a0 [<ffffffff9c7b7c15>] kvasprintf+0x65/0xd0 [<ffffffff9c7b7d6e>] kasprintf+0x4e/0x70 [<ffffffffc04cb662>] int3400_notify+0x82/0x120 [int3400_thermal] [<ffffffff9c8b7358>] acpi_ev_notify_dispatch+0x54/0x71 [<ffffffff9c88f1a7>] acpi_os_execute_deferred+0x17/0x30 [<ffffffff9c2c2c0a>] process_one_work+0x21a/0x3f0 [<ffffffff9c2c2e2a>] worker_thread+0x4a/0x3b0 [<ffffffff9c2cb4dd>] kthread+0xfd/0x130 [<ffffffff9c201c1f>] ret_from_fork+0x1f/0x30 Fix it by calling kfree() accordingly.	2024-08-22	5.5	Medium
CVE-2022-48928	Linux	In the Linux kernel, the following vulnerability has been resolved: iio: adc: men_z188_adc: Fix a resource leak in an error handling path If iio_device_register() fails, a previous ioremap() is left unbalanced. Update the error handling path and add the missing iounmap() call, as already done in the remove function.	2024-08-22	5.5	Medium
CVE-2022-48929	Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix crash due to out of bounds access into reg2btf_ids. When commit e6ac2450d6de ("bpf: Support bpf program calling kernel function") added kfunc support, it defined reg2btf_ids as a cheap way to translate the verifier reg type to the appropriate btf_vmlinux BTF ID, however commit c25b2ae13603 ("bpf: Replace PTR_TO_XXX_OR_NULL with PTR_TO_XXX | PTR_MAYBE_NULL") moved the __BPF_REG_TYPE_MAX from the last member of bpf_reg_type enum to after the base register types, and defined other variants using type flag composition. However, now, the direct usage of reg->type to index into reg2btf_ids may no longer fall into __BPF_REG_TYPE_MAX range, and hence lead to out of bounds access and kernel crash on dereference of bad pointer.	2024-08-22	5.5	Medium
CVE-2022-48930	Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/ib_srp: Fix a deadlock Remove the flush_workqueue(system_long_wq) call since flushing system_long_wq is deadlock-prone and since that call is redundant with a preceding cancel_work_sync()	2024-08-22	5.5	Medium
CVE-2022-48932	Linux	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: DR, Fix slab-out-of-bounds in mlx5_cmd_dr_create_fte When adding a rule with 32 destinations, we hit the following out-of-band access issue:	2024-08-22	5.5	Medium

		BUG: KASAN: slab-out-of-bounds in mlx5_cmd_dr_create_fte+0x18ee/0x1e70 This patch fixes the issue by both increasing the allocated buffers to accommodate for the needed actions and by checking the number of actions to prevent this issue when a rule with too many actions is provided.			
CVE-2022-48933	Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: fix memory leak during stateful obj update stateful objects can be updated from the control plane. The transaction logic allocates a temporary object for this purpose. The ->init function was called for this object, so plain kfree() leaks resources. We must call ->destroy function of the object. nft_obj_destroy does this, but it also decrements the module refcount, but the update path doesn't increment it. To avoid special-casing the update object release, do module_get for the update case too and release it via nft_obj_destroy().	2024-08-22	5.5	Medium
CVE-2022-48934	Linux	In the Linux kernel, the following vulnerability has been resolved: nfp: flower: Fix a potential leak in nfp_tunnel_add_shared_mac() ida_simple_get() returns an id between min (0) and max (NFP_MAX_MAC_INDEX) inclusive. So NFP_MAX_MAC_INDEX (0xff) is a valid id. In order for the error handling path to work correctly, the 'invalid' value for 'ida_idx' should not be in the 0..NFP_MAX_MAC_INDEX range, inclusive. So set it to -1.	2024-08-22	5.5	Medium
CVE-2022-48935	Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: unregister flowtable hooks on netns exit Unregister flowtable hooks before they are releases via nf_tables_flowtable_destroy() otherwise hook core reports UAF. BUG: KASAN: use-after-free in nf_hook_entries_grow+0x5a7/0x700 net/netfilter/core.c:142 net/netfilter/core.c:142 Read of size 4 at addr ffff8880736f7438 by task syz-executor579/3666 CPU: 0 PID: 3666 Comm: syz-executor579 Not tainted 5.16.0-rc5-syzkaller #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 01/01/2011 Call Trace: <TASK> __dump_stack lib/dump_stack.c:88 [inline] __dump_stack lib/dump_stack.c:88 [inline] lib/dump_stack.c:106 dump_stack_lvl+0x1dc/0x2d8 lib/dump_stack.c:106 lib/dump_stack.c:106 print_address_description+0x65/0x380 mm/kasan/report.c:247 mm/kasan/report.c:247 __kasan_report mm/kasan/report.c:433 [inline] __kasan_report mm/kasan/report.c:433 [inline] mm/kasan/report.c:450 kasan_report+0x19a/0x1f0 mm/kasan/report.c:450 mm/kasan/report.c:450 nf_hook_entries_grow+0x5a7/0x700 net/netfilter/core.c:142 net/netfilter/core.c:142 __nf_register_net_hook+0x27e/0x8d0 net/netfilter/core.c:429 net/netfilter/core.c:429 nf_register_net_hook+0xaa/0x180 net/netfilter/core.c:571 net/netfilter/core.c:571 nft_register_flowtable_net_hooks+0x3c5/0x730 net/netfilter/nf_tables_api.c:7232	2024-08-22	5.5	Medium

		net/netfilter/nf_tables_api.c:7232 nf_tables_newflowtable+0x2022/0x2cf0 net/netfilter/nf_tables_api.c:7430 net/netfilter/nf_tables_api.c:7430 nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline] nfnetlink_rcv_batch net/netfilter/nfnetlink.c:513 [inline] net/netfilter/nfnetlink.c:652 nfnetlink_rcv_skb_batch net/netfilter/nfnetlink.c:634 [inline] net/netfilter/nfnetlink.c:652 nfnetlink_rcv+0x10e6/0x2550 net/netfilter/nfnetlink.c:652 net/netfilter/nfnetlink.c:652 __nft_release_hook() calls nft_unregister_flowtable_net_hooks() which only unregisters the hooks, then after RCU grace period, it is guaranteed that no packets add new entries to the flowtable (no flow offload rules and flowtable hooks are reachable from packet path), so it is safe to call nf_flow_table_free() which cleans up the remaining entries from the flowtable (both software and hardware) and it unbinds the flow_block.			
CVE-2022-48938	Linux	In the Linux kernel, the following vulnerability has been resolved: CDC-NCM: avoid overflow in sanity checking A broken device may give an extreme offset like 0xFFF0 and a reasonable length for a fragment. In the sanity check as formulated now, this will create an integer overflow, defeating the sanity check. Both offset and offset + len need to be checked in such a manner that no overflow can occur. And those quantities should be unsigned.	2024-08-22	5.5	Medium
CVE-2022-48940	Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix crash due to incorrect copy_map_value When both bpf_spin_lock and bpf_timer are present in a BPF map value, copy_map_value needs to skirt both objects when copying a value into and out of the map. However, the current code does not set both s_off and t_off in copy_map_value, which leads to a crash when e.g. bpf_spin_lock is placed in map value with bpf_timer, as bpf_map_update_elem call will be able to overwrite the other timer object. When the issue is not fixed, an overwriting can produce the following splat: [root@(none) bpf]# ./test_progs -t timer_crash [15.930339] bpf_testmod: loading out-of-tree module taints kernel. [16.037849] ========== [16.038458] BUG: KASAN: user-memory-access in __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.038944] Write of size 8 at addr 0000000000043ec0 by task test_progs/325 [16.039399] [16.039514] CPU: 0 PID: 325 Comm: test_progs Tainted: G OE 5.16.0+ #278 [16.039983] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS ArchLinux 1.15.0-1 04/01/2014 [16.040485] Call Trace: [16.040645] <TASK> [16.040805] dump_stack_lvl+0x59/0x73 [16.041069] ? __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.041427] kasan_report.cold+0x116/0x11b [16.041673] ? __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.042040] __pv_queued_spin_lock_slowpath+0x32b/0x520 [16.042328] ? memcpy+0x39/0x60 [16.042552] ? pv_hash+0xd0/0xd0 [16.042785] ? lockdep_hardirqs_off+0x95/0xd0	2024-08-22	5.5	Medium

		[16.043079] __bpf_spin_lock_irqsave+0xdf/0xf0 [16.043366] ? bpf_get_current_comm+0x50/0x50 [16.043608] ? jhash+0x11a/0x270 [16.043848] bpf_timer_cancel+0x34/0xe0 [16.044119] bpf_prog_c4ea1c0f7449940d_sys_enter+0x7c/0x81 [16.044500] bpf_trampoline_6442477838_0+0x36/0x1000 [16.044836] __x64_sys_nanosleep+0x5/0x140 [16.045119] do_syscall_64+0x59/0x80 [16.045377] ? lock_is_held_type+0xe4/0x140 [16.045670] ? irqentry_exit_to_user_mode+0xa/0x40 [16.046001] ? mark_held_locks+0x24/0x90 [16.046287] ? asm_exc_page_fault+0x1e/0x30 [16.046569] ? asm_exc_page_fault+0x8/0x30 [16.046851] ? lockdep_hardirqs_on+0x7e/0x100 [16.047137] entry_SYSCALL_64_after_hwframe+0x44/0xae [16.047405] RIP: 0033:0x7f9e4831718d [16.047602] Code: b4 0c 00 0f 05 eb a9 66 0f 1f 44 00 00 f3 0f 1e fa 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d b3 6c 0c 00 f7 d8 64 89 01 48 [16.048764] RSP: 002b:00007fff488086b8 EFLAGS: 00000206 ORIG_RAX: 0000000000000023 [16.049275] RAX: ffffffffffffffda RBX: 00007f9e48683740 RCX: 00007f9e4831718d [16.049747] RDX: 0000000000000000 RSI: 0000000000000000 RDI: 00007fff488086d0 [16.050225] RBP: 00007fff488086f0 R08: 00007fff488085d7 R09: 00007f9e4cb594a0 [16.050648] R10: 0000000000000000 R11: 0000000000000206 R12: 00007f9e484cde30 [16.051124] R13: 0000000000000000 R14: 0000000000000000 R15: 0000000000000000 [16.051608] </TASK> [16.051762] ==========			
		In the Linux kernel, the following vulnerability has been resolved: hwmon: Handle failure to register sensor with thermal zone correctly If an attempt is made to a sensor with a thermal zone and it fails, the call to devm_thermal_zone_of_sensor_register() may return -ENODEV. This may result in crashes similar to the following. Unable to handle kernel NULL pointer dereference at virtual address 00000000000003cd ... Internal error: Oops: 96000021 [#1] PREEMPT SMP ... pstate: 60400009 (nZCv daif +PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : mutex_lock+0x18/0x60 lr : thermal_zone_device_update+0x40/0x2e0 sp : ffff800014c4fc60 x29: ffff800014c4fc60 x28: ffff365ee3f6e000 x27: ffffdde218426790 x26: ffff365ee3f6e000 x25: 0000000000000000 x24: ffff365ee3f6e000 x23: ffffdde218426870 x22: ffff365ee3f6e000 x21: 00000000000003cd x20: ffff365ee8bf3308 x19: ffffffffffffffed x18: 0000000000000000 x17: ffffdde21842689c x16: ffffdde1cb7a0b7c x15: 0000000000000040 x14: ffffdde21a4889a0 x13: 0000000000000228 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : 0000000000000000 x8 : 0000000001120000 x7 : 0000000000000001 x6 : 0000000000000000 x5 : 0068000878e20f07 x4 : 0000000000000000 x3 : 00000000000003cd x2 : ffff365ee3f6e000 x1 : 0000000000000000 x0 : 00000000000003cd Call trace: mutex_lock+0x18/0x60 hwmon_notify_event+0xfc/0x110 0xffffdde1cb7a0a90 0xffffdde1cb7a0b7c irq_thread_fn+0x2c/0xa0			
CVE-2022-48942	Linux		2024-08-22	5.5	Medium

		irq_thread+0x134/0x240 kthread+0x178/0x190 ret_from_fork+0x10/0x20 Code: d503201f d503201f d2800001 aa0103e4 (c8e47c02) Jon Hunter reports that the exact call sequence is: hwmon_notify_event() --> hwmon_thermal_notify() --> thermal_zone_device_update() --> update_temperature() --> mutex_lock() The hwmon core needs to handle all errors returned from calls to devm_thermal_zone_of_sensor_register(). If the call fails with -ENODEV, report that the sensor was not attached to a thermal zone but continue to register the hwmon device.			
CVE-2024-38869	ManageEngine	Zohocorp ManageEngine Endpoint Central affected by Incorrect authorization vulnerability in remote office deploy configurations.This issue affects Endpoint Central: before 11.3.2416.04 and before 11.3.2400.25.	2024-08-23	5.4	Medium
CVE-2024-41841	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-08-23	5.4	Medium
CVE-2024-41843	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-08-23	5.4	Medium
CVE-2024-41844	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-08-23	5.4	Medium
CVE-2024-41845	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-08-23	5.4	Medium
CVE-2024-41846	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-08-23	5.4	Medium
CVE-2024-41847	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-08-23	5.4	Medium
CVE-2024-41848	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-08-23	5.4	Medium
CVE-2024-41875	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-08-23	5.4	Medium
CVE-2024-41876	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2024-08-23	5.4	Medium
CVE-2024-41877	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-08-23	5.4	Medium
CVE-2024-41878	Adobe	Adobe Experience Manager versions 6.5.19 and earlier are affected by a DOM-based Cross-Site Scripting (XSS) vulnerability.	2024-08-23	5.4	Medium

		This vulnerability could allow an attacker to inject and execute arbitrary JavaScript code within the context of the user's browser session. Exploitation of this issue requires user interaction, such as convincing a victim to click on a malicious link.			
CVE-2024-7922	D-Link	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function cgi_audio_search/cgi_create_playlist/cgi_get_album_all_tracks/cgi_get_alltracks_editlist/cgi_get_artist_all_album/cgi_get_genre_all_tracks/cgi_get_tracks_list/cgi_set_airplay_content/cgi_write_playlist of the file /cgi-bin/myMusic.cgi. The manipulation leads to command injection. The attack may be launched 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. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-19	5.3	Medium
CVE-2024-8127	D-Link	A vulnerability classified as critical was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This vulnerability affects the function cgi_unzip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack can be initiated 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. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-24	5.3	Medium
CVE-2024-8128	D-Link	A vulnerability, which was classified as critical, has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. This issue affects the function cgi_add_zip of the file /cgi-bin/webfile_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument path leads to command injection. The attack may be initiated 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. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-24	5.3	Medium
CVE-2024-8129	D-Link	A vulnerability, which was classified as critical, was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. Affected is the function cgi_s3_modify of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_job_name leads to 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. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-24	5.3	Medium
CVE-2024-8130	D-Link	A vulnerability has been found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this vulnerability is the function cgi_s3 of the file /cgi-bin/s3.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_a_key leads to command injection. The attack can be launched 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. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-24	5.3	Medium
CVE-2024-8131	D-Link	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814 and classified as critical. Affected by this issue is the function module_enable_disable of the file /cgi-bin/apkg_mgr.cgi of the component HTTP POST Request Handler. The manipulation	2024-08-24	5.3	Medium

		of the argument f_module_name leads to command injection. The attack may be launched 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. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.			
CVE-2024-8132	D-Link	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been classified as critical. This affects the function webdav_mgr of the file /cgi-bin/webdav_mgr.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_path leads to command injection. It is possible to initiate 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. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-24	5.3	Medium
CVE-2024-8133	D-Link	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been declared as critical. This vulnerability affects the function cgi_FMT_R5_SpareDsk_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack can be initiated 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. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-24	5.3	Medium
CVE-2024-8134	D-Link	A vulnerability was found in D-Link DNS-120, DNR-202L, DNS-315L, DNS-320, DNS-320L, DNS-320LW, DNS-321, DNR-322L, DNS-323, DNS-325, DNS-326, DNS-327L, DNR-326, DNS-340L, DNS-343, DNS-345, DNS-726-4, DNS-1100-4, DNS-1200-05 and DNS-1550-04 up to 20240814. It has been rated as critical. This issue affects the function cgi_FMT_Std2R5_1st_DiskMGR of the file /cgi-bin/hd_config.cgi of the component HTTP POST Request Handler. The manipulation of the argument f_source_dev leads to command injection. The attack may be initiated 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. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-08-24	5.3	Medium
CVE-2024-41842	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim’s browser when they browse to the page containing the vulnerable field.	2024-08-23	4.8	Medium
CVE-2022-48931	Linux	In the Linux kernel, the following vulnerability has been resolved: configfs: fix a race in configfs_{,un}register_subsystem() When configfs_register_subsystem() or configfs_unregister_subsystem() is executing link_group() or unlink_group(), it is possible that two processes add or delete list concurrently. Some unfortunate interleavings of them can cause kernel panic. One of cases is: A --> B --> C --> D A <-- B <-- C <-- D delete list_head *B | delete list_head *C ---|--- configfs_unregister_subsystem | configfs_unregister_subsystem unlink_group | unlink_group unlink_obj | unlink_obj list_del_init | list_del_init __list_del_entry | __list_del_entry __list_del | __list_del // next == C | next->prev = prev | | next->prev = prev prev->next = next | | // prev == B	2024-08-22	4.7	Medium

		| prev->next = next Fix this by adding mutex when calling link_group() or unlink_group(), but parent configfs_subsystem is NULL when config_item is root. So I create a mutex configfs_subsystem_mutex.			
CVE-2022-48941	Linux	In the Linux kernel, the following vulnerability has been resolved: ice: fix concurrent reset and removal of VFs Commit c503e63200c6 ("ice: Stop processing VF messages during teardown") introduced a driver state flag, ICE_VF_DEINIT_IN_PROGRESS, which is intended to prevent some issues with concurrently handling messages from VFs while tearing down the VFs. This change was motivated by crashes caused while tearing down and bringing up VFs in rapid succession. It turns out that the fix actually introduces issues with the VF driver caused because the PF no longer responds to any messages sent by the VF during its .remove routine. This results in the VF potentially removing its DMA memory before the PF has shut down the device queues. Additionally, the fix doesn't actually resolve concurrency issues within the ice driver. It is possible for a VF to initiate a reset just prior to the ice driver removing VFs. This can result in the remove task concurrently operating while the VF is being reset. This results in similar memory corruption and panics purportedly fixed by that commit. Fix this concurrency at its root by protecting both the reset and removal flows using the existing VF cfg_lock. This ensures that we cannot remove the VF while any outstanding critical tasks such as a virtchnl message or a reset are occurring. This locking change also fixes the root cause originally fixed by commit c503e63200c6 ("ice: Stop processing VF messages during teardown"), so we can simply revert it. Note that I kept these two changes together because simply reverting the original commit alone would leave the driver vulnerable to worse race conditions.	2024-08-22	4.7	Medium
CVE-2024-6322	Grafana	Access control for plugin data sources protected by the ReqActions json field of the plugin.json is bypassed if the user or service account is granted associated access to any other data source, as the ReqActions check was not scoped to each specific datasource. The account must have prior query access to the impacted datasource.	2024-08-20	4.4	Medium
CVE-2024-7975	Google	Inappropriate implementation in Permissions in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2024-08-21	4.3	Medium
CVE-2024-7976	Google	Inappropriate implementation in FedCM in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2024-08-21	4.3	Medium
CVE-2024-7978	Google	Insufficient policy enforcement in Data Transfer in Google Chrome prior to 128.0.6613.84 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2024-08-21	4.3	Medium
CVE-2024-7981	Google	Inappropriate implementation in Views in Google Chrome prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2024-08-21	4.3	Medium
CVE-2024-8033	Google	Inappropriate implementation in WebApp Installs in Google Chrome on Windows prior to 128.0.6613.84 allowed an attacker who convinced a user to install a malicious application to perform	2024-08-21	4.3	Medium

		UI spoofing via a crafted HTML page. (Chromium security severity: Low)			
CVE-2024-8034	Google	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2024-08-21	4.3	Medium
CVE-2024-8035	Google	Inappropriate implementation in Extensions in Google Chrome on Windows prior to 128.0.6613.84 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2024-08-21	4.3	Medium
CVE-2024-39744	IBM	IBM Sterling Connect:Direct Web Services 6.0, 6.1, 6.2, and 6.3 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.	2024-08-22	4.3	Medium
CVE-2024-41849	Adobe	Adobe Experience Manager versions 6.5.20 and earlier are affected by an Improper Input Validation vulnerability that could lead to a security feature bypass. An low-privileged attacker could leverage this vulnerability to slightly affect the integrity of the page. Exploitation of this issue requires user interaction and scope is changed.	2024-08-23	4.1	Medium
CVE-2022-48937	Linux	In the Linux kernel, the following vulnerability has been resolved: io_uring: add a schedule point in io_add_buffers() Looping ~65535 times doing kmalloc() calls can trigger soft lockups, especially with DEBUG features (like KASAN). [253.536212] watchdog: BUG: soft lockup - CPU#64 stuck for 26s! [b219417889:12575] [253.544433] Modules linked in: vfat fat i2c_mux_pca954x i2c_mux spidev cdc_acm xhci_pci xhci_hcd sha3_generic gq(O) [253.544451] CPU: 64 PID: 12575 Comm: b219417889 Tainted: G S O 5.17.0-smp-DEV #801 [253.544457] RIP: 0010:kernel_text_address (./include/asm-generic/sections.h:192 ./include/linux/kallsyms.h:29 kernel/extable.c:67 kernel/extable.c:98) [253.544464] Code: 0f 93 c0 48 c7 c1 e0 63 d7 a4 48 39 cb 0f 92 c1 20 c1 0f b6 c1 5b 5d c3 90 0f 1f 44 00 00 55 48 89 e5 41 57 41 56 53 48 89 fb <48> c7 c0 00 00 80 a0 41 be 01 00 00 00 48 39 c7 72 0c 48 c7 c0 40 [253.544468] RSP: 0018:ffff8882d8baf4c0 EFLAGS: 00000246 [253.544471] RAX: 1ffff1105b175e00 RBX: ffffffffa13ef09a RCX: 00000000a13ef001 [253.544474] RDX: ffffffffa13ef09a RSI: ffff8882d8baf558 RDI: ffffffffa13ef09a [253.544476] RBP: ffff8882d8baf4d8 R08: ffff8882d8baf5e0 R09: 0000000000000004 [253.544479] R10: ffff8882d8baf5e8 R11: ffffffffa0d59a50 R12: ffff8882eab20380 [253.544481] R13: ffffffffa0d59a50 R14: dffffc0000000000 R15: 1ffff1105b175eb0 [253.544483] FS: 00000000016d3380(0000) GS:ffff88af48c00000(0000) knlGS:0000000000000000 [253.544486] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [253.544488] CR2: 00000000004af0f0 CR3: 00000002eabfa004 CR4: 00000000003706e0 [253.544491] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [253.544492] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [253.544494] Call Trace: [253.544496] <TASK> [253.544498] ? io_queue_sqe (fs/io_uring.c:7143) [253.544505] __kernel_text_address (kernel/extable.c:78) [253.544508] unwind_get_return_address (arch/x86/kernel/unwind_frame.c:19) [253.544514] arch_stack_walk (arch/x86/kernel/stacktrace.c:27) [253.544517] ? io_queue_sqe (fs/io_uring.c:7143) [253.544521] stack_trace_save (kernel/stacktrace.c:123) [253.544527] ____kasan_kmalloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:515) [253.544531] ? ____kasan_kmalloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:515) [253.544533] ? __kasan_kmalloc (mm/kasan/common.c:524) [253.544535] ? kmem_cache_alloc_trace (./include/linux/kasan.h:270 mm/slab.c:3567)	2024-08-22	3.3	Low

		[253.544541] ? io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828) [253.544544] ? __io_queue_sqe (fs/io_uring.c:?) [253.544551] __kasan_kmalloc (mm/kasan/common.c:524) [253.544553] kmem_cache_alloc_trace (./include/linux/kasan.h:270 mm/slab.c:3567) [253.544556] ? io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828) [253.544560] io_issue_sqe (fs/io_uring.c:4556 fs/io_uring.c:4589 fs/io_uring.c:6828) [253.544564] ? __kasan_slab_alloc (mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:469) [253.544567] ? __kasan_slab_alloc (mm/kasan/common.c:39 mm/kasan/common.c:45 mm/kasan/common.c:436 mm/kasan/common.c:469) [253.544569] ? kmem_cache_alloc_bulk (mm/slab.h:732 mm/slab.c:3546) [253.544573] ? __io_alloc_req_refill (fs/io_uring.c:2078) [253.544578] ? io_submit_sqes (fs/io_uring.c:7441) [253.544581] ? __se_sys_io_uring_enter (fs/io_uring.c:10154 fs/io_uring.c:10096) [253.544584] ? __x64_sys_io_uring_enter (fs/io_uring.c:10096) [253.544587] ? do_syscall_64 (arch/x86/entry/common.c:50 arch/x86/entry/common.c:80) [253.544590] ? entry_SYSCALL_64_after_hwframe (??:?) [253.544596] __io_queue_sqe (fs/io_uring.c:?) [253.544600] io_queue_sqe (fs/io_uring.c:7143) [253.544603] io_submit_sqe (fs/io_uring.c:?) [253.544608] io_submit_sqes (fs/io_uring.c:?) [253.544612] __se_sys_io_uring_enter (fs/io_uring.c:10154 fs/io_uri ---truncated---			
CVE-2022-48939	Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Add schedule points in batch ops syzbot reported various soft lockups caused by bpf batch operations. INFO: task kworker/1:1:27 blocked for more than 140 seconds. INFO: task hung in rcu_barrier Nothing prevents batch ops to process huge amount of data, we need to add schedule points in them. Note that maybe_wait_bpf_programs(map) calls from generic_map_delete_batch() can be factorized by moving the call after the loop. This will be done later in -next tree once we get this fix merged, unless there is strong opinion doing this optimization sooner.	2024-08-22	3.3	Low