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 ٢٩ ديسمبر إلى ٤ يناير. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 29th of December to 4th of January. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2024-53842	google - Android	In cc_SendCcImsInfoIndMsg of cc_MmConManagement.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	9.8
CVE-2024-56737	gnu - GRUB2	GNU GRUB (aka GRUB2) through 2.12 has a heap-based buffer overflow in fs/hfs.c via crafted sblock data in an HFS filesystem.	2024-12-29	8.8
CVE-2024-43767	google - Android	In prepare_to_draw_into_mask of SkBlurMaskFilterImpl.cpp, there is a possible heap overflow due to improper input validation. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	8.8
CVE-2024-56740	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: nfs/localio: must clear res.replen in nfs_local_read_done Otherwise memory corruption can occur due to NFSv3 LOCALIO reads leaving garbage in res.replen: - nfs3_read_done() copies that into server->read_hdrsize; from there nfs3_proc_read_setup() copies it to args.replen in new requests. - nfs3_xdr_enc_read3args() passes that to rpc_prepare_reply_pages() which includes it in hdrsize for xdr_init_pages, so that rq_rcv_buf contains a ridiculous len. - This is copied to rq_private_buf and xs_read_stream_request() eventually passes the kvec to sock_recvmsg() which receives incoming data into entirely the wrong place. This is easily reproduced with NFSv3 LOCALIO that is servicing reads when it is made to pivot back to using normal RPC. This switch back to using normal NFSv3 with RPC can occur for a few reasons but this issue was exposed with a test that stops and then restarts the NFSv3 server while LOCALIO is performing heavy read IO.	2024-12-29	7.8
CVE-2024-13043	watchguard - panda_dome	Panda Security Dome Link Following Local Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of Panda Security Dome. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the Hotspot Shield. By creating a junction, an attacker can abuse the application to delete arbitrary files. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of SYSTEM. Was ZDI-CAN-23478.	2024-12-30	7.8
CVE-2024-43077	google - Android	In DevmemValidateFlags of devicemem_server.c , there is a possible out of bounds write due to memory corruption. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8
CVE-2024-43097	google - Android	In resizeToAtLeast of SkRegion.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8

CVE-2024-43762	google - Android	In multiple locations, there is a possible way to avoid unbinding of a service from the system due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8
CVE-2024-43764	google - Android	In onPrimaryClipChanged of ClipboardListener.java, there is a possible way to partially bypass lock screen. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8
CVE-2024-43768	google - Android	In skia_alloc_func of SkDeflate.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8
CVE-2024-43769	google - Android	In isPackageDeviceAdmin of PackageManagerService.java, there is a possible edge case which could prevent the uninstallation of CloudDpc due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8
CVE-2024-11624	google - Android	there is a possible to add apps to bypass VPN due to Undeclared Permission . This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8
CVE-2024-47032	google - Android	In construct_transaction_from_cmd of lwis_ioctl.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8
CVE-2024-53833	google - Android	In prepare_response_locked of lwis_transaction.c, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8
CVE-2024-53835	google - Android	there is a possible biometric bypass due to an unusual root cause. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8
CVE-2024-53837	google - Android	In prepare_response of lwis_periodic_io.c, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8
CVE-2024-53838	google - Android	In Exynos_parsing_user_data_registered_itu_t_t35 of VendorVideoAPI.cpp, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8
CVE-2024-53840	google - Android	there is a possible biometric bypass due to an unusual root cause. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8
CVE-2024-53841	google - Android	In startListeningForDeviceStateChanges, there is a possible Permission Bypass due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.8
CVE-2024-45497	red hat - multiple products	A flaw was found in the OpenShift build process, where the docker-build container is configured with a hostPath volume mount that maps the node's /var/lib/kubelet/config.json file into the build pod. This file contains sensitive credentials necessary for pulling images from private repositories. The mount is not read-only, which allows the attacker to overwrite it. By modifying the config.json file, the attacker can cause a denial of service by preventing the node from pulling new images and potentially exfiltrating sensitive secrets. This flaw impacts the availability of services dependent on image pulls and exposes sensitive information to unauthorized parties.	2024-12-31	7.6
CVE-2024-53834	google - Android	In sms_DisplayHexDumpOfPrivacyBuffer of sms_Utilities.c, there is a possible out of bounds read due to an incorrect bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	7.5
CVE-2024-41766	ibm - Engineering Lifecycle Optimization Publishing	IBM Engineering Lifecycle Optimization - Publishing 7.0.2 and 7.0.3 could allow a remote attacker to cause a denial of service using a complex regular expression.	2025-01-04	7.5
CVE-2024-41767	ibm - Engineering Lifecycle Optimization Publishing	IBM Engineering Lifecycle Optimization - Publishing 7.0.2 and 7.0.3 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify, or delete information in the back-end database.	2025-01-04	7.3
CVE-2024-54181	ibm - WebSphere Automation	IBM WebSphere Automation 1.7.5 could allow a remote privileged user, who has authorized access to the swagger UI, to execute arbitrary code. Using specially crafted input, the user could exploit this vulnerability to execute arbitrary code on the system.	2024-12-30	7.2
CVE-2024-56721	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: x86/CPU/AMD: Terminate the erratum_1386_microcode array The erratum_1386_microcode array requires an empty entry at the end. Otherwise x86_match_cpu_with_stepping() will continue iterate the array after it ended. Add an empty entry to erratum_1386_microcode to its end.	2024-12-29	7.1
CVE-2024-13030	d-link - DIR-823G	A vulnerability was found in D-Link DIR-823G 1.0.2B05_20181207. It has been rated as critical. This issue affects the function SetAutoRebootSettings/SetClientInfo/SetDMZSettings/SetFirewallSettings/SetParentsControlInfo/SetQoSSettings/SetVirtualServerSettings of the file /HNAP1/ of the component Web Management Interface. The manipulation leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.	2024-12-30	6.9
CVE-2024-13102	d-link - DIR-816 A2	A vulnerability classified as critical was found in D-Link DIR-816 A2 1.10CNB05_R1B011D88210. This vulnerability affects unknown code of the file /goform/DDNS of the component DDNS Service. The manipulation leads to improper access controls. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-01-02	6.9
CVE-2024-13103	d-link - DIR-816 A2	A vulnerability, which was classified as critical, has been found in D-Link DIR-816 A2 1.10CNB05_R1B011D88210. This issue affects some unknown processing of the file	2025-01-02	6.9

		/goform/form2AddVrtsrv.cgi of the component Virtual Service Handler. The manipulation leads to improper access controls. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used.		
CVE-2024-13104	d-link - DIR-816 A2	A vulnerability, which was classified as critical, was found in D-Link DIR-816 A2 1.10CNB05_R1B011D88210. Affected is an unknown function of the file /goform/form2AdvanceSetup.cgi of the component WiFi Settings Handler. The manipulation leads to improper access controls. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used.	2025-01-02	6.9
CVE-2024-13105	d-link - DIR-816 A2	A vulnerability has been found in D-Link DIR-816 A2 1.10CNB05_R1B011D88210 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /goform/form2Dhcpd.cgi of the component DHCPD Setting Handler. The manipulation leads to improper access controls. The attack can be launched remotely. The exploit has been disclosed to the public and may be used.	2025-01-02	6.9
CVE-2024-13106	d-link - DIR-816 A2	A vulnerability was found in D-Link DIR-816 A2 1.10CNB05_R1B011D88210 and classified as critical. Affected by this issue is some unknown functionality of the file /goform/form2IPQoSTcAdd of the component IP QoS Handler. The manipulation leads to improper access controls. The attack may be launched remotely. The exploit has been disclosed to the public and may be used.	2025-01-02	6.9
CVE-2024-13107	d-link - DIR-816 A2	A vulnerability was found in D-Link DIR-816 A2 1.10CNB05_R1B011D88210. It has been classified as critical. This affects an unknown part of the file /goform/form2LocalAclEditcfg.cgi of the component ACL Handler. The manipulation leads to improper access controls. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used.	2025-01-02	6.9
CVE-2024-13108	d-link - DIR-816 A2	A vulnerability was found in D-Link DIR-816 A2 1.10CNB05_R1B011D88210. It has been declared as critical. This vulnerability affects unknown code of the file /goform/form2NetSniper.cgi. The manipulation leads to improper access controls. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used.	2025-01-02	6.9
CVE-2024-53836	google - Android	In wbrc_bt_dev_write of wb_regon_coordinator.c, there is a possible out of bounds write due to a buffer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2025-01-03	6.7
CVE-2024-46542	veritas - Data Insight	Veritas / Arctera Data Insight before 7.1.1 allows Application Administrators to conduct SQL injection attacks.	2024-12-30	6.5
CVE-2024-41765	ibm - Engineering Lifecycle Optimization Publishing	IBM Engineering Lifecycle Optimization - Publishing 7.0.2 and 7.0.3 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system.	2025-01-04	6.5
CVE-2024-41768	ibm - Engineering Lifecycle Optimization Publishing	IBM Engineering Lifecycle Optimization - Publishing 7.0.2 and 7.0.3 could allow a remote attacker to cause an unhandled SSL exception which could leave the connection in an unexpected or insecure state.	2025-01-04	6.5
CVE-2024-41763	ibm - Engineering Lifecycle Optimization Publishing	IBM Engineering Lifecycle Optimization - Publishing 7.0.2 and 7.0.3 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	2025-01-04	5.9
CVE-2024-56710	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ceph: fix memory leak in ceph_direct_read_write() The bvecs array which is allocated in iter_get_bvecs_alloc() is leaked and pages remain pinned if ceph_alloc_sparse_ext_map() fails. There is no need to delay the allocation of sparse_ext map until after the bvecs array is set up, so fix this by moving sparse_ext allocation a bit earlier. Also, make a similar adjustment in __ceph_sync_read() for consistency (a leak of the same kind in __ceph_sync_read() has been addressed differently).	2024-12-29	5.5
CVE-2024-56711	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/panel: himax-hx83102: Add a check to prevent NULL pointer dereference drm_mode_duplicate() could return NULL due to lack of memory, which will then call NULL pointer dereference. Add a check to prevent it.	2024-12-29	5.5
CVE-2024-56712	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: udmabuf: fix memory leak on last export_udmabuf() error path In export_udmabuf(), if dma_buf_fd() fails because the FD table is full, a dma_buf owning the udmabuf has already been created; but the error handling in udmabuf_create() will tear down the udmabuf without doing anything about the containing dma_buf. This leaves a dma_buf in memory that contains a dangling pointer; though that doesn't seem to lead to anything bad except a memory leak. Fix it by moving the dma_buf_fd() call out of export_udmabuf() so that we can give it different error handling. Note that the shape of this code changed a lot in commit 5e72b2b41a21 ("udmabuf: convert udmabuf driver to use folios"); but the memory leak seems to have existed since the introduction of udmabuf.	2024-12-29	5.5

CVE-2024-56715	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ionic: Fix netdev notifier unregister on failure If register_netdev() fails, then the driver leaks the netdev notifier. Fix this by calling ionic_lif_unregister() on register_netdev() failure. This will also call ionic_lif_unregister_phc() if it has already been registered.	2024-12-29	5.5
CVE-2024-56716	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netdevsim: prevent bad user input in nsim_dev_health_break_write() If either a zero count or a large one is provided, kernel can crash.	2024-12-29	5.5
CVE-2024-56717	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: mscc: ocelot: fix incorrect IFH SRC_PORT field in ocelot_ifh_set_basic() Packets injected by the CPU should have a SRC_PORT field equal to the CPU port module index in the Analyzer block (ocelot->num_phys_ports). The blamed commit copied the ocelot_ifh_set_basic() call incorrectly from ocelot_xmit_common() in net/dsa/tag_ocelot.c. Instead of calling with "x", it calls with BIT_ULL(x), but the field is not a port mask, but rather a single port index.	2024-12-29	5.5
CVE-2024-56718	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net/smc: protect link down work from execute after lgr freed link down work may be scheduled before lgr freed but execute after lgr freed, which may result in crash. So it is need to hold a reference before shedule link down work, and put the reference after work executed or canceled.	2024-12-29	5.5
CVE-2024-56719	linux - multiple products	The buf (dma cookie) and len stored in this structure are passed to dma_unmap_single() by stmmac_tx_clean(). The DMA API requires that the dma cookie passed to dma_unmap_single() is the same as the value returned from dma_map_single(). However, by moving the assignment later, this is not the case when priv->dma_cap.addr64 > 32 as "des" is offset by proto_hdr_len.	2024-12-29	5.5
CVE-2024-56720	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: bpf, sockmap: Several fixes to bpf_msg_pop_data Several fixes to bpf_msg_pop_data, 1. In sk_msg_shift_left, we should put_page 2. if (len == 0), return early is better 3. pop the entire sk_msg (last == msg->sg.size) should be supported 4. Fix for the value of variable "a" 5. In sk_msg_shift_left, after shifting, i has already pointed to the next element. Addtional sk_msg_iter_var_next may result in BUG.	2024-12-29	5.5
CVE-2024-56722	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: RDMA/hns: Fix cpu stuck caused by printings during reset During reset, cmd to destroy resources such as qp, cq, and mr may fail, and error logs will be printed. When a large number of resources are destroyed, there will be lots of printings, and it may lead to a cpu stuck. Delete some unnecessary printings and replace other printing functions in these paths with the ratelimited version.	2024-12-29	5.5
CVE-2024-56723	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mfd: intel_soc_pmic_bxtwc: Use IRQ domain for PMIC devices While design wise the idea of converting the driver to use the hierarchy of the IRQ chips is correct, the implementation has (inherited) flaws. This was unveiled when platform_get_irq() had started WARN() on IRQ 0 that is supposed to be a Linux IRQ number (also known as vIRQ). Rework the driver to respect IRQ domain when creating each MFD device separately, as the domain is not the same for all of them.	2024-12-29	5.5
CVE-2024-56724	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mfd: intel_soc_pmic_bxtwc: Use IRQ domain for TMU device While design wise the idea of converting the driver to use the hierarchy of the IRQ chips is correct, the implementation has (inherited) flaws. This was unveiled when platform_get_irq() had started WARN() on IRQ 0 that is supposed to be a Linux	2024-12-29	5.5

		IRQ number (also known as vIRQ). Rework the driver to respect IRQ domain when creating each MFD device separately, as the domain is not the same for all of them.		
CVE-2024-56725	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: octeontx2-pf: handle otx2_mbox_get_rsp errors in otx2_dcbnl.c Add error pointer check after calling otx2_mbox_get_rsp().	2024-12-29	5.5
CVE-2024-56726	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: octeontx2-pf: handle otx2_mbox_get_rsp errors in cn10k.c Add error pointer check after calling otx2_mbox_get_rsp().	2024-12-29	5.5
CVE-2024-56727	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: octeontx2-pf: handle otx2_mbox_get_rsp errors in otx2_flows.c Adding error pointer check after calling otx2_mbox_get_rsp().	2024-12-29	5.5
CVE-2024-56728	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: octeontx2-pf: handle otx2_mbox_get_rsp errors in otx2_ethtool.c Add error pointer check after calling otx2_mbox_get_rsp().	2024-12-29	5.5
CVE-2024-56730	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: net/9p/usbg: fix handling of the failed kzalloc() memory allocation On the linux-next, next-20241108 vanilla kernel, the coccinelle tool gave the following error report: ./net/9p/trans_usbg.c:912:5-11: ERROR: allocation function on line 911 returns NULL not ERR_PTR on failure kzalloc() failure is fixed to handle the NULL return case on the memory exhaustion.	2024-12-29	5.5
CVE-2024-56739	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: rtc: check if __rtc_read_time was successful in rtc_timer_do_work() If the __rtc_read_time call fails,, the struct rtc_time tm; may contain uninitialized data, or an illegal date/time read from the RTC hardware. When calling rtc_tm_to_ktime later, the result may be a very large value (possibly KTIME_MAX). If there are periodic timers in rtc->timerqueue, they will continually expire, may causing kernel softlockup.	2024-12-29	5.5
CVE-2024-56741	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: apparmor: test: Fix memory leak for aa_unpack_strdup() The string allocated by kmemdup() in aa_unpack_strdup() is not freed and cause following memory leaks	2024-12-29	5.5
CVE-2024-56742	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: vfio/mlx5: Fix an unwind issue in mlx5vf_add_migration_pages() Fix an unwind issue in mlx5vf_add_migration_pages(). If a set of pages is allocated but fails to be added to the SG table, they need to be freed to prevent a memory leak. Any pages successfully added to the SG table will be freed as part of mlx5vf_free_data_buffer().	2024-12-29	5.5
CVE-2024-56743	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: nfs_common: must not hold RCU while calling nfsd_file_put_local Move holding the RCU from nfs_to_nfsd_file_put_local to nfs_to_nfsd_net_put. It is the call to nfs_to->nfsd_serv_put that requires the RCU anyway (the puts for nfsd_file and netns were combined to avoid an extra indirect reference but that micro-optimization isn't possible now). This fixes xfstests generic/013 and it triggering: "Voluntary context switch within RCU read-side critical section!"	2024-12-29	5.5
CVE-2024-56744	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: f2fs: fix to avoid potential deadlock in f2fs_record_stop_reason()	2024-12-29	5.5

		syzbot reports deadlock issue of f2fs as below: === WARNING: possible circular locking dependency detected 6.12.0-rc3-syzkaller-00087-gc964ced77262 #0 Not tainted -- kswapd0/79 is trying to acquire lock: ffff888011824088 (&sbi->sb_lock){++++}-{3:3}, at: f2fs_down_write fs/f2fs/f2fs.h:2199 [inline] ffff888011824088 (&sbi->sb_lock){++++}-{3:3}, at: f2fs_record_stop_reason+0x52/0x1d0 fs/f2fs/super.c:4068 but task is already holding lock: ffff88804bd92610 (sb_internal#2){.+.+}-{0:0}, at: f2fs_evict_inode+0x662/0x15c0 fs/f2fs/inode.c:842 which lock already depends on the new lock.		
CVE-2024-56745	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: PCI: Fix reset_method_store() memory leak In reset_method_store(), a string is allocated via kstrndup() and assigned to the local "options". options is then used in with strsep() to find spaces: while ((name = strsep(&options, " ")) != NULL) { If there are no remaining spaces, then options is set to NULL by strsep(), so the subsequent kfree(options) doesn't free the memory allocated via kstrndup(). Fix by using a separate tmp_options to iterate with strsep() so options is preserved.	2024-12-29	5.5
CVE-2024-56746	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: fbdev: sh7760fb: Fix a possible memory leak in sh7760fb_alloc_mem() When information such as info->screen_base is not ready, calling sh7760fb_free_mem() does not release memory correctly. Call dma_free_coherent() instead.	2024-12-29	5.5
CVE-2024-56747	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: scsi: qedi: Fix a possible memory leak in qedi_alloc_and_init_sb() Hook "qedi_ops->common->sb_init = qed_sb_init" does not release the DMA memory sb_virt when it fails. Add dma_free_coherent() to free it. This is the same way as qedr_alloc_mem_sb() and qede_alloc_mem_sb().	2024-12-29	5.5
CVE-2024-56748	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: scsi: qedf: Fix a possible memory leak in qedf_alloc_and_init_sb() Hook "qed_ops->common->sb_init = qed_sb_init" does not release the DMA memory sb_virt when it fails. Add dma_free_coherent() to free it. This is the same way as qedr_alloc_mem_sb() and qede_alloc_mem_sb().	2024-12-29	5.5
CVE-2024-56749	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: dlm: fix dlm_recover_members refcount on error If dlm_recover_members() fails we don't drop the references of the previous created root_list that holds and keep all rsbs alive during the recovery. It might be not an unlikely event because ping_members() could run into an -EINTR if another recovery progress was triggered again.	2024-12-29	5.5
CVE-2024-56750	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: erofs: fix blksize < PAGE_SIZE for file-backed mounts Adjust sb->s_blocksize{,_bits} directly for file-backed mounts when the fs block size is smaller than PAGE_SIZE. Previously, EROFS used sb_set_blocksize(), which caused a panic if bdev-backed mounts is not used.	2024-12-29	5.5
CVE-2024-56751	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ipv6: release nexthop on device removal The CI is hitting some aperiodic hangup at device removal time in the pmtu.sh self-test: unregister_netdevice: waiting for veth_A-R1 to become free. Usage count = 6 ref_tracker: veth_A-R1@ffff888013df15d8 has 1/5 users at dst_init+0x84/0x4a0	2024-12-29	5.5

		dst_alloc+0x97/0x150 ip6_dst_alloc+0x23/0x90 ip6_rt_pcpu_alloc+0x1e6/0x520 ip6_pol_route+0x56f/0x840 fib6_rule_lookup+0x334/0x630 ip6_route_output_flags+0x259/0x480 ip6_dst_lookup_tail.constprop.0+0x5c2/0x940 ip6_dst_lookup_flow+0x88/0x190 udp_tunnel6_dst_lookup+0x2a7/0x4c0 vxlan_xmit_one+0xbde/0x4a50 [vxlan] vxlan_xmit+0x9ad/0xf20 [vxlan] dev_hard_start_xmit+0x10e/0x360 __dev_queue_xmit+0xf95/0x18c0 arp_solicit+0x4a2/0xe00 neigh_probe+0xaa/0xf0 While the first suspect is the dst_cache, explicitly tracking the dst owing the last device reference via probes proved such dst is held by the nexthop in the originating fib6_info. Similar to commit f5b51fe804ec ("ipv6: route: purge exception on removal"), we need to explicitly release the originating fib info when disconnecting a to-be-removed device from a live ipv6 dst: move the fib6_info cleanup into ip6_dst_ifdown(). Tested running: ./pmtu.sh cleanup_ipv6_exception in a tight loop for more than 400 iterations with no spat, running an unpatched kernel I observed a splat every ~10 iterations.		
CVE-2024-56752	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/nouveau/gr/gf100: Fix missing unlock in gf100_gr_chan_new() When the call to gf100_grctx_generate() fails, unlock gr->fecs.mutex before returning the error. Fixes smatch warning: drivers/gpu/drm/nouveau/nvkm/engine/gr/gf100.c:480 gf100_gr_chan_new() warn: inconsistent returns '&gr->fecs.mutex'.	2024-12-29	5.5
CVE-2024-56753	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/gfx9: Add Cleaner Shader Deinitialization in gfx_v9_0 Module This commit addresses an omission in the previous patch related to the cleaner shader support for GFX9 hardware. Specifically, it adds the necessary deinitialization code for the cleaner shader in the gfx_v9_0_sw_fini function. The added line amdgpu_gfx_cleaner_shader_sw_fini(adev); ensures that any allocated resources for the cleaner shader are freed correctly, avoiding potential memory leaks and ensuring that the GPU state is clean for the next initialization sequence.	2024-12-29	5.5
CVE-2024-56754	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: crypto: caam - Fix the pointer passed to caam_qi_shutdown() The type of the last parameter given to devm_add_action_or_reset() is "struct caam_drv_private *", but in caam_qi_shutdown(), it is casted to "struct device *". Pass the correct parameter to devm_add_action_or_reset() so that the resources are released as expected.	2024-12-29	5.5
CVE-2024-56755	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netfs/fscache: Add a memory barrier for FSCACHE_VOLUME_CREATING In fscache_create_volume(), there is a missing memory barrier between the bit-clearing operation and the wake-up operation. This may cause a situation where, after a wake-up, the bit-clearing operation hasn't been detected yet, leading to an indefinite wait. The triggering process is as follows: [cookie1] [cookie2] [volume_work] fscache_perform_lookup fscache_create_volume fscache_perform_lookup fscache_create_volume	2024-12-29	5.5

		fscache_create_volume_work cachefiles_acquire_volume clear_and_wake_up_bit test_and_set_bit test_and_set_bit goto maybe_wait goto no_wait In the above process, cookie1 and cookie2 has the same volume. When cookie1 enters the -no_wait- process, it will clear the bit and wake up the waiting process. If a barrier is missing, it may cause cookie2 to remain in the -wait- process indefinitely. In commit 3288666c7256 ("fscache: Use clear_and_wake_up_bit() in fscache_create_volume_work()"), barriers were added to similar operations in fscache_create_volume_work(), but fscache_create_volume() was missed. By combining the clear and wake operations into clear_and_wake_up_bit() to fix this issue.		
CVE-2024-56756	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: nvme-pci: fix freeing of the HMB descriptor table The HMB descriptor table is sized to the maximum number of descriptors that could be used for a given device, but __nvme_alloc_host_mem could break out of the loop earlier on memory allocation failure and end up using less descriptors than planned for, which leads to an incorrect size passed to dma_free_coherent. In practice this was not showing up because the number of descriptors tends to be low and the dma coherent allocator always allocates and frees at least a page.	2024-12-29	5.5
CVE-2022-49035	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: media: s5p_cec: limit msg.len to CEC_MAX_MSG_SIZE I expect that the hardware will have limited this to 16, but just in case it hasn't, check for this corner case.	2025-01-02	5.5
CVE-2024-53839	google - Android	In GetCellInfoList() of protocolnetadapter.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with baseband firmware compromise required. User Interaction is not needed for exploitation.	2025-01-03	5.5
CVE-2024-55896	ibm - i	IBM PowerHA SystemMirror for i 7.4 and 7.5 contains improper restrictions when rendering content via iFrames. This vulnerability could allow an attacker to gain improper access and perform unauthorized actions on the system.	2025-01-03	5.4
CVE-2024-56738	gnu - GRUB2	GNU GRUB (aka GRUB2) through 2.12 does not use a constant-time algorithm for grub_crypto_memcmp and thus allows side-channel attacks.	2024-12-29	5.3
CVE-2024-56729	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: smb: Initialize cfid->tcon before performing network ops Avoid leaking a tcon ref when a lease break races with opening the cached directory. Processing the leak break might take a reference to the tcon in cached_dir_lease_break() and then fail to release the ref in cached_dir_offload_close, since cfid->tcon is still NULL.	2024-12-29	4.7
CVE-2024-5591	ibm - Jazz Foundation	IBM Jazz Foundation 7.0.2, 7.0.3, and 7.1.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.	2025-01-03	4.3
CVE-2024-55897	ibm - i	IBM PowerHA SystemMirror for i 7.4 and 7.5 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic.	2025-01-03	4.3
CVE-2024-41780	ibm - Jazz Foundation	IBM Jazz Foundation 7.0.2, 7.0.3, and 7.1.0 could could allow a physical user to obtain sensitive information due to not masking passwords during entry.	2025-01-03	4.2

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.