الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

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

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 23rd of February to 1st of March. 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**

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

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 ٢٣ فبراير إلى ١ مارس. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2025-0159	IBM	IBM FlashSystem (IBM Storage Virtualize (8.5.0.0 through 8.5.0.13, 8.5.1.0, 8.5.2.0 through 8.5.2.3, 8.5.3.0 through 8.5.3.1, 8.5.4.0, 8.6.0.0 through 8.6.0.5, 8.6.1.0, 8.6.2.0 through 8.6.2.1, 8.6.3.0, 8.7.0.0 through 8.7.0.2, 8.7.1.0, 8.7.2.0 through 8.7.2.1) could allow a remote attacker to bypass RPCAdapter endpoint authentication by sending a specifically crafted HTTP request.	2025-02-28	9.1
CVE-2025-0975	IBM	IBM MQ 9.3 LTS, 9.3 CD, 9.4 LTS, and 9.4 CD console could allow an authenticated user to execute code due to improper neutralization of escape characters.	2025-02-28	8.8
CVE-2024-55898	IBM	IBM i 7.2, 7.3, 7.4, and 7.5 could allow a user with the capability to compile or restore a program to gain elevated privileges due to an unqualified library call. A malicious actor could cause user-controlled code to run with administrator privilege.	2025-02-24	8.5
CVE-2025-0160	IBM	IBM FlashSystem (IBM Storage Virtualize (8.5.0.0 through 8.5.0.13, 8.5.1.0, 8.5.2.0 through 8.5.2.3, 8.5.3.0 through 8.5.3.1, 8.5.4.0, 8.6.0.0 through 8.6.0.5, 8.6.1.0, 8.6.2.0 through 8.6.2.1, 8.6.3.0, 8.7.0.0 through 8.7.0.2, 8.7.1.0, 8.7.2.0 through 8.7.2.1) could allow a remote attacker with access to the system to execute arbitrary Java code due to improper restrictions in the RPCAdapter service.	2025-02-28	8.1
CVE-2023-52926	Linux	In the Linux kernel, the following vulnerability has been resolved: IORING_OP_READ did not correctly consume the provided buffer list when	2025-02-24	7.8
CVE-2021-47634	Linux	In the Linux kernel, the following vulnerability has been resolved: ubi: Fix race condition between ctrl_cdev_ioctl and ubi_cdev_ioctl	2025-02-26	7.8
CVE-2021-47639	Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: x86/mmu: Zap _all_ roots when unmapping gfn range in TDP MMU	2025-02-26	7.8
CVE-2021-47646	Linux	In the Linux kernel, the following vulnerability has been resolved: Revert "Revert "block, bfq: honor already-setup queue merges""	2025-02-26	7.8
CVE-2021-47653	Linux	In the Linux kernel, the following vulnerability has been resolved: media: davinci: vpif: fix use-after-free on driver unbind	2025-02-26	7.8
CVE-2021-47656	Linux	In the Linux kernel, the following vulnerability has been resolved: jffs2: fix use-after-free in jffs2_clear_xattr_subsystem	2025-02-26	7.8
CVE-2022-49047	Linux	In the Linux kernel, the following vulnerability has been resolved: ep93xx: clock: Fix UAF in ep93xx_clk_register_gate()	2025-02-26	7.8
CVE-2022-49053	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: target: tcmu: Fix possible page UAF	2025-02-26	7.8
CVE-2022-49059	Linux	In the Linux kernel, the following vulnerability has been resolved: nfc: nci: add flush_workqueue to prevent uaf	2025-02-26	7.8
CVE-2022-49063	Linux	In the Linux kernel, the following vulnerability has been resolved: ice: arfs: fix use-after-free when freeing @rx_cpu_rmap	2025-02-26	7.8

CVE-2022-49076	Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/hfi1: Fix use-after-free bug for mm struct	2025-02-26	7.8
CVE-2022-49078	Linux	In the Linux kernel, the following vulnerability has been resolved: lz4: fix LZ4_decompress_safe_partial read out of bound	2025-02-26	7.8
CVE-2022-49082	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: mpt3sas: Fix use after free in _scsih_expander_node_remove()	2025-02-26	7.8
CVE-2022-49085	Linux	In the Linux kernel, the following vulnerability has been resolved: drbd: Fix five use after free bugs in get_initial_state	2025-02-26	7.8
CVE-2022-49087	Linux	In the Linux kernel, the following vulnerability has been resolved: rxrpc: fix a race in rxrpc_exit_net()	2025-02-26	7.8
CVE-2022-49093	Linux	In the Linux kernel, the following vulnerability has been resolved: skbuff: fix coalescing for page_pool fragment recycling	2025-02-26	7.8
CVE-2022-49111	Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: Fix use after free in hci_send_acl	2025-02-26	7.8
CVE-2022-49114	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: libfc: Fix use after free in fc_exch_abts_resp()	2025-02-26	7.8
CVE-2022-49127	Linux	In the Linux kernel, the following vulnerability has been resolved: ref_tracker: implement use-after-free detection	2025-02-26	7.8
CVE-2022-49129	Linux	In the Linux kernel, the following vulnerability has been resolved: mt76: mt7921: fix crash when startup fails.	2025-02-26	7.8
CVE-2022-49136	Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_sync: Fix queuing commands when HCI_UNREGISTER is set	2025-02-26	7.8
CVE-2022-49168	Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: do not clean up repair bio if submit fails	2025-02-26	7.8
CVE-2022-49176	Linux	In the Linux kernel, the following vulnerability has been resolved: bfq: fix use-after-free in bfq_dispatch_request	2025-02-26	7.8
CVE-2022-49179	Linux	In the Linux kernel, the following vulnerability has been resolved: block, bfq: don't move oom_bfqq	2025-02-26	7.8
CVE-2022-49182	Linux	In the Linux kernel, the following vulnerability has been resolved: net: hns3: add vlan list lock to protect vlan list	2025-02-26	7.8
CVE-2022-49196	Linux	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries: Fix use after free in remove_phb_dynamic()	2025-02-26	7.8
CVE-2022-49223	Linux	In the Linux kernel, the following vulnerability has been resolved: cxl/port: Hold port reference until decoder release	2025-02-26	7.8
CVE-2022-49236	Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix UAF due to race between btf_try_get_module and load_module	2025-02-26	7.8
CVE-2022-49238	Linux	In the Linux kernel, the following vulnerability has been resolved: ath11k: free peer for station when disconnect from AP for QCA6390/WCN6855	2025-02-26	7.8
CVE-2022-49258	Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: ccree - Fix use after free in cc_cipher_exit()	2025-02-26	7.8
CVE-2022-49270	Linux	In the Linux kernel, the following vulnerability has been resolved: dm: fix use-after-free in dm_cleanup_zoned_dev()	2025-02-26	7.8
CVE-2022-49275	Linux	In the Linux kernel, the following vulnerability has been resolved: can: m_can: m_can_tx_handler(): fix use after free of skb	2025-02-26	7.8
CVE-2022-49287	Linux	In the Linux kernel, the following vulnerability has been resolved: tpm: fix reference counting for struct tpm_chip	2025-02-26	7.8
CVE-2022-49288	Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: Fix races among concurrent prealloc proc writes	2025-02-26	7.8
CVE-2022-49291	Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: Fix races among concurrent hw_params and hw_free calls	2025-02-26	7.8
CVE-2022-49328	Linux	In the Linux kernel, the following vulnerability has been resolved: mt76: fix use-after-free by removing a non-RCU wcid pointer	2025-02-26	7.8

CVE-2022-49349	Linux	In the Linux kernel, the following vulnerability has been resolved: ext4: fix use-after-free in ext4_rename_dir_prepare	2025-02-26	7.8
CVE-2022-49359	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/panfrost: Job should reference MMU not file_priv	2025-02-26	7.8
CVE-2022-49362	Linux	In the Linux kernel, the following vulnerability has been resolved: NFSD: Fix potential use-after-free in nfsd_file_put()	2025-02-26	7.8
CVE-2022-49377	Linux	In the Linux kernel, the following vulnerability has been resolved: blk-mq: don't touch ->tagset in blk_mq_get_sq_hctx	2025-02-26	7.8
CVE-2022-49385	Linux	In the Linux kernel, the following vulnerability has been resolved: driver: base: fix UAF when driver_attach failed	2025-02-26	7.8
CVE-2022-49388	Linux	In the Linux kernel, the following vulnerability has been resolved: ubi: ubi_create_volume: Fix use-after-free when volume creation failed	2025-02-26	7.8
CVE-2022-49390	Linux	In the Linux kernel, the following vulnerability has been resolved: macsec: fix UAF bug for real_dev	2025-02-26	7.8
CVE-2022-49411	Linux	In the Linux kernel, the following vulnerability has been resolved: bfq: Make sure bfqg for which we are queueing requests is online	2025-02-26	7.8
CVE-2022-49412	Linux	In the Linux kernel, the following vulnerability has been resolved: bfq: Avoid merging queues with different parents	2025-02-26	7.8
CVE-2022-49413	Linux	In the Linux kernel, the following vulnerability has been resolved: bfq: Update cgroup information before merging bio	2025-02-26	7.8
CVE-2022-49416	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mac80211: fix use-after-free in chanctx code	2025-02-26	7.8
CVE-2022-49419	Linux	In the Linux kernel, the following vulnerability has been resolved: video: fbdev: vesafb: Fix a use-after-free due early fb_info cleanup	2025-02-26	7.8
CVE-2022-49426	Linux	In the Linux kernel, the following vulnerability has been resolved: iommu/arm-smmu-v3-sva: Fix mm use-after-free	2025-02-26	7.8
CVE-2022-49464	Linux	In the Linux kernel, the following vulnerability has been resolved: erofs: fix buffer copy overflow of ztailpacking feature	2025-02-26	7.8
CVE-2022-49465	Linux	In the Linux kernel, the following vulnerability has been resolved: blk-throttle: Set BIO_THROTTLED when bio has been throttled	2025-02-26	7.8
CVE-2022-49470	Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btmtksdio: fix use-after-free at btmtksdio_recv_event	2025-02-26	7.8
CVE-2022-49474	Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: fix dangling sco_conn and use-after-free in sco_sock_timeout	2025-02-26	7.8
CVE-2022-49479	Linux	In the Linux kernel, the following vulnerability has been resolved: mt76: fix tx status related use-after-free race on station removal	2025-02-26	7.8
CVE-2022-49489	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/msm/disp/dpu1: set vbif hw config to NULL to avoid use after memory free during pm runtime resume	2025-02-26	7.8
CVE-2022-49493	Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: rt5645: Fix errorenous cleanup order	2025-02-26	7.8
CVE-2022-49501	Linux	In the Linux kernel, the following vulnerability has been resolved: usbnet: Run unregister_netdev() before unbind() again	2025-02-26	7.8
CVE-2022-49505	Linux	In the Linux kernel, the following vulnerability has been resolved: NFC: NULL out the dev->rfkill to prevent UAF	2025-02-26	7.8
CVE-2022-49524	Linux	In the Linux kernel, the following vulnerability has been resolved: media: pci: cx23885: Fix the error handling in cx23885_initdev()	2025-02-26	7.8
CVE-2022-49530	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: fix double free in si_parse_power_table()	2025-02-26	7.8
CVE-2022-49535	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Fix null pointer dereference after failing to issue FLOGI and PLOGI	2025-02-26	7.8
CVE-2022-49541	Linux	In the Linux kernel, the following vulnerability has been resolved: cifs: fix potential double free during failed mount	2025-02-26	7.8

CVE-2022-49548	Linux	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix potential array overflow in bpf_trampoline_get_progs()	2025-02-26	7.8
CVE-2022-49622	Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: avoid skb access on nf_stolen	2025-02-26	7.8
CVE-2022-49626	Linux	In the Linux kernel, the following vulnerability has been resolved: sfc: fix use after free when disabling sriov	2025-02-26	7.8
CVE-2022-49647	Linux	In the Linux kernel, the following vulnerability has been resolved: cgroup: Use separate src/dst nodes when preloading css_sets for migration	2025-02-26	7.8
CVE-2022-49651	Linux	In the Linux kernel, the following vulnerability has been resolved: srcu: Tighten cleanup_srcu_struct() GP checks	2025-02-26	7.8
CVE-2022-49667	Linux	In the Linux kernel, the following vulnerability has been resolved: net: bonding: fix use-after-free after 802.3ad slave unbind	2025-02-26	7.8
CVE-2022-49669	Linux	In the Linux kernel, the following vulnerability has been resolved: mptcp: fix race on unaccepted mptcp sockets	2025-02-26	7.8
CVE-2022-49685	Linux	In the Linux kernel, the following vulnerability has been resolved: iio: trigger: sysfs: fix use-after-free on remove	2025-02-26	7.8
CVE-2022-49694	Linux	In the Linux kernel, the following vulnerability has been resolved: block: disable the elevator int del_gendisk	2025-02-26	7.8
CVE-2022-49695	Linux	In the Linux kernel, the following vulnerability has been resolved: igb: fix a use-after-free issue in igb_clean_tx_ring	2025-02-26	7.8
CVE-2022-49696	Linux	In the Linux kernel, the following vulnerability has been resolved: tipc: fix use-after-free Read in tipc_named_reinit	2025-02-26	7.8
CVE-2022-49700	Linux	In the Linux kernel, the following vulnerability has been resolved: mm/slub: add missing TID updates on slab deactivation	2025-02-26	7.8
CVE-2022-49711	Linux	In the Linux kernel, the following vulnerability has been resolved: bus: fsl-mc-bus: fix KASAN use-after-free in fsl_mc_bus_remove()	2025-02-26	7.8
CVE-2022-49720	Linux	In the Linux kernel, the following vulnerability has been resolved: block: Fix handling of offline queues in blk_mq_alloc_request_hctx()	2025-02-26	7.8
CVE-2022-49730	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Resolve NULL ptr dereference after an ELS LOGO is aborted	2025-02-26	7.8
CVE-2024-57979	Linux	In the Linux kernel, the following vulnerability has been resolved: pps: Fix a use-after-free	2025-02-27	7.8
CVE-2024-57980	Linux	In the Linux kernel, the following vulnerability has been resolved: media: uvcvideo: Fix double free in error path	2025-02-27	7.8
CVE-2024-57983	Linux	In the Linux kernel, the following vulnerability has been resolved: mailbox: th1520: Fix memory corruption due to incorrect array size	2025-02-27	7.8
CVE-2024-57984	Linux	In the Linux kernel, the following vulnerability has been resolved: i3c: dw: Fix use-after-free in dw_i3c_master driver due to race condition	2025-02-27	7.8
CVE-2024-57990	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7925: fix off by one in mt7925_load_clc()	2025-02-27	7.8
CVE-2024-57995	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: fix read pointer after free in ath12k_mac_assign_vif_to_vdev()	2025-02-27	7.8
CVE-2025-21714	Linux	In the Linux kernel, the following vulnerability has been resolved: RDMA/mlx5: Fix implicit ODP use after free	2025-02-27	7.8
CVE-2025-21715	Linux	In the Linux kernel, the following vulnerability has been resolved: net: davicom: fix UAF in dm9000_drv_remove	2025-02-27	7.8
CVE-2025-21722	Linux	In the Linux kernel, the following vulnerability has been resolved: nilfs2: do not force clear folio if buffer is referenced	2025-02-27	7.8
CVE-2025-21726	Linux	In the Linux kernel, the following vulnerability has been resolved: padata: avoid UAF for reorder_work	2025-02-27	7.8
CVE-2025-21727	Linux	In the Linux kernel, the following vulnerability has been resolved: padata: fix UAF in padata_reorder	2025-02-27	7.8

CVE-2025-21729	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: fix race between cancel_hw_scan and hw_scan completion	2025-02-27	7.8
CVE-2025-21731	Linux	In the Linux kernel, the following vulnerability has been resolved: nbd: don't allow reconnect after disconnect	2025-02-27	7.8
CVE-2024-49570	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/tracing: Fix a potential TP_printk UAF	2025-02-27	7.8
CVE-2024-54458	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: bsg: Set bsg_queue to NULL after removal	2025-02-27	7.8
CVE-2024-58002	Linux	In the Linux kernel, the following vulnerability has been resolved: media: uvcvideo: Remove dangling pointers	2025-02-27	7.8
CVE-2024-58013	Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: MGMT: Fix slab-use-after-free Read in mgmt_remove_adv_monitor_sync	2025-02-27	7.8
CVE-2025-21735	Linux	In the Linux kernel, the following vulnerability has been resolved: NFC: nci: Add bounds checking in nci_hci_create_pipe()	2025-02-27	7.8
CVE-2025-21739	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Fix use-after free in init error and remove paths	2025-02-27	7.8
CVE-2025-21751	Linux	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: HWS, change error flow on matcher disconnect	2025-02-27	7.8
CVE-2025-21753	Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix use-after-free when attempting to join an aborted transaction	2025-02-27	7.8
CVE-2025-21756	Linux	In the Linux kernel, the following vulnerability has been resolved: vsock: Keep the binding until socket destruction	2025-02-27	7.8
CVE-2025-21759	Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: mcast: extend RCU protection in igmp6_send()	2025-02-27	7.8
CVE-2025-21760	Linux	In the Linux kernel, the following vulnerability has been resolved: ndisc: extend RCU protection in ndisc_send_skb()	2025-02-27	7.8
CVE-2025-21761	Linux	In the Linux kernel, the following vulnerability has been resolved: openvswitch: use RCU protection in ovs_vport_cmd_fill_info()	2025-02-27	7.8
CVE-2025-21762	Linux	In the Linux kernel, the following vulnerability has been resolved: arp: use RCU protection in arp_xmit()	2025-02-27	7.8
CVE-2025-21763	Linux	In the Linux kernel, the following vulnerability has been resolved: neighbour: use RCU protection in __neigh_notify()	2025-02-27	7.8
CVE-2025-21764	Linux	In the Linux kernel, the following vulnerability has been resolved: ndisc: use RCU protection in ndisc_alloc_skb()	2025-02-27	7.8
CVE-2025-21780	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: avoid buffer overflow attach in smu_sys_set_pp_table()	2025-02-27	7.8
CVE-2025-21785	Linux	In the Linux kernel, the following vulnerability has been resolved: arm64: cacheinfo: Avoid out-of-bounds write to cacheinfo array	2025-02-27	7.8
CVE-2025-21786	Linux	In the Linux kernel, the following vulnerability has been resolved: workqueue: Put the pwq after detaching the rescuer from the pool	2025-02-27	7.8
CVE-2025-21791	Linux	In the Linux kernel, the following vulnerability has been resolved: vrf: use RCU protection in l3mdev_l3_out()	2025-02-27	7.8
CVE-2025-21796	Linux	In the Linux kernel, the following vulnerability has been resolved: nfsd: clear acl_access/acl_default after releasing them	2025-02-27	7.8
CVE-2025-21797	Linux	In the Linux kernel, the following vulnerability has been resolved: HID: corsair-void: Add missing delayed work cancel for headset status	2025-02-27	7.8
CVE-2024-58034	Linux	In the Linux kernel, the following vulnerability has been resolved: memory: tegra20-emc: fix an OF node reference bug in tegra_emc_find_node_by_ram_code()	2025-02-27	7.8
CVE-2025-21811	Linux	In the Linux kernel, the following vulnerability has been resolved: nilfs2: protect access to buffers with no active references	2025-02-27	7.8
CVE-2025-21812	Linux	In the Linux kernel, the following vulnerability has been resolved: ax25: rcu protect dev->ax25_ptr	2025-02-27	7.8

CVE-2025-20111	Cisco	A vulnerability in the health monitoring diagnostics of Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an unauthenticated, adjacent attacker to cause the device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to the incorrect handling of specific Ethernet frames. An attacker could exploit this vulnerability by sending a sustained rate of crafted Ethernet frames to an affected device. A successful exploit could allow the attacker to cause the device to reload.	2025-02-26	7.4
CVE-2022-49551	Linux	In the Linux kernel, the following vulnerability has been resolved: usb: isp1760: Fix out-of-bounds array access	2025-02-26	7.1
CVE-2022-49560	Linux	In the Linux kernel, the following vulnerability has been resolved: exfat: check if cluster num is valid	2025-02-26	7.1
CVE-2024-57982	Linux	In the Linux kernel, the following vulnerability has been resolved: xfrm: state: fix out-of-bounds read during lookup	2025-02-27	7.1
CVE-2024-58007	Linux	In the Linux kernel, the following vulnerability has been resolved: soc: qcom: socinfo: Avoid out of bounds read of serial number	2025-02-27	7.1
CVE-2025-21741	Linux	In the Linux kernel, the following vulnerability has been resolved: usbnet: ipheth: fix DPE OoB read	2025-02-27	7.1
CVE-2025-21742	Linux	In the Linux kernel, the following vulnerability has been resolved: usbnet: ipheth: use static NDP16 location in URB	2025-02-27	7.1
CVE-2025-21743	Linux	In the Linux kernel, the following vulnerability has been resolved: usbnet: ipheth: fix possible overflow in DPE length check	2025-02-27	7.1
CVE-2025-21782	Linux	In the Linux kernel, the following vulnerability has been resolved: orangefs: fix a oob in orangefs_debug_write	2025-02-27	7.1
CVE-2025-21789	Linux	In the Linux kernel, the following vulnerability has been resolved: LoongArch: csum: Fix OoB access in IP checksum code for negative lengths	2025-02-27	7.1
CVE-2025-21794	Linux	In the Linux kernel, the following vulnerability has been resolved: HID: hid-thrustmaster: fix stack-out-of-bounds read in usb_check_int_endpoints()	2025-02-27	7.1
CVE-2025-21718	Linux	In the Linux kernel, the following vulnerability has been resolved: net: rose: fix timer races against user threads	2025-02-27	7
CVE-2024-54169	IBM	IBM EntireX 11.1 could allow an authenticated 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.	2025-02-27	6.5
CVE-2024-56340	IBM	IBM Cognos Analytics 11.2.0 through 11.2.4 FP5 is vulnerable to local file inclusion vulnerability, allowing an attacker to access sensitive files by inserting path traversal payloads inside the deficon parameter.	2025-02-28	6.5
CVE-2025-0823	IBM	IBM Cognos Analytics 11.2.0 through 11.2.4 FP5 and 12.0.0 through 12.0.4 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.	2025-02-28	6.5
CVE-2025-23225	IBM	IBM MQ 9.3 LTS, 9.3 CD, 9.4 LTS, and 9.4 CD could allow an authenticated user to cause a denial of service due to the improper handling of invalid headers sent to the queue.	2025-02-28	6.5
CVE-2025-0719	IBM	IBM Cloud Pak for Data 4.0.0 through 4.8.5 and 5.0.0 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-02-26	6.1
CVE-2024-5848	WSO2	A reflected cross-site scripting (XSS) vulnerability exists in multiple WSO2 products due to improper input validation. User-supplied data is directly included in server responses from vulnerable service endpoints without proper sanitization or encoding, allowing an attacker to inject malicious JavaScript. Successful exploitation could lead to UI manipulation, redirection to malicious websites, or data exfiltration from the browser. While session-related sensitive cookies are protected with the httpOnly flag, mitigating session hijacking risks, the impact may vary depending on gateway-level service restrictions.	2025-02-27	6.1
CVE-2025-20119	Cisco	A vulnerability in the system file permission handling of Cisco APIC could allow an authenticated, local attacker to overwrite critical system files, which could cause a DoS condition. To exploit this vulnerability, the attacker must have valid administrative credentials. This vulnerability is due to a race condition with handling system files. An attacker could exploit this vulnerability by doing specific operations on the file system. A successful exploit could allow the attacker to overwrite system files, which could lead to the device being in an inconsistent state and cause a DoS condition.	2025-02-26	6
CVE-2024-2321	WSO2	An incorrect authorization vulnerability exists in multiple WSO2 products, allowing protected APIs to be accessed directly using a refresh token instead of the expected access token. Due to improper authorization checks and token mapping, session cookies are not required for API access, potentially enabling unauthorized operations.	2025-02-27	5.6

		Exploitation requires an attacker to obtain a valid refresh token of an admin user. Since refresh tokens generally have a longer expiration time, this could lead to prolonged unauthorized access to API resources, impacting data confidentiality and integrity.		
CVE-2022-49527	Linux	In the Linux kernel, the following vulnerability has been resolved: media: venus: hfi: avoid null dereference in deinit	2025-02-26	5.5
CVE-2022-49529	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/pm: fix the null pointer while the smu is disabled	2025-02-26	5.5
CVE-2022-49532	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/virtio: fix NULL pointer dereference in virtio_gpu_conn_get_modes	2025-02-26	5.5
CVE-2022-49534	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Protect memory leak for NPIV ports sending PLOGI_RJT	2025-02-26	5.5
CVE-2022-49536	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Fix SCSI I/O completion and abort handler deadlock	2025-02-26	5.5
CVE-2022-49538	Linux	In the Linux kernel, the following vulnerability has been resolved: ALSA: jack: Access input_dev under mutex	2025-02-26	5.5
CVE-2022-49542	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: lpfc: Move cfg_log_verbose check before calling lpfc_dmp_dbg()	2025-02-26	5.5
CVE-2022-49544	Linux	In the Linux kernel, the following vulnerability has been resolved: ipw2x00: Fix potential NULL dereference in libipw_xmit()	2025-02-26	5.5
CVE-2022-49546	Linux	In the Linux kernel, the following vulnerability has been resolved: x86/kexec: fix memory leak of elf header buffer	2025-02-26	5.5
CVE-2022-49547	Linux	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix deadlock between concurrent dio writes when low on free data space	2025-02-26	5.5
CVE-2022-49549	Linux	In the Linux kernel, the following vulnerability has been resolved: x86/MCE/AMD: Fix memory leak when threshold_create_bank() fails	2025-02-26	5.5
CVE-2022-49550	Linux	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: provide block_invalidate_folio to fix memory leak	2025-02-26	5.5
CVE-2022-49563	Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: qat - add param check for RSA	2025-02-26	5.5
CVE-2022-49564	Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: qat - add param check for DH	2025-02-26	5.5
CVE-2022-49566	Linux	In the Linux kernel, the following vulnerability has been resolved: crypto: qat - fix memory leak in RSA	2025-02-26	5.5
CVE-2022-49567	Linux	In the Linux kernel, the following vulnerability has been resolved: mm/mempolicy: fix uninit-value in mpol_rebind_policy()	2025-02-26	5.5
CVE-2022-49568	Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: Don't null dereference ops->destroy	2025-02-26	5.5
CVE-2022-49569	Linux	In the Linux kernel, the following vulnerability has been resolved: spi: bcm2835: bcm2835_spi_handle_err(): fix NULL pointer deref for non DMA transfers	2025-02-26	5.5
CVE-2022-49570	Linux	In the Linux kernel, the following vulnerability has been resolved: gpio: gpio-xilinx: Fix integer overflow	2025-02-26	5.5
CVE-2022-49582	Linux	In the Linux kernel, the following vulnerability has been resolved: net: dsa: fix NULL pointer dereference in dsa_port_reset_vlan_filtering	2025-02-26	5.5
CVE-2022-49583	Linux	In the Linux kernel, the following vulnerability has been resolved: iavf: Fix handling of dummy receive descriptors	2025-02-26	5.5
CVE-2022-49591	Linux	In the Linux kernel, the following vulnerability has been resolved: net: dsa: microchip: ksz_common: Fix refcount leak bug	2025-02-26	5.5
CVE-2022-49717	Linux	In the Linux kernel, the following vulnerability has been resolved: irqchip/apple-aic: Fix refcount leak in build_fiq_affinity	2025-02-26	5.5
CVE-2022-49718	Linux	In the Linux kernel, the following vulnerability has been resolved: irqchip/apple-aic: Fix refcount leak in aic_of_ic_init	2025-02-26	5.5
CVE-2022-49719	Linux	In the Linux kernel, the following vulnerability has been resolved: irqchip/gic/realview: Fix refcount leak in realview_gic_of_init	2025-02-26	5.5

CVE-2022-49727	Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: Fix signed integer overflow in l2tp_ip6_sendmsg	2025-02-26	5.5
CVE-2022-49728	Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: Fix signed integer overflow in __ip6_append_data	2025-02-26	5.5
CVE-2022-49729	Linux	In the Linux kernel, the following vulnerability has been resolved: nfc: nfcmrvl: Fix memory leak in nfcmrvl_play_deferred	2025-02-26	5.5
CVE-2022-49731	Linux	In the Linux kernel, the following vulnerability has been resolved: ata: libata-core: fix NULL pointer deref in ata_host_alloc_pinfo()	2025-02-26	5.5
CVE-2024-57953	Linux	In the Linux kernel, the following vulnerability has been resolved: rtc: tps6594: Fix integer overflow on 32bit systems	2025-02-27	5.5
CVE-2024-57973	Linux	In the Linux kernel, the following vulnerability has been resolved: rdma/cxgb4: Prevent potential integer overflow on 32bit	2025-02-27	5.5
CVE-2024-57977	Linux	In the Linux kernel, the following vulnerability has been resolved: memcg: fix soft lockup in the OOM process	2025-02-27	5.5
CVE-2024-57978	Linux	In the Linux kernel, the following vulnerability has been resolved: media: imx-jpeg: Fix potential error pointer dereference in detach_pm()	2025-02-27	5.5
CVE-2024-57981	Linux	In the Linux kernel, the following vulnerability has been resolved: usb: xhci: Fix NULL pointer dereference on certain command aborts	2025-02-27	5.5
CVE-2024-57987	Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btrtl: check for NULL in btrtl_setup_realtek()	2025-02-27	5.5
CVE-2024-57988	Linux	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: btbcm: Fix NULL deref in btbcm_get_board_name()	2025-02-27	5.5
CVE-2024-57989	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7925: fix NULL deref check in mt7925_change_vif_links	2025-02-27	5.5
CVE-2024-57991	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: rtw89: chan: fix soft lockup in rtw89_entity_recalc_mgnt_roles()	2025-02-27	5.5
CVE-2024-57996	Linux	In the Linux kernel, the following vulnerability has been resolved: net_sched: sch_sfq: don't allow 1 packet limit	2025-02-27	5.5
CVE-2024-57997	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: wcn36xx: fix channel survey memory allocation size	2025-02-27	5.5
CVE-2025-21707	Linux	In the Linux kernel, the following vulnerability has been resolved: mptcp: consolidate suboption status	2025-02-27	5.5
CVE-2025-21711	Linux	In the Linux kernel, the following vulnerability has been resolved: net/rose: prevent integer overflows in rose_setsockopt()	2025-02-27	5.5
CVE-2025-21713	Linux	In the Linux kernel, the following vulnerability has been resolved: powerpc/pseries/iommu: Don't unset window if it was never set	2025-02-27	5.5
CVE-2025-21716	Linux	In the Linux kernel, the following vulnerability has been resolved: vxlan: Fix uninit-value in vxlan_vnifilter_dump()	2025-02-27	5.5
CVE-2025-21723	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: mpi3mr: Fix possible crash when setting up bsg fails	2025-02-27	5.5
CVE-2024-52557	Linux	In the Linux kernel, the following vulnerability has been resolved: drm: zynqmp_dp: Fix integer overflow in zynqmp_dp_rate_get()	2025-02-27	5.5
CVE-2024-52559	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/msm/gem: prevent integer overflow in msm_ioctl_gem_submit()	2025-02-27	5.5
CVE-2024-57834	Linux	In the Linux kernel, the following vulnerability has been resolved: media: vidtv: Fix a null-ptr-deref in vidtv_mux_stop_thread	2025-02-27	5.5
CVE-2024-58005	Linux	In the Linux kernel, the following vulnerability has been resolved: tpm: Change to kvalloc() in eventlog/acpi.c	2025-02-27	5.5
CVE-2024-58010	Linux	In the Linux kernel, the following vulnerability has been resolved: binfmt_flat: Fix integer overflow bug on 32 bit systems	2025-02-27	5.5
CVE-2024-58011	Linux	In the Linux kernel, the following vulnerability has been resolved: platform/x86: int3472: Check for adev == NULL	2025-02-27	5.5

CVE-2024-58012	Linux	In the Linux kernel, the following vulnerability has been resolved: ASoC: SOF: Intel: hda-dai: Ensure DAI widget is valid during params	2025-02-27	5.5
CVE-2024-58017	Linux	In the Linux kernel, the following vulnerability has been resolved: printk: Fix signed integer overflow when defining LOG_BUF_LEN_MAX	2025-02-27	5.5
CVE-2024-58020	Linux	In the Linux kernel, the following vulnerability has been resolved: HID: multitouch: Add NULL check in mt_input_configured	2025-02-27	5.5
CVE-2024-58021	Linux	In the Linux kernel, the following vulnerability has been resolved: HID: winwing: Add NULL check in winwing_init_led()	2025-02-27	5.5
CVE-2025-21736	Linux	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix possible int overflows in nilfs_fiemap()	2025-02-27	5.5
CVE-2025-21737	Linux	In the Linux kernel, the following vulnerability has been resolved: ceph: fix memory leak in ceph_mds_auth_match()	2025-02-27	5.5
CVE-2025-21740	Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: x86/mmu: Ensure NX huge page recovery thread is alive before waking	2025-02-27	5.5
CVE-2025-21744	Linux	In the Linux kernel, the following vulnerability has been resolved: wifi: brcmfmac: fix NULL pointer dereference in brcmf_txfinalize()	2025-02-27	5.5
CVE-2025-21745	Linux	In the Linux kernel, the following vulnerability has been resolved: blk-cgroup: Fix class @block_class's subsystem refcount leakage	2025-02-27	5.5
CVE-2025-21748	Linux	In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix integer overflows on 32 bit systems	2025-02-27	5.5
CVE-2025-21749	Linux	In the Linux kernel, the following vulnerability has been resolved: net: rose: lock the socket in rose_bind()	2025-02-27	5.5
CVE-2025-21755	Linux	In the Linux kernel, the following vulnerability has been resolved: vsock: Orphan socket after transport release	2025-02-27	5.5
CVE-2025-21769	Linux	In the Linux kernel, the following vulnerability has been resolved: ptp: vmclock: Add .owner to vmclock_miscdev_fops	2025-02-27	5.5
CVE-2025-21770	Linux	In the Linux kernel, the following vulnerability has been resolved: iommu: Fix potential memory leak in iopf_queue_remove_device()	2025-02-27	5.5
CVE-2025-21773	Linux	In the Linux kernel, the following vulnerability has been resolved: can: etas_es58x: fix potential NULL pointer dereference on udev->serial	2025-02-27	5.5
CVE-2025-21774	Linux	In the Linux kernel, the following vulnerability has been resolved: can: rockchip: rkcanfd_handle_rx_fifo_overflow_int(): bail out if skb cannot be allocated	2025-02-27	5.5
CVE-2025-21775	Linux	In the Linux kernel, the following vulnerability has been resolved: can: ctucanfd: handle skb allocation failure	2025-02-27	5.5
CVE-2025-21776	Linux	In the Linux kernel, the following vulnerability has been resolved: USB: hub: Ignore non-compliant devices with too many configs or interfaces	2025-02-27	5.5
CVE-2025-21779	Linux	In the Linux kernel, the following vulnerability has been resolved: KVM: x86: Reject Hyper-V's SEND_IPI hypercalls if local APIC isn't in-kernel	2025-02-27	5.5
CVE-2025-21783	Linux	In the Linux kernel, the following vulnerability has been resolved: gpiolib: Fix crash on error in gpiochip_get_ngpios()	2025-02-27	5.5
CVE-2025-21787	Linux	In the Linux kernel, the following vulnerability has been resolved: team: better TEAM_OPTION_TYPE_STRING validation	2025-02-27	5.5
CVE-2025-21788	Linux	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: ti: am65-cpsw: fix memleak in certain XDP cases	2025-02-27	5.5
CVE-2025-21790	Linux	In the Linux kernel, the following vulnerability has been resolved: vxlan: check vxlan_vnigroup_init() return value	2025-02-27	5.5
CVE-2025-21792	Linux	In the Linux kernel, the following vulnerability has been resolved: ax25: Fix refcount leak caused by setting SO_BINDTODEVICE sockopt	2025-02-27	5.5
CVE-2025-21793	Linux	In the Linux kernel, the following vulnerability has been resolved: spi: sn-f-ospi: Fix division by zero	2025-02-27	5.5
CVE-2024-54170	IBM	IBM EntireX 11.1 could allow a local user to cause a denial of service due to use of a regular expression with an inefficient complexity that consumes excessive CPU cycles.	2025-02-27	5.5

CVE-2024-58022	Linux	In the Linux kernel, the following vulnerability has been resolved: mailbox: th1520: Fix a NULL vs IS_ERR() bug	2025-02-27	5.5
CVE-2024-58042	Linux	In the Linux kernel, the following vulnerability has been resolved: rhashtable: Fix potential deadlock by moving schedule_work outside lock	2025-02-27	5.5
CVE-2025-21798	Linux	In the Linux kernel, the following vulnerability has been resolved: firewire: test: Fix potential null dereference in firewire kunit test	2025-02-27	5.5
CVE-2025-21809	Linux	In the Linux kernel, the following vulnerability has been resolved: rxrpc, afs: Fix peer hash locking vs RCU callback	2025-02-27	5.5
CVE-2025-21814	Linux	In the Linux kernel, the following vulnerability has been resolved: ptp: Ensure info->enable callback is always set	2025-02-27	5.5
CVE-2025-21820	Linux	In the Linux kernel, the following vulnerability has been resolved: tty: xilinx_uartps: split sysrq handling	2025-02-27	5.5
CVE-2025-21824	Linux	In the Linux kernel, the following vulnerability has been resolved: gpu: host1x: Fix a use of uninitialized mutex	2025-02-27	5.5
CVE-2024-54175	IBM	IBM MQ 9.3 LTS, 9.3 CD, 9.4 LTS, and 9.4 CD could allow a local user to cause a denial of service due to an improper check for unusual or exceptional conditions.	2025-02-28	5.5
CVE-2025-0985	IBM	IBM MQ 9.3 LTS, 9.3 CD, 9.4 LTS, and 9.4 CD stores potentially sensitive information in environment variables that could be obtained by a local user.	2025-02-28	5.5
CVE-2024-0392	WSO2	A Cross-Site Request Forgery (CSRF) vulnerability exists in the management console of WSO2 Enterprise Integrator 6.6.0 due to the absence of CSRF token validation. This flaw allows attackers to craft malicious requests that can trigger state-changing operations on behalf of an authenticated user, potentially compromising account settings and data integrity. The vulnerability only affects a limited set of state-changing operations, and successful exploitation requires social engineering to trick a user with access to the management console into performing the malicious action.	2025-02-27	5.4
CVE-2024-41778	IBM	IBM Controller 11.0.0 through 11.0.1 and 11.1.0 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts.	2025-03-01	5.3
CVE-2025-1800	D-Link	A vulnerability has been found in D-Link DAR-7000 3.2 and classified as critical. This vulnerability affects the function get_ip_addr_details of the file /view/vpn/sxh_vpn/sxh_vpnlic.php of the component HTTP POST Request Handler. The manipulation of the argument ethname leads to command injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-03-01	5.3
CVE-2025-20117	Cisco	A vulnerability in the CLI of Cisco APIC could allow an authenticated, local attacker to execute arbitrary commands as root&nbsp;on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials. This vulnerability is due to insufficient validation of arguments that are passed to specific CLI commands. An attacker could exploit this vulnerability by including crafted input as the argument of an affected CLI command. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with the privileges of root.	2025-02-26	5.1
CVE-2025-20161	Cisco	A vulnerability in the software upgrade process of Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode could allow an authenticated, local attacker with valid Administrator credentials to execute a command injection attack on the underlying operating system of an affected device. This vulnerability is due to insufficient validation of specific elements within a software image. An attacker could exploit this vulnerability by installing a crafted image. A successful exploit could allow the attacker to execute arbitrary commands on the underlying operating system with root privileges.&nbsp; Note: Administrators should validate the hash of any software image before installation.	2025-02-26	5.1
CVE-2025-20116	Cisco	A vulnerability in the web UI of Cisco APIC could allow an authenticated, remote attacker to perform a stored XSS attack on an affected system. To exploit this vulnerability, the attacker must have valid administrative credentials. This vulnerability is due to improper input validation in the web UI. An authenticated attacker could exploit this vulnerability by injecting malicious code into specific pages of the web UI. A successful exploit could allow the attacker to execute arbitrary script code in the context of the web UI or access sensitive, browser-based information.	2025-02-26	4.8
CVE-2022-49571	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix data-races around sysctl_tcp_max_reordering.	2025-02-26	4.7

CVE-2022-49572	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix data-races around sysctl_tcp_slow_start_after_idle.	2025-02-26	4.7
CVE-2022-49573	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix a data-race around sysctl_tcp_early_retrans.	2025-02-26	4.7
CVE-2022-49574	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix data-races around sysctl_tcp_recovery.	2025-02-26	4.7
CVE-2022-49575	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix a data-race around sysctl_tcp_thin_linear_timeouts.	2025-02-26	4.7
CVE-2022-49576	Linux	In the Linux kernel, the following vulnerability has been resolved: ipv4: Fix data-races around sysctl_fib_multipath_hash_fields.	2025-02-26	4.7
CVE-2022-49577	Linux	In the Linux kernel, the following vulnerability has been resolved: udp: Fix a data-race around sysctl_udp_l3mdev_accept.	2025-02-26	4.7
CVE-2022-49578	Linux	In the Linux kernel, the following vulnerability has been resolved: ip: Fix data-races around sysctl_ip_prot_sock.	2025-02-26	4.7
CVE-2022-49579	Linux	In the Linux kernel, the following vulnerability has been resolved: ipv4: Fix data-races around sysctl_fib_multipath_hash_policy.	2025-02-26	4.7
CVE-2022-49580	Linux	In the Linux kernel, the following vulnerability has been resolved: ipv4: Fix a data-race around sysctl_fib_multipath_use_neigh.	2025-02-26	4.7
CVE-2022-49585	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix data-races around sysctl_tcp_fastopen_blackhole_timeout.	2025-02-26	4.7
CVE-2022-49586	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix data-races around sysctl_tcp_fastopen.	2025-02-26	4.7
CVE-2022-49587	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix a data-race around sysctl_tcp_notsent_lowat.	2025-02-26	4.7
CVE-2022-49588	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix data-races around sysctl_tcp_migrate_req.	2025-02-26	4.7
CVE-2022-49589	Linux	In the Linux kernel, the following vulnerability has been resolved: igmp: Fix data-races around sysctl_igmp_qrv.	2025-02-26	4.7
CVE-2022-49590	Linux	In the Linux kernel, the following vulnerability has been resolved: igmp: Fix data-races around sysctl_igmp_llm_reports.	2025-02-26	4.7
CVE-2022-49593	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix a data-race around sysctl_tcp_probe_interval.	2025-02-26	4.7
CVE-2022-49594	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix a data-race around sysctl_tcp_mtu_probe_floor.	2025-02-26	4.7
CVE-2022-49595	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix a data-race around sysctl_tcp_probe_threshold.	2025-02-26	4.7
CVE-2022-49596	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix data-races around sysctl_tcp_min_snd_mss.	2025-02-26	4.7
CVE-2022-49597	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix data-races around sysctl_tcp_base_mss.	2025-02-26	4.7
CVE-2022-49598	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix data-races around sysctl_tcp_mtu_probing.	2025-02-26	4.7
CVE-2022-49599	Linux	In the Linux kernel, the following vulnerability has been resolved: tcp: Fix data-races around sysctl_tcp_l3mdev_accept.	2025-02-26	4.7
CVE-2024-54173	IBM	IBM MQ 9.3 LTS, 9.3 CD, 9.4 LTS, and 9.4 CD reveals potentially sensitive information in trace files that could be read by a local user when webconsole trace is enabled.	2025-02-28	4.7
CVE-2025-20118	Cisco	A vulnerability in the implementation of the internal system processes of Cisco APIC could allow an authenticated, local attacker to access sensitive information on an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials. This vulnerability is due to insufficient masking of sensitive information that is displayed through system CLI commands. An attacker could exploit this vulnerability by using reconnaissance techniques at the device CLI. A successful exploit could allow the attacker to access sensitive information on an affected device that could be used for additional attacks.	2025-02-26	4.4

CVE-2024-56493	IBM	IBM EntireX 11.1 could allow a local user to obtain sensitive information when a detailed technical error message is returned. This information could be used in further attacks against the system.	2025-02-27	3.3
CVE-2024-56494	IBM	IBM EntireX 11.1 could allow a local user to obtain sensitive information when a detailed technical error message is returned. This information could be used in further attacks against the system.	2025-02-27	3.3
CVE-2024-56495	IBM	IBM EntireX 11.1 could allow a local user to obtain sensitive information when a detailed technical error message is returned. This information could be used in further attacks against the system.	2025-02-27	3.3
CVE-2024-56496	IBM	IBM EntireX 11.1 could allow a local user to obtain sensitive information when a detailed technical error message is returned. This information could be used in further attacks against the system.	2025-02-27	3.3
CVE-2024-56810	IBM	IBM EntireX 11.1 could allow a local user to obtain sensitive information when a detailed technical error message is returned. This information could be used in further attacks against the system.	2025-02-27	3.3
CVE-2024-56811	IBM	IBM EntireX 11.1 could allow a local user to obtain sensitive information when a detailed technical error message is returned. This information could be used in further attacks against the system.	2025-02-27	3.3
CVE-2024-56812	IBM	IBM EntireX 11.1 could allow a local user to obtain sensitive information when a detailed technical error message is returned. This information could be used in further attacks against the system.	2025-02-27	3.3
CVE-2025-0759	IBM	IBM EntireX 11.1 could allow a local user to unintentionally modify data timestamp integrity due to improper shared resource synchronization.	2025-02-27	3.3
CVE-2024-51539	Dell	The Dell Secure Connect Gateway (SCG) Application and Appliance, versions prior to 5.28, contains a SQL injection vulnerability due to improper neutralization of special elements used in an SQL command. This vulnerability can only be exploited locally on the affected system. A high-privilege attacker with access to the system could potentially exploit this vulnerability, leading to the disclosure of non-sensitive information that does not include any customer data.	2025-02-25	2.3

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.