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 ١ ديسمبر إلى ٧ ديسمبر. 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 1st of December to 7th of December. 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-2018-9416	google - Android	In sg_remove_scat of scsi/sg.c, there is a possible memory corruption due to an unusual root cause. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	10
CVE-2018-9430	google - Android	In prop2cfg of btif_storage.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-12-02	9.8
CVE-2024-52335	siemens - syngo.plaza VB30E	A vulnerability has been identified in syngo.plaza VB30E (All versions < VB30E_HF05). The affected application do not properly sanitize input data before sending it to the SQL server. This could allow an attacker with access to the application could use this vulnerability to execute malicious SQL commands to compromise the whole database.	2024-12-06	9.3
CVE-2018-9380	google - Android	In l2c_lcc_proc_pdu of l2c_fcr.cc, there is a possible out of bounds write due to improper input validation. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2024-12-02	8.8
CVE-2018-9418	google - Android	In handle_app_cur_val_response of dtif_rc.cc, there is a possible stack buffer overflow 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.	2024-12-02	8.8
CVE-2024-12053	google - Chrome	Type Confusion in V8 in Google Chrome prior to 131.0.6778.108 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	2024-12-03	8.8
CVE-2024-40717	veeam - Backup & Replication	A vulnerability in Veeam Backup & Replication allows a low-privileged user with certain roles to perform remote code execution (RCE) by updating existing jobs. These jobs can be configured to run pre- and post-scripts, which can be located on a network share and are executed with elevated privileges by default. The user can update a job and schedule it to run almost immediately, allowing arbitrary code execution on the server.	2024-12-04	8.8
CVE-2024-42452	veeam - Backup & Replication	A vulnerability in Veeam Backup & Replication allows a low-privileged user to start an agent remotely in server mode and obtain credentials, effectively escalating privileges to system-level access. This allows the attacker to upload files to the server with elevated privileges. The vulnerability exists because remote calls bypass permission checks, leading to full system compromise.	2024-12-04	8.8
CVE-2024-42456	veeam - Backup & Replication	A vulnerability in Veeam Backup & Replication platform allows a low-privileged user with a specific role to exploit a method that updates critical configuration settings, such as modifying the trusted client certificate used for authentication on a specific port. This can result in unauthorized access, enabling the user to call privileged methods and initiate critical services. The issue arises due to insufficient permission requirements on the method, allowing users with low privileges to perform actions that should require higher-level permissions.	2024-12-04	8.8
CVE-2024-51465	ibm - App Connect Enterprise Certified Container	IBM App Connect Enterprise Certified Container 11.4, 11.5, 11.6, 12.0, 12.1, 12.2, and 12.3 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request.	2024-12-04	8.8
CVE-2018-9402	google - Android	In multiple functions of gl_proc.c, there is a buffer overwrite due to a missing bounds check. This could lead to escalation of privileges in the kernel.	2024-12-05	8.8
CVE-2024-11148	openbsd - OpenBSD	In OpenBSD 7.4 before errata 006 and OpenBSD 7.3 before errata 020, httpd(8) is vulnerable to a NULL dereference when handling a malformed fastcgi request.	2024-12-05	8.7

CVE-2024-54126	tp-link - Archer C50 Wireless Router	This vulnerability exists in the TP-Link Archer C50 due to improper signature verification mechanism in the firmware upgrade process at its web interface. An attacker with administrative privileges within the router's Wi-Fi range could exploit this vulnerability by uploading and executing malicious firmware which could lead to complete compromise of the targeted device.	2024-12-05	8.5
CVE-2024-33044	qualcomm - 315_5g_iot_modem_firmware	Memory corruption while Configuring the SMR/S2CR register in Bypass mode.	2024-12-02	8.4
CVE-2024-33056	qualcomm - 315_5g_iot_modem_firmware	Memory corruption when allocating and accessing an entry in an SMEM partition continuously.	2024-12-02	8.4
CVE-2024-42422	dell - NetWorker	Dell NetWorker, version(s) 19.10, contain(s) an Authorization Bypass Through User-Controlled Key vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	2024-12-03	8.3
CVE-2022-41137	apache software foundation - Apache Hive	Apache Hive Metastore (HMS) uses SerializationUtilities#deserializeObjectWithTypeInformation method when filtering and fetching partitions that is unsafe and can lead to Remote Code Execution (RCE) since it allows the deserialization of arbitrary data. In real deployments, the vulnerability can be exploited only by authenticated users/clients that were able to successfully establish a connection to the Metastore. From an API perspective any code that calls the unsafe method may be vulnerable unless it performs additional prerechecks on the input arguments.	2024-12-05	8.3
CVE-2024-45106	apache software foundation - Apache Ozone	Improper authentication of an HTTP endpoint in the S3 Gateway of Apache Ozone 1.4.0 allows any authenticated Kerberos user to revoke and regenerate the S3 secrets of any other user. This is only possible if: * ozone.s3g.secret.http.enabled is set to true. The default value of this configuration is false. * The user configured in ozone.s3g.kerberos.principal is also configured in ozone.s3.administrators or ozone.administrators. Users are recommended to upgrade to Apache Ozone version 1.4.1 which disables the affected endpoint.	2024-12-03	8.1
CVE-2024-11398	synology - Synology Router Manager (SRM)	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in OTP reset functionality in Synology Router Manager (SRM) before 1.3.1-9346-9 allows remote authenticated users to delete arbitrary files via unspecified vectors.	2024-12-04	8.1
CVE-2024-45318	sonicwall - SMA100	A vulnerability in the SonicWall SMA100 SSLVPN web management interface allows remote attackers to cause Stack-based buffer overflow and potentially lead to code execution.	2024-12-05	8.1
CVE-2024-53703	sonicwall - SMA100	A vulnerability in the SonicWall SMA100 SSLVPN firmware 10.2.1.13-72sv and earlier versions mod_httprp library loaded by the Apache web server allows remote attackers to cause Stack-based buffer overflow and potentially lead to code execution.	2024-12-05	8.1
CVE-2018-9413	google - Android	In handle_notification_response of btif_rc.cc, 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 needed for exploitation.	2024-12-02	8.0
CVE-2024-40691	ibm - multiple products	IBM Cognos Controller 11.0.0 and 11.0.1 could be vulnerable to malicious file upload by not validating the content of the file uploaded to the web interface. Attackers can make use of this weakness and upload malicious executable files into the system, and it can be sent to victim for performing further attacks.	2024-12-03	8.0
CVE-2024-53104	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: media: uvcvideo: Skip parsing frames of type UVC_VS_UNDEFINED in uvc_parse_format This can lead to out of bounds writes since frames of this type were not taken into account when calculating the size of the frames buffer in uvc_parse_streaming.	2024-12-02	7.8
CVE-2024-43048	qualcomm - fastconnect_6200_firmware	Memory corruption when invalid input is passed to invoke GPU Headroom API call.	2024-12-02	7.8
CVE-2024-43049	qualcomm - fastconnect_6700_firmware	Memory corruption while invoking IOCTL calls from user space to set generic private command inside WLAN driver.	2024-12-02	7.8
CVE-2024-43050	qualcomm - aqt1000_firmware	Memory corruption while invoking IOCTL calls from user space to issue factory test command inside WLAN driver.	2024-12-02	7.8
CVE-2024-43052	qualcomm - apq8017_firmware	Memory corruption while processing API calls to NPU with invalid input.	2024-12-02	7.8
CVE-2024-43053	qualcomm - fastconnect_6700_firmware	Memory corruption while invoking IOCTL calls from user space to read WLAN target diagnostic information.	2024-12-02	7.8
CVE-2018-9376	google - Android	In rpc_msg_handler and related handlers of drivers/misc/mediatek/eccci/port_rpc.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-02	7.8
CVE-2018-9414	google - Android	In gattServerSendResponseNative of com_android_bluetooth_gatt.cpp, there is a possible out of bounds stack write due to a missing bounds check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	2024-12-02	7.8
CVE-2018-9431	google - Android	In OSUInfo of OSUInfo.java, there is a possible escalation of privilege 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.	2024-12-02	7.8
CVE-2024-47476	dell - NetWorker Management Console	Dell NetWorker Management Console, version(s) 19.11, contain(s) an Improper Verification of Cryptographic Signature vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to Code execution.	2024-12-03	7.8
CVE-2024-53126	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: vdpa: solidrun: Fix UB bug with devres	2024-12-04	7.8

		In psnet_open_pf_bar() and snet_open_vf_bar() a string later passed to pcim_iomap_regions() is placed on the stack. Neither pcim_iomap_regions() nor the functions it calls copy that string. Should the string later ever be used, this, consequently, causes undefined behavior since the stack frame will by then have disappeared. Fix the bug by allocating the strings on the heap through devm_kasprintf().		
CVE-2024-53133	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Handle dml allocation failure to avoid crash [Why] In the case where a dml allocation fails for any reason, the current state's dml contexts would no longer be valid. Then subsequent calls dc_state_copy_internal would shallow copy invalid memory and if the new state was released, a double free would occur. [How] Reset dml pointers in new_state to NULL and avoid invalid pointer (cherry picked from commit bcafdc61529a48f6f06355d78eb41b3aeda5296c)	2024-12-04	7.8
CVE-2024-53139	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: sctp: fix possible UAF in sctp_v6_available() A lockdep report [1] with CONFIG_PROVE_RCU_LIST=y hints that sctp_v6_available() is calling dev_get_by_index_rcu() and ipv6_chk_addr() without holding rcu. [1] ============================= WARNING: suspicious RCU usage 6.12.0-rc5-virtme #1216 Tainted: G W ----------------------------- net/core/dev.c:876 RCU-list traversed in non-reader section!! other info that might help us debug this: rcu_scheduler_active = 2, debug_locks = 1 1 lock held by sctp_hello/31495: #0: ffff9f1ebbdb7418 (sk_lock-AF_INET6){+.+.}-{0:0}, at: sctp_bind (./arch/x86/include/asm/jump_label.h:27 net/sctp/socket.c:315) sctp stack backtrace: CPU: 7 UID: 0 PID: 31495 Comm: sctp_hello Tainted: G W 6.12.0-rc5-virtme #1216 Tainted: [W]=WARN Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:123) lockdep_rcu_suspicious (kernel/locking/lockdep.c:6822) dev_get_by_index_rcu (net/core/dev.c:876 (discriminator 7)) sctp_v6_available (net/sctp/ipv6.c:701) sctp sctp_do_bind (net/sctp/socket.c:400 (discriminator 1)) sctp sctp_bind (net/sctp/socket.c:320) sctp inet6_bind_sk (net/ipv6/af_inet6.c:465) ? security_socket_bind (security/security.c:4581 (discriminator 1)) __sys_bind (net/socket.c:1848 net/socket.c:1869) ? do_user_addr_fault (./include/linux/rcupdate.h:347 ./include/linux/rcupdate.h:880 ./include/linux/mm.h:729 arch/x86/mm/fault.c:1340) ? do_user_addr_fault (./arch/x86/include/asm/preempt.h:84 (discriminator 13) ./include/linux/rcupdate.h:98 (discriminator 13) ./include/linux/rcupdate.h:882 (discriminator 13) ./include/linux/mm.h:729 (discriminator 13) arch/x86/mm/fault.c:1340 (discriminator 13)) __x64_sys_bind (net/socket.c:1877 (discriminator 1) net/socket.c:1875 (discriminator 1) net/socket.c:1875 (discriminator 1)) do_syscall_64 (arch/x86/entry/common.c:52 (discriminator 1) arch/x86/entry/common.c:83 (discriminator 1)) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) RIP: 0033:0x7f59b934a1e7 Code: 44 00 00 48 8b 15 39 8c 0c 00 f7 d8 64 89 02 b8 ff ff ff ff eb bd 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 b8 31 00 00 00 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 8b 0d 09 8c 0c 00 f7 d8 64 89 01 48 All code ======== 0: 44 00 00 add %r8b,(%rax) 3: 48 8b 15 39 8c 0c 00 mov 0xc8c39(%rip),%rdx # 0xc8c43	2024-12-04	7.8

		a: f7 d8 neg %eax c: 64 89 02 mov %eax,%fs:(%rdx) f: b8 ff ff ff ff mov $0xffffffff,%eax 14: eb bd jmp 0xffffffffffffffd3 16: 66 2e 0f 1f 84 00 00 cs nopw 0x0(%rax,%rax,1) 1d: 00 00 00 20: 0f 1f 00 nopl (%rax) 23: b8 31 00 00 00 mov $0x31,%eax 28: 0f 05 syscall 2a:* 48 3d 01 f0 ff ff cmp $0xfffffffffffff001,%rax <-- trapping instruction 30: 73 01 jae 0x33 32: c3 ret 33: 48 8b 0d 09 8c 0c 00 mov 0xc8c09(%rip),%rcx # 0xc8c43 3a: f7 d8 neg %eax 3c: 64 89 01 mov %eax,%fs:(%rcx) 3f: 48 rex.W Code starting with the faulting instruction ========== 0: 48 3d 01 f0 ff ff cmp $0xfffffffffffff001,%rax 6: 73 01 jae 0x9 8: c3 ret 9: 48 8b 0d 09 8c 0c 00 mov 0xc8c09(%rip),%rcx # 0xc8c19 10: f7 d8 neg %eax 12: 64 89 01 mov %eax,%fs:(%rcx) 15: 48 rex.W RSP: 002b:00007ffe2d0ad398 EFLAGS: 00000202 ORIG_RAX: 0000000000000031 RAX: ffffffffffffffda RBX: 00007ffe2d0ad3d0 RCX: 00007f59b934a1e7 RDX: 000000000000001c RSI: 00007ffe2d0ad3d0 RDI: 0000000000000005 RBP: 0000000000000005 R08: 1999999999999999 R09: 0000000000000000 R10: 00007f59b9253298 R11: 000000000000 ---truncated---		
CVE-2018-9392	google - Android	In get_binary of vendor/mediatek/proprietary/hardware/connectivity/gps/gps_hal/src/data_coder.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-04	7.8
CVE-2018-9393	google - Android	In procfile_write of drivers/misc/mediatek/connectivity/wlan/gen2/os/linux/gl_proc.c, there is a possible OOB write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-04	7.8
CVE-2018-9394	google - Android	In mtk_p2p_wext_set_key of drivers/misc/mediatek/connectivity/wlan/gen2/os/linux/gl_p2p.c, there is a possible OOB write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-04	7.8
CVE-2018-9395	google - Android	In mtk_cfg80211_vendor_packet_keep_alive_start and mtk_cfg80211_vendor_set_config of drivers/misc/mediatek/connectivity/wlan/gen2/os/linux/gl_vendor.c, there is a possible OOB write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-04	7.8
CVE-2018-9396	google - Android	In rpc_msg_handler and related handlers of drivers/misc/mediatek/eccci/port_rpc.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-04	7.8
CVE-2018-9397	google - Android	In WMT_unlocked_ioctl of MTK WMT device driver, there is a possible OOB write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	7.8
CVE-2018-9398	google - Android	In fm_set_stat of mediatek FM radio driver, there is a possible OOB write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	7.8
CVE-2018-9399	google - Android	In /proc/driver/wmt_dbg driver, there are several possible out of bounds writes. These could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	7.8
CVE-2018-9400	google - Android	In gt1x_debug_write_proc and gt1x_tool_write of drivers/input/touchscreen/mediatek/GT1151/gt1x_generic.c and gt1x_tools.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	7.8
CVE-2018-9403	google - Android	In the MTK_FLP_MSG_HAL_DIAG_REPORT_DATA_NTF handler of flp2hal_- interface.c, there is a possible stack buffer overflow due to a missing bounds check. This could lead to local escalation of privilege in a privileged process with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	7.8
CVE-2018-9404	google - Android	In oemCallback of ril.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	7.8
CVE-2018-9439	google - Android	In __unregister_prot_hook and packet_release of af_packet.c, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the kernel with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	7.8
CVE-2018-9462	google - Android	In store_cmd of ftm4_pdc.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	7.8
CVE-2018-9463	google - Android	In sw49408_irq_runtime_engine_debug of touch_sw49408.c, there is a possible out of bounds write due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	7.8

CVE-2018-9388	google - Android	In store_upgrade and store_cmd of drivers/input/touchscreen/stm/ftm4_pdc.c, there are out of bound writes due to missing bounds checks or integer underflows. These could lead to escalation of privilege.	2024-12-05	7.8
CVE-2024-53141	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netfilter: ipset: add missing range check in bitmap_ip_uadt When tb[IPSET_ATTR_IP_TO] is not present but tb[IPSET_ATTR_CIDR] exists, the values of ip and ip_to are slightly swapped. Therefore, the range check for ip should be done later, but this part is missing and it seems that the vulnerability occurs. So we should add missing range checks and remove unnecessary range checks.	2024-12-06	7.8

CVE-2024-53142	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved:
		
		initramfs: avoid filename buffer overrun
		
		The initramfs filename field is defined in
		Documentation/driver-api/early-userspace/buffer-format.rst as:
		
		37 cpio_file := ALGN(4) + cpio_header + filename + "\0" + ALGN(4) + data
		...
		55 ============ ================= ========================
		56 Field name Field size Meaning
		57 ============ ================= ========================
		...
		70 c_namesize 8 bytes Length of filename, including final \0
		
		When extracting an initramfs cpio archive, the kernel's do_name() path
		handler assumes a zero-terminated path at @collected, passing it
		directly to filp_open() / init_mkdir() / init_mknod().
		
		If a specially crafted cpio entry carries a non-zero-terminated filename
		and is followed by uninitialized memory, then a file may be created with
		trailing characters that represent the uninitialized memory. The ability
		to create an initramfs entry would imply already having full control of
		the system, so the buffer overrun shouldn't be considered a security
		vulnerability.
		
		Append the output of the following bash script to an existing initramfs
		and observe any created /initramfs_test_fname_overrunAA* path. E.g.
		./reproducer.sh | gzip >> /myinitramfs
		
		It's easiest to observe non-zero uninitialized memory when the output is
		gzipped, as it'll overflow the heap allocated @out_buf in __gunzip(),
		rather than the initrd_start+initrd_size block.
		
		---- reproducer.sh ----
		nilchar="A" # change to "\0" to properly zero terminate / pad
		magic="070701"
		ino=1
		mode=$((0100777))
		uid=0
		gid=0
		nlink=1
		mtime=1
		filesize=0
		devmajor=0
		devminor=1
		rdevmajor=0
		rdevminor=0
		csum=0
		fname="initramfs_test_fname_overrun"
		namelen=$((${#fname} + 1)) # plus one to account for terminator
		
		printf "%s%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%08x%s" \
		$magic $ino $mode $uid $gid $nlink $mtime $filesize \
		$devmajor $devminor $rdevmajor $rdevminor $namelen $csum $fname
		
		termpadlen=$((1 + ((4 - ((110 + $namelen) & 3)) % 4)))
		printf "%.s${nilchar}" $(seq 1 $termpadlen)
		---- reproducer.sh ----
		
		Symlink filename fields handled in do_symlink() won't overrun past the
		data segment, due to the explicit zero-termination of the symlink
		target.
		
		Fix filename buffer overrun by aborting the initramfs FSM if any cpio
		entry doesn't carry a zero-terminator at the expected (name_len - 1)
		offset.
			2024-12-06	7.8

CVE-2024-53143	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: fsnotify: Fix ordering of iput() and watched_objects decrement Ensure the superblock is kept alive until we're done with iput(). Holding a reference to an inode is not allowed unless we ensure the superblock stays alive, which fsnotify does by keeping the watched_objects count elevated, so iput() must happen before the watched_objects decrement. This can lead to a UAF of something like sb->s_fs_info in tmpfs, but the UAF is hard to hit because race orderings that oops are more likely, thanks to the CHECK_DATA_CORRUPTION() block in generic_shutdown_super(). Also, ensure that fsnotify_put_sb_watched_objects() doesn't call fsnotify_sb_watched_objects() on a superblock that may have already been freed, which would cause a UAF read of sb->s_fsnotify_info.	2024-12-07	7.8
CVE-2024-47115	ibm - AIX	IBM AIX 7.2, 7.3 and VIOS 3.1 and 4.1 could allow a local user to execute arbitrary commands on the system due to improper neutralization of input.	2024-12-07	7.8
CVE-2024-42451	veeam - Backup & Replication	A vulnerability in Veeam Backup & Replication allows low-privileged users to leak all saved credentials in plaintext. This is achieved by calling a series of methods over an external protocol, ultimately retrieving the credentials using a malicious setup on the attacker's side. This exposes sensitive data, which could be used for further attacks, including unauthorized access to systems managed by the platform.	2024-12-04	7.7
CVE-2024-42457	veeam - Backup & Replication	A vulnerability in Veeam Backup & Replication allows users with certain operator roles to expose saved credentials by leveraging a combination of methods in a remote management interface. This can be achieved using a session object that allows for credential enumeration and exploitation, leading to the leak of plaintext credentials to a malicious host. The attack is facilitated by improper usage of a method that allows operators to add a new host with an attacker-controlled IP, enabling them to retrieve sensitive credentials in plaintext.	2024-12-04	7.7
CVE-2024-45204	veeam - Backup & Replication	A vulnerability exists where a low-privileged user can exploit insufficient permissions in credential handling to leak NTLM hashes of saved credentials. The exploitation involves using retrieved credentials to expose sensitive NTLM hashes, impacting systems beyond the initial target and potentially leading to broader security vulnerabilities.	2024-12-04	7.7
CVE-2024-33063	qualcomm - ar8035_firmware	Transient DOS while parsing the ML IE when a beacon with common info length of the ML IE greater than the ML IE inside which this element is present.	2024-12-02	7.5
CVE-2018-9381	google - Android	In gatts_process_read_by_type_req of gatt_sr.c, there is a possible information disclosure due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-12-02	7.5
CVE-2024-8748	zyxel - VMG8825-T50K firmware	A buffer overflow vulnerability in the packet parser of the third-party library "libclinkc" in Zyxel VMG8825-T50K firmware versions through V5.50(ABOM.8.4)C0 could allow an attacker to cause a temporary denial of service (DoS) condition against the web management interface by sending a crafted HTTP POST request to a vulnerable device.	2024-12-03	7.5
CVE-2024-41777	ibm - multiple products	IBM Cognos Controller 11.0.0 and 11.0.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data.	2024-12-03	7.5
CVE-2024-40763	sonicwall - SMA100	Heap-based buffer overflow vulnerability in the SonicWall SMA100 SSLVPN due to the use of strcpy. This allows remote authenticated attackers to cause Heap-based buffer overflow and potentially lead to code execution.	2024-12-05	7.5
CVE-2024-11941	drupal - Drupal Core	A vulnerability in Drupal Core allows Excessive Allocation.This issue affects Drupal Core: from 10.2.0 before 10.2.2, from 10.1.0 before 10.1.8.	2024-12-05	7.5
CVE-2024-42453	veeam - Backup & Replication	A vulnerability Veeam Backup & Replication allows low-privileged users to control and modify configurations on connected virtual infrastructure hosts. This includes the ability to power off virtual machines, delete files in storage, and make configuration changes, potentially leading to Denial of Service (DoS) and data integrity issues. The vulnerability is caused by improper permission checks in methods accessed via management services.	2024-12-04	7.4
CVE-2024-9200	zyxel - VMG4005-B50A firmware	A post-authentication command injection vulnerability in the "host" parameter of the diagnostic function in Zyxel VMG4005-B50A firmware versions through V5.15(ABQA.2.2)C0 could allow an authenticated attacker with administrator privileges to execute operating system (OS) commands on a vulnerable device.	2024-12-03	7.2
CVE-2024-51771	HPE - HPE Aruba Networking ClearPass Policy Manager	A vulnerability in the HPE Aruba Networking ClearPass Policy Manager web-based management interface could allow an authenticated remote threat actor to conduct a remote code execution attack. Successful exploitation could enable the attacker to run arbitrary commands on the underlying operating system.	2024-12-03	7.2
CVE-2024-53108	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Adjust VSDB parser for replay feature At some point, the IEEE ID identification for the replay check in the AMD EDID was added. However, this check causes the following out-of-bounds issues when using KASAN: [27.804016] BUG: KASAN: slab-out-of-bounds in amdgpu_dm_update_freesync_caps+0xefa/0x17a0 [amdgpu] [27.804788] Read of size 1 at addr ffff8881647fdb00 by task systemd-udevd/383 ... [27.821207] Memory state around the buggy address: [27.821215] ffff8881647fda00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	2024-12-02	7.1

		[27.821224] ffff8881647fda80: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [27.821234] >ffff8881647fdb00: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [27.821243] ^ [27.821250] ffff8881647fdb80: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [27.821259] ffff8881647fdc00: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 [27.821268] == This is caused because the ID extraction happens outside of the range of the edid lenght. This commit addresses this issue by considering the amd_vsdb_block size. (cherry picked from commit b7e381b1ccd5e778e3d9c44c669ad38439a861d8)		
CVE-2024-42449	veeam - Service Provider Console	From the VSPC management agent machine, under condition that the management agent is authorized on the server, it is possible to remove arbitrary files on the VSPC server machine.	2024-12-04	7.1
CVE-2024-42455	veeam - Backup & Replication	A vulnerability in Veeam Backup & Replication allows a low-privileged user to connect to remoting services and exploit insecure deserialization by sending a serialized temporary file collection. This exploit allows the attacker to delete any file on the system with service account privileges. The vulnerability is caused by an insufficient blacklist during the deserialization process.	2024-12-04	7.1
CVE-2024-12147	netgear - R6900	A vulnerability was found in Netgear R6900 1.0.1.26_1.0.20. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file upgrade_check.cgi of the component HTTP Header Handler. The manipulation of the argument Content-Length leads to buffer overflow. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2024-12-04	7.1
CVE-2024-45207	veeam - Agent for Windows	DLL injection in Veeam Agent for Windows can occur if the system's PATH variable includes insecure locations. When the agent runs, it searches these directories for necessary DLLs. If an attacker places a malicious DLL in one of these directories, the Veeam Agent might load it inadvertently, allowing the attacker to execute harmful code. This could lead to unauthorized access, data theft, or disruption of services	2024-12-04	7.0
CVE-2024-45717	solarwinds - SolarWinds Platform	The SolarWinds Platform was susceptible to a XSS vulnerability that affects the search and node information section of the user interface. This vulnerability requires authentication and requires user interaction.	2024-12-04	7.0
CVE-2024-33036	qualcomm - c-v2x_9150_firmware	Memory corruption while parsing sensor packets in camera driver, user-space variable is used while allocating memory in kernel and parsing which can lead to huge allocation or invalid memory access.	2024-12-02	6.7
CVE-2024-33039	qualcomm - qam8255p_firmware	Memory corruption when PAL client calls PAL service APIs by passing a random value as handle and the handle is not validated by the service.	2024-12-02	6.7
CVE-2024-33040	qualcomm - fastconnect_6800_firmware	Memory corruption while invoking redundant release command to release one buffer from user space as race condition can occur in kernel space between buffer release and buffer access.	2024-12-02	6.7
CVE-2024-33053	qualcomm - c-v2x_9150_firmware	Memory corruption when multiple threads try to unregister the CVP buffer at the same time.	2024-12-02	6.7
CVE-2017-13308	google - Android	In tscpu_write_GPIO_out and mtkts_Abts_write of mtk_ts_Abts.c, there is a possible buffer overflow in an sscanf due to improper input validation. This could lead to a local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	6.7
CVE-2018-9386	google - Android	In reboot_block_command of htc reboot_block driver, there is a possible stack buffer overflow due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	6.7
CVE-2018-9390	google - Android	In procfile_write of gl_proc.c, there is a possible out of bounds read of a function pointer due to an incorrect bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	6.7
CVE-2018-9391	google - Android	In update_gps_sv and output_vzw_debug of vendor/mediatek/proprietary/hardware/connectivity/gps/gps_hal/src/gpshal_wor ker.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	6.7
CVE-2018-9426	google - Android	In RsaKeyPairGenerator::getNumberOfIterations of RSAKeyPairGenerator.java, an incorrect implementation could cause weak RSA key pairs being generated. This could lead to crypto vulnerability with no additional execution privileges needed. User interaction is not needed for exploitation. Bulletin Fix: The fix is designed to correctly implement the key generation according to FIPS standard.	2024-12-02	6.5
CVE-2018-9429	google - Android	In buildImageItemsIfPossible of ItemTable.cpp there is a possible out of bound read due to uninitialized data. This could lead to information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	2024-12-02	6.5
CVE-2024-41776	ibm - multiple products	IBM Cognos Controller 11.0.0 and 11.0.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	2024-12-03	6.5
CVE-2024-45206	veeam - Service Provider Console	A vulnerability in Veeam Service Provider Console has been identified, which allows to perform arbitrary HTTP requests to arbitrary hosts of the network and get information about internal resources.	2024-12-04	6.5
CVE-2024-53135	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: KVM: VMX: Bury Intel PT virtualization (guest/host mode) behind CONFIG_BROKEN Hide KVM's pt_mode module param behind CONFIG_BROKEN, i.e. disable support for virtualizing Intel PT via guest/host mode unless BROKEN=y. There are myriad bugs in the implementation, some of which are fatal to the guest, and others which put the stability and health of the host at risk.	2024-12-04	6.5

		For guest fatalities, the most glaring issue is that KVM fails to ensure tracing is disabled, and *stays* disabled prior to VM-Enter, which is necessary as hardware disallows loading (the guest's) RTIT_CTL if tracing is enabled (enforced via a VMX consistency check). Per the SDM: If the logical processor is operating with Intel PT enabled (if IA32_RTIT_CTL.TraceEn = 1) at the time of VM entry, the "load IA32_RTIT_CTL" VM-entry control must be 0. On the host side, KVM doesn't validate the guest CPUID configuration provided by userspace, and even worse, uses the guest configuration to decide what MSRs to save/load at VM-Enter and VM-Exit. E.g. configuring guest CPUID to enumerate more address ranges than are supported in hardware will result in KVM trying to passthrough, save, and load non-existent MSRs, which generates a variety of WARNs, ToPA ERRORs in the host, a potential deadlock, etc.		
CVE-2018-9407	google - Android	In emmc_rpmb_ioctl of emmc_rpmb.c, there is an Information Disclosure due to a Missing Bounds Check. This could lead to Information Disclosure of kernel data.	2024-12-05	6.5
CVE-2024-51772	HPE - HPE Aruba Networking ClearPass Policy Manager	An authenticated RCE vulnerability in the ClearPass Policy Manager web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system.	2024-12-03	6.4
CVE-2024-47107	ibm - QRadar SIEM	IBM QRadar SIEM 7.5 is vulnerable to stored cross-site scripting. This vulnerability allows authenticated users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2024-12-07	6.4
CVE-2024-45319	sonicwall - SMA100	A vulnerability in the SonicWall SMA100 SSLVPN firmware 10.2.1.13-72sv and earlier versions allows a remote authenticated attacker can circumvent the certificate requirement during authentication.	2024-12-05	6.3
CVE-2018-9435	google - Android	In gatt_process_error_rsp of gatt_cl.cc, there is a possible out of bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-12-02	6.2
CVE-2024-11149	openbsd - OpenBSD	In OpenBSD 7.4 before errata 014, vmm(4) did not restore GDTR limits properly on Intel (VMX) CPUs.	2024-12-06	6.2
CVE-2024-33037	qualcomm - c-v2x_9150_firmware	Information disclosure as NPU firmware can send invalid IPC message to NPU driver as the driver doesn`t validate the IPC message received from the firmware.	2024-12-02	6.1
CVE-2021-29892	ibm - multiple products	IBM Cognos Controller 11.0.0 and 11.0.1 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.	2024-12-03	5.9
CVE-2024-41775	ibm - multiple products	IBM Cognos Controller 11.0.0 and 11.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	2024-12-03	5.9
CVE-2024-11942	drupal - Drupal Core	A vulnerability in Drupal Core allows File Manipulation.This issue affects Drupal Core: from 10.0.0 before 10.2.10.	2024-12-05	5.9
CVE-2024-53107	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: fs/proc/task_mmu: prevent integer overflow in pagemap_scan_get_args() The "arg->vec_len" variable is a u64 that comes from the user at the start of the function. The "arg->vec_len * sizeof(struct page_region))" multiplication can lead to integer wrapping. Use size_mul() to avoid that. Also the size_add/mul() functions work on unsigned long so for 32bit systems we need to ensure that "arg->vec_len" fits in an unsigned long.	2024-12-02	5.5
CVE-2024-53109	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: nommu: pass NULL argument to vma_iter_prealloc() When deleting a vma entry from a maple tree, it has to pass NULL to vma_iter_prealloc() in order to calculate internal state of the tree, but it passed a wrong argument. As a result, nommu kernels crashed upon accessing a vma iterator, such as acct_collect() reading the size of vma entries after do_munmap(). This commit fixes this issue by passing a right argument to the preallocation call.	2024-12-02	5.5
CVE-2024-53110	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: vp_vdpa: fix id_table array not null terminated error Allocate one extra virtio_device_id as null terminator, otherwise vdpa_mgmtdev_get_classes() may iterate multiple times and visit undefined memory.	2024-12-02	5.5
CVE-2024-53111	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mm/mremap: fix address wraparound in move_page_tables() On 32-bit platforms, it is possible for the expression `len + old_addr <	2024-12-02	5.5

		old_end` to be false-positive if `len + old_addr` wraps around. `old_addr` is the cursor in the old range up to which page table entries have been moved; so if the operation succeeded, `old_addr` is the *end* of the old region, and adding `len` to it can wrap. The overflow causes mremap() to mistakenly believe that PTEs have been copied; the consequence is that mremap() bails out, but doesn't move the PTEs back before the new VMA is unmapped, causing anonymous pages in the region to be lost. So basically if userspace tries to mremap() a private-anon region and hits this bug, mremap() will return an error and the private-anon region's contents appear to have been zeroed. The idea of this check is that `old_end - len` is the original start address, and writing the check that way also makes it easier to read; so fix the check by rearranging the comparison accordingly. (An alternate fix would be to refactor this function by introducing an "orig_old_start" variable or such.) Tested in a VM with a 32-bit X86 kernel; without the patch: ``` user@horn:~/big_mremap$ cat test.c #define _GNU_SOURCE #include <stdlib.h> #include <stdio.h> #include <err.h> #include <sys/mman.h> #define ADDR1 ((void*)0x60000000) #define ADDR2 ((void*)0x10000000) #define SIZE 0x50000000uL int main(void) { unsigned char *p1 = mmap(ADDR1, SIZE, PROT_READ|PROT_WRITE, MAP_ANONYMOUS|MAP_PRIVATE|MAP_FIXED_NOREPLACE, -1, 0); if (p1 == MAP_FAILED) err(1, "mmap 1"); unsigned char *p2 = mmap(ADDR2, SIZE, PROT_NONE, MAP_ANONYMOUS|MAP_PRIVATE|MAP_FIXED_NOREPLACE, -1, 0); if (p2 == MAP_FAILED) err(1, "mmap 2"); *p1 = 0x41; printf("first char is 0x%02hhx\n", *p1); unsigned char *p3 = mremap(p1, SIZE, SIZE, MREMAP_MAYMOVE|MREMAP_FIXED, p2); if (p3 == MAP_FAILED) { printf("mremap() failed; first char is 0x%02hhx\n", *p1); } else { printf("mremap() succeeded; first char is 0x%02hhx\n", *p3); } } user@horn:~/big_mremap$ gcc -static -o test test.c user@horn:~/big_mremap$ setarch -R ./test first char is 0x41 mremap() failed; first char is 0x00 ``` With the patch: ``` user@horn:~/big_mremap$ setarch -R ./test first char is 0x41 mremap() succeeded; first char is 0x41 ```		
CVE-2024-53112	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ocfs2: uncache inode which has failed entering the group Syzbot has reported the following BUG: kernel BUG at fs/ocfs2/uptodate.c:509! ... Call Trace: <TASK> ? __die_body+0x5f/0xb0 ? die+0x9e/0xc0 ? do_trap+0x15a/0x3a0 ? ocfs2_set_new_buffer_uptodate+0x145/0x160	2024-12-02	5.5

		? do_error_trap+0x1dc/0x2c0 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? __pfx_do_error_trap+0x10/0x10 ? handle_invalid_op+0x34/0x40 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ? exc_invalid_op+0x38/0x50 ? asm_exc_invalid_op+0x1a/0x20 ? ocfs2_set_new_buffer_uptodate+0x2e/0x160 ? ocfs2_set_new_buffer_uptodate+0x144/0x160 ? ocfs2_set_new_buffer_uptodate+0x145/0x160 ocfs2_group_add+0x39f/0x15a0 ? __pfx_ocfs2_group_add+0x10/0x10 ? __pfx_lock_acquire+0x10/0x10 ? mnt_get_write_access+0x68/0x2b0 ? __pfx_lock_release+0x10/0x10 ? rcu_read_lock_any_held+0xb7/0x160 ? __pfx_rcu_read_lock_any_held+0x10/0x10 ? smack_log+0x123/0x540 ? mnt_get_write_access+0x68/0x2b0 ? mnt_get_write_access+0x68/0x2b0 ? mnt_get_write_access+0x226/0x2b0 ocfs2_ioctl+0x65e/0x7d0 ? __pfx_ocfs2_ioctl+0x10/0x10 ? smack_file_ioctl+0x29e/0x3a0 ? __pfx_smack_file_ioctl+0x10/0x10 ? lockdep_hardirqs_on_prepare+0x43d/0x780 ? __pfx_lockdep_hardirqs_on_prepare+0x10/0x10 ? __pfx_ocfs2_ioctl+0x10/0x10 __se_sys_ioctl+0xfb/0x170 do_syscall_64+0xf3/0x230 entry_SYSCALL_64_after_hwframe+0x77/0x7f ... </TASK> When 'ioctl(OCFS2_IOC_GROUP_ADD, ...)' has failed for the particular inode in 'ocfs2_verify_group_and_input()', corresponding buffer head remains cached and subsequent call to the same 'ioctl()' for the same inode issues the BUG() in 'ocfs2_set_new_buffer_uptodate()' (trying to cache the same buffer head of that inode). Fix this by uncaching the buffer head with 'ocfs2_remove_from_cache()' on error path in 'ocfs2_group_add()'.		
CVE-2024-53113	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mm: fix NULL pointer dereference in alloc_pages_bulk_noprof We triggered a NULL pointer dereference for ac.preferred_zoneref->zone in alloc_pages_bulk_noprof() when the task is migrated between cpusets. When cpuset is enabled, in prepare_alloc_pages(), ac->nodemask may be &current->mems_allowed. when first_zones_zonelist() is called to find preferred_zoneref, the ac->nodemask may be modified concurrently if the task is migrated between different cpusets. Assuming we have 2 NUMA Node, when traversing Node1 in ac->zonelist, the nodemask is 2, and when traversing Node2 in ac->zonelist, the nodemask is 1. As a result, the ac->preferred_zoneref points to NULL zone. In alloc_pages_bulk_noprof(), for_each_zone_zonelist_nodemask() finds a allowable zone and calls zonelist_node_idx(ac.preferred_zoneref), leading to NULL pointer dereference. __alloc_pages_noprof() fixes this issue by checking NULL pointer in commit ea57485af8f4 ("mm, page_alloc: fix check for NULL preferred_zone") and commit df76cee6bbeb ("mm, page_alloc: remove redundant checks from alloc fastpath"). To fix it, check NULL pointer for preferred_zoneref->zone.	2024-12-02	5.5
CVE-2024-53114	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: x86/CPU/AMD: Clear virtualized VMLOAD/VMSAVE on Zen4 client A number of Zen4 client SoCs advertise the ability to use virtualized VMLOAD/VMSAVE, but using these instructions is reported to be a cause of a random host reboot. These instructions aren't intended to be advertised on Zen4 client so clear the capability.	2024-12-02	5.5
CVE-2024-53115	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/vmwgfx: avoid null_ptr_deref in vmw_framebuffer_surface_create_handle	2024-12-02	5.5

		The 'vmw_user_object_buffer' function may return NULL with incorrect inputs. To avoid possible null pointer dereference, add a check whether the 'bo' is NULL in the vmw_framebuffer_surface_create_handle.		
CVE-2024-53116	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Fix handling of partial GPU mapping of BOs This commit fixes the bug in the handling of partial mapping of the buffer objects to the GPU, which caused kernel warnings. Panthor didn't correctly handle the case where the partial mapping spanned multiple scatterlists and the mapping offset didn't point to the 1st page of starting scatterlist. The offset variable was not cleared after reaching the starting scatterlist. Following warning messages were seen. WARNING: CPU: 1 PID: 650 at drivers/iommu/io-pgtable-arm.c:659 __arm_lpae_unmap+0x254/0x5a0 <snip> pc : __arm_lpae_unmap+0x254/0x5a0 lr : __arm_lpae_unmap+0x2cc/0x5a0 <snip> Call trace: __arm_lpae_unmap+0x254/0x5a0 __arm_lpae_unmap+0x108/0x5a0 __arm_lpae_unmap+0x108/0x5a0 __arm_lpae_unmap+0x108/0x5a0 __arm_lpae_unmap+0x108/0x5a0 arm_lpae_unmap_pages+0x80/0xa0 panthor_vm_unmap_pages+0xac/0x1c8 [panthor] panthor_gpuva_sm_step_unmap+0x4c/0xc8 [panthor] op_unmap_cb.isra.23.constprop.30+0x54/0x80 __drm_gpuvm_sm_unmap+0x184/0x1c8 drm_gpuvm_sm_unmap+0x40/0x60 panthor_vm_exec_op+0xa8/0x120 [panthor] panthor_vm_bind_exec_sync_op+0xc4/0xe8 [panthor] panthor_ioctl_vm_bind+0x10c/0x170 [panthor] drm_ioctl_kernel+0xbc/0x138 drm_ioctl+0x210/0x4b0 __arm64_sys_ioctl+0xb0/0xf8 invoke_syscall+0x4c/0x110 el0_svc_common.constprop.1+0x98/0xf8 do_el0_svc+0x24/0x38 el0_svc+0x34/0xc8 el0t_64_sync_handler+0xa0/0xc8 el0t_64_sync+0x174/0x178 <snip> panthor : [drm] drm_WARN_ON(unmapped_sz != pgsize * pgcount) WARNING: CPU: 1 PID: 650 at drivers/gpu/drm/panthor/panthor_mmu.c:922 panthor_vm_unmap_pages+0x124/0x1c8 [panthor] <snip> pc : panthor_vm_unmap_pages+0x124/0x1c8 [panthor] lr : panthor_vm_unmap_pages+0x124/0x1c8 [panthor] <snip> panthor : [drm] *ERROR* failed to unmap range ffffa388f000-ffffa3890000 (requested range ffffa388c000-ffffa3890000)	2024-12-02	5.5
CVE-2024-53117	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: virtio/vsock: Improve MSG_ZEROCOPY error handling Add a missing kfree_skb() to prevent memory leaks.	2024-12-02	5.5
CVE-2024-53118	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: vsock: Fix sk_error_queue memory leak Kernel queues MSG_ZEROCOPY completion notifications on the error queue. Where they remain, until explicitly recv()ed. To prevent memory leaks, clean up the queue when the socket is destroyed. unreferenced object 0xffff8881028beb00 (size 224): comm "vsock_test", pid 1218, jiffies 4294694897 hex dump (first 32 bytes): 90 b0 21 17 81 88 ff ff 90 b0 21 17 81 88 ff ff ..!.....!..... 00 00 00 00 00 00 00 00 00 b0 21 17 81 88 ff ff ....!..... backtrace (crc 6c7031ca): [<ffffffff81418ef7>] kmem_cache_alloc_node_noprof+0x2f7/0x370 [<ffffffff81d35882>] __alloc_skb+0x132/0x180 [<ffffffff81d2d32b>] sock_omalloc+0x4b/0x80 [<ffffffff81d3a8ae>] msg_zerocopy_realloc+0x9e/0x240 [<ffffffff81fe5cb2>] virtio_transport_send_pkt_info+0x412/0x4c0 [<ffffffff81fe6183>] virtio_transport_stream_enqueue+0x43/0x50 [<ffffffff81fe0813>] vsock_connectible_sendmsg+0x373/0x450	2024-12-02	5.5

		[<ffffffff81d233d5>] ____sys_sendmsg+0x365/0x3a0 [<ffffffff81d246f4>] ___sys_sendmsg+0x84/0xd0 [<ffffffff81d26f47>] __sys_sendmsg+0x47/0x80 [<ffffffff820d3df3>] do_syscall_64+0x93/0x180 [<ffffffff8220012b>] entry_SYSCALL_64_after_hwframe+0x76/0x7e		
CVE-2024-53119	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: virtio/vsock: Fix accept_queue memory leak As the final stages of socket destruction may be delayed, it is possible that virtio_transport_recv_listen() will be called after the accept_queue has been flushed, but before the SOCK_DONE flag has been set. As a result, sockets enqueued after the flush would remain unremoved, leading to a memory leak. vsock_release __vsock_release lock virtio_transport_release virtio_transport_close schedule_delayed_work(close_work) sk_shutdown = SHUTDOWN_MASK (!) flush accept_queue release virtio_transport_recv_pkt vsock_find_bound_socket lock if flag(SOCK_DONE) return virtio_transport_recv_listen child = vsock_create_connected (!) vsock_enqueue_accept(child) release close_work lock virtio_transport_do_close set_flag(SOCK_DONE) virtio_transport_remove_sock vsock_remove_sock vsock_remove_bound release Introduce a sk_shutdown check to disallow vsock_enqueue_accept() during socket destruction. unreferenced object 0xffff888109e3f800 (size 2040): comm "kworker/5:2", pid 371, jiffies 4294940105 hex dump (first 32 bytes): 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .... 28 00 0b 40 00 00 00 00 00 00 00 00 00 00 00 00 (..@............ backtrace (crc 9e5f4e84): [<ffffffff81418ff1>] kmem_cache_alloc_noprof+0x2c1/0x360 [<ffffffff81d27aa0>] sk_prot_alloc+0x30/0x120 [<ffffffff81d2b54c>] sk_alloc+0x2c/0x4b0 [<ffffffff81fe049a>] __vsock_create.constprop.0+0x2a/0x310 [<ffffffff81fe6d6c>] virtio_transport_recv_pkt+0x4dc/0x9a0 [<ffffffff81fe745d>] vsock_loopback_work+0xfd/0x140 [<ffffffff810fc6ac>] process_one_work+0x20c/0x570 [<ffffffff810fce3f>] worker_thread+0x1bf/0x3a0 [<ffffffff811070dd>] kthread+0xdd/0x110 [<ffffffff81044fdd>] ret_from_fork+0x2d/0x50 [<ffffffff8100785a>] ret_from_fork_asm+0x1a/0x30	2024-12-02	5.5
CVE-2024-53120	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: CT: Fix null-ptr-deref in add rule err flow In error flow of mlx5_tc_ct_entry_add_rule(), in case ct_rule_add() callback returns error, zone_rule->attr is used uninitiated. Fix it to use attr which has the needed pointer value. Kernel log: BUG: kernel NULL pointer dereference, address: 0000000000000110 RIP: 0010:mlx5_tc_ct_entry_add_rule+0x2b1/0x2f0 [mlx5_core] … Call Trace: <TASK> ? __die+0x20/0x70 ? page_fault_oops+0x150/0x3e0 ? exc_page_fault+0x74/0x140 ? asm_exc_page_fault+0x22/0x30 ? mlx5_tc_ct_entry_add_rule+0x2b1/0x2f0 [mlx5_core]	2024-12-02	5.5

		? mlx5_tc_ct_entry_add_rule+0x1d5/0x2f0 [mlx5_core] mlx5_tc_ct_block_flow_offload+0xc6a/0xf90 [mlx5_core] ? nf_flow_offload_tuple+0xd8/0x190 [nf_flow_table] nf_flow_offload_tuple+0xd8/0x190 [nf_flow_table] flow_offload_work_handler+0x142/0x320 [nf_flow_table] ? finish_task_switch.isra.0+0x15b/0x2b0 process_one_work+0x16c/0x320 worker_thread+0x28c/0x3a0 ? __pfx_worker_thread+0x10/0x10 kthread+0xb8/0xf0 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x2d/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK>		
CVE-2024-53121	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: fs, lock FTE when checking if active The referenced commits introduced a two-step process for deleting FTEs: - Lock the FTE, delete it from hardware, set the hardware deletion function to NULL and unlock the FTE. - Lock the parent flow group, delete the software copy of the FTE, and remove it from the xarray. However, this approach encounters a race condition if a rule with the same match value is added simultaneously. In this scenario, fs_core may set the hardware deletion function to NULL prematurely, causing a panic during subsequent rule deletions. To prevent this, ensure the active flag of the FTE is checked under a lock, which will prevent the fs_core layer from attaching a new steering rule to an FTE that is in the process of deletion. [438.967589] MOSHE: 2496 mlx5_del_flow_rules del_hw_func [438.968205] ------------[cut here]------------ [438.968654] refcount_t: decrement hit 0; leaking memory. [438.969249] WARNING: CPU: 0 PID: 8957 at lib/refcount.c:31 refcount_warn_saturate+0xfb/0x110 [438.970054] Modules linked in: act_mirred cls_flower act_gact sch_ingress openvswitch nsh mlx5_vdpa vringh vhost_iotlb vdpa mlx5_ib mlx5_core xt_conntrack xt_MASQUERADE nf_conntrack_netlink nfnetlink xt_addrtype iptable_nat nf_nat br_netfilter rpcsec_gss_krb5 auth_rpcgss oid_registry overlay rpcrdma rdma_ucm ib_iser libiscsi scsi_transport_iscsi ib_umad rdma_cm ib_ipoib iw_cm ib_cm ib_uverbs ib_core zram zsmalloc fuse [last unloaded: cls_flower] [438.973288] CPU: 0 UID: 0 PID: 8957 Comm: tc Not tainted 6.12.0-rc1+ #8 [438.973888] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS rel-1.13.0-0-gf21b5a4aeb02-prebuilt.qemu.org 04/01/2014 [438.974874] RIP: 0010:refcount_warn_saturate+0xfb/0x110 [438.975363] Code: 40 66 3b 82 c6 05 16 e9 4d 01 01 e8 1f 7c a0 ff 0f 0b c3 cc cc cc cc 48 c7 c7 10 66 3b 82 c6 05 fd e8 4d 01 01 e8 05 7c a0 ff <0f> 0b c3 cc cc cc cc 66 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 00 90 [438.976947] RSP: 0018:ffff888124a53610 EFLAGS: 00010286 [438.977446] RAX: 0000000000000000 RBX: ffff888119d56de0 RCX: 0000000000000000 [438.978090] RDX: ffff88852c828700 RSI: ffff88852c81b3c0 RDI: ffff88852c81b3c0 [438.978721] RBP: ffff888120fa0e88 R08: 0000000000000000 R09: ffff888124a534b0 [438.979353] R10: 0000000000000001 R11: 0000000000000001 R12: ffff888119d56de0 [438.979979] R13: ffff888120fa0ec0 R14: ffff888120fa0ee8 R15: ffff888119d56de0 [438.980607] FS: 00007fe6dcc0f800(0000) GS:ffff88852c800000(0000) knlGS:0000000000000000 [438.983984] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [438.984544] CR2: 00000000004275e0 CR3: 0000000186982001 CR4: 0000000000372eb0 [438.985205] DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 [438.985842] DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 [438.986507] Call Trace: [438.986799] <TASK> [438.987070] ? __warn+0x7d/0x110 [438.987426] ? refcount_warn_saturate+0xfb/0x110 [438.987877] ? report_bug+0x17d/0x190 [438.988261] ? prb_read_valid+0x17/0x20 [438.988659] ? handle_bug+0x53/0x90 [438.989054] ? exc_invalid_op+0x14/0x70 [438.989458] ? asm_exc_invalid_op+0x16/0x20 [438.989883] ? refcount_warn_saturate+0xfb/0x110 [438.990348] mlx5_del_flow_rules+0x2f7/0x340 [mlx5_core] [438.990932] __mlx5_eswitch_del_rule+0x49/0x170 [mlx5_core] [438.991519] ? mlx5_lag_is_sriov+0x3c/0x50 [mlx5_core] [438.992054] ? xas_load+0x9/0xb0 [438.992407] mlx5e_tc_rule_unoffload+0x45/0xe0 [mlx5_core] [438.993037] mlx5e_tc_del_fdb_flow+0x2a6/0x2e0 [mlx5_core] [438.993623] mlx5e_flow_put+0x29/0x60 [mlx5_core] [438.994161] mlx5e_delete_flower+0x261/0x390 [mlx5_core]	2024-12-02	5.5

		[438.994728] tc_setup_cb_destroy+0xb9/0x190 [438.995150] fl_hw_destroy_filter+0x94/0xc0 [cls_flower] [438.995650] fl_change+0x11a4/0x13c0 [cls_flower] [438.996105] tc_new_tfilter+0x347/0xbc0 [438.996503] ? __ ---truncated---		
CVE-2024-53122	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mptcp: cope racing subflow creation in mptcp_rcv_space_adjust Additional active subflows - i.e. created by the in kernel path manager - are included into the subflow list before starting the 3whs. A racing recvmsg() spooling data received on an already established subflow would unconditionally call tcp_cleanup_rbuf() on all the current subflows, potentially hitting a divide by zero error on the newly created ones. Explicitly check that the subflow is in a suitable state before invoking tcp_cleanup_rbuf().	2024-12-02	5.5
CVE-2024-53123	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mptcp: error out earlier on disconnect Eric reported a division by zero splat in the MPTCP protocol: Oops: divide error: 0000 [#1] PREEMPT SMP KASAN PTI CPU: 1 UID: 0 PID: 6094 Comm: syz-executor317 Not tainted 6.12.0-rc5-syzkaller-00291-g05b92660cdfe #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 09/13/2024 RIP: 0010:__tcp_select_window+0x5b4/0x1310 net/ipv4/tcp_output.c:3163 Code: f6 44 01 e3 89 df e8 9b 75 09 f8 44 39 f3 0f 8d 11 ff ff ff e8 0d 74 09 f8 45 89 f4 e9 04 ff ff ff e8 00 74 09 f8 44 89 f0 99 <f7> 7c 24 14 41 29 d6 45 89 f4 e9 ec fe ff ff e8 e8 73 09 f8 48 89 RSP: 0018:ffffc900041f7930 EFLAGS: 00010293 RAX: 0000000000017e67 RBX: 0000000000017e67 RCX: ffffffff8983314b RDX: 0000000000000000 RSI: ffffffff898331b0 RDI: 0000000000000004 RBP: 00000000005d6000 R08: 0000000000000004 R09: 0000000000017e67 R10: 0000000000003e80 R11: 0000000000000000 R12: 0000000000003e80 R13: ffff888031d9b440 R14: 0000000000017e67 R15: 00000000002eb000 FS: 00007feb5d7f16c0(0000) GS:ffff8880b8700000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007feb5d8adbb8 CR3: 0000000074e4c000 CR4: 00000000003526f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> __tcp_cleanup_rbuf+0x3e7/0x4b0 net/ipv4/tcp.c:1493 mptcp_rcv_space_adjust net/mptcp/protocol.c:2085 [inline] mptcp_recvmsg+0x2156/0x2600 net/mptcp/protocol.c:2289 inet_recvmsg+0x469/0x6a0 net/ipv4/af_inet.c:885 sock_recvmsg_nosec net/socket.c:1051 [inline] sock_recvmsg+0x1b2/0x250 net/socket.c:1073 __sys_recvfrom+0x1a5/0x2e0 net/socket.c:2265 __do_sys_recvfrom net/socket.c:2283 [inline] __se_sys_recvfrom net/socket.c:2279 [inline] __x64_sys_recvfrom+0xe0/0x1c0 net/socket.c:2279 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x250 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7feb5d857559 Code: 28 00 00 00 75 05 48 83 c4 28 c3 e8 51 18 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 b0 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007feb5d7f1208 EFLAGS: 00000246 ORIG_RAX: 000000000000002d RAX: ffffffffffffffda RBX: 00007feb5d8e1318 RCX: 00007feb5d857559 RDX: 000000800000000e RSI: 0000000000000000 RDI: 0000000000000003 RBP: 00007feb5d8e1310 R08: 0000000000000000 R09: ffffffff81000000 R10: 0000000000000100 R11: 0000000000000246 R12: 00007feb5d8e131c R13: 00007feb5d8ae074 R14: 000000800000000e R15: 00000000ffffffdef and provided a nice reproducer. The root cause is the current bad handling of racing disconnect. After the blamed commit below, sk_wait_data() can return (with error) with the underlying socket disconnected and a zero rcv_mss.	2024-12-02	5.5

		Catch the error and return without performing any additional operations on the current socket.		
CVE-2018-9423	google - Android	In ihevcd_parse_slice_header of ihevcd_parse_slice_header.c there is a possible out of bound read due to missing bounds check. This could lead to denial of service with no additional execution privileges needed. User interaction is needed for exploitation.	2024-12-02	5.5
CVE-2018-9441	google - Android	In sdp_copy_raw_data of sdp_discovery.cc, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	2024-12-03	5.5
CVE-2018-9449	google - Android	In process_service_search_attr_rsp of sdp_discovery.cc, there is a possible out of bound read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2024-12-03	5.5
CVE-2024-25019	ibm - multiple products	IBM Cognos Controller 11.0.0 and 11.0.1 could be vulnerable to malicious file upload by not validating the type of file uploaded to Journal entry attachments. Attackers can make use of this weakness and upload malicious executable files into the system that can be sent to victims for performing further attacks.	2024-12-03	5.5
CVE-2024-25020	ibm - multiple products	IBM Cognos Controller 11.0.0 and 11.0.1 is vulnerable to malicious file upload by allowing unrestricted filetype attachments in the Journal entry page. Attackers can make use of this weakness and upload malicious executable files into the system and can be sent to victims for performing further attacks.	2024-12-03	5.5
CVE-2024-53127	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: Revert "mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K" The commit 8396c793ffdf ("mmc: dw_mmc: Fix IDMAC operation with pages bigger than 4K") increased the max_req_size, even for 4K pages, causing various issues: - Panic booting the kernel/rootfs from an SD card on Rockchip RK3566 - Panic booting the kernel/rootfs from an SD card on StarFive JH7100 - "swiotlb buffer is full" and data corruption on StarFive JH7110 At this stage no fix have been found, so it's probably better to just revert the change. This reverts commit 8396c793ffdf28bb8aee7cfe0891080f8cab7890.	2024-12-04	5.5
CVE-2024-53128	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: sched/task_stack: fix object_is_on_stack() for KASAN tagged pointers When CONFIG_KASAN_SW_TAGS and CONFIG_KASAN_STACK are enabled, the object_is_on_stack() function may produce incorrect results due to the presence of tags in the obj pointer, while the stack pointer does not have tags. This discrepancy can lead to incorrect stack object detection and subsequently trigger warnings if CONFIG_DEBUG_OBJECTS is also enabled. Example of the warning: ODEBUG: object 3eff800082ea7bb0 is NOT on stack ffff800082ea0000, but annotated. ------------[cut here]------------ WARNING: CPU: 0 PID: 1 at lib/debugobjects.c:557 __debug_object_init+0x330/0x364 Modules linked in: CPU: 0 UID: 0 PID: 1 Comm: swapper/0 Not tainted 6.12.0-rc5 #4 Hardware name: linux,dummy-virt (DT) pstate: 600000c5 (nZCv daIF -PAN -UAO -TCO -DIT -SSBS BTYPE=--) pc : __debug_object_init+0x330/0x364 lr : __debug_object_init+0x330/0x364 sp : ffff800082ea7b40 x29: ffff800082ea7b40 x28: 98ff0000c0164518 x27: 98ff0000c0164534 x26: ffff800082d93ec8 x25: 0000000000000001 x24: 1cff0000c00172a0 x23: 0000000000000000 x22: ffff800082d93ed0 x21: ffff800081a24418 x20: 3eff800082ea7bb0 x19: efff800000000000 x18: 0000000000000000 x17: 00000000000000ff x16: 0000000000000047 x15: 206b63617473206e x14: 0000000000000018 x13: ffff800082ea7780 x12: 0ffff800082ea78e x11: 0ffff800082ea790 x10: 0ffff800082ea79d x9 : 34d77febe173e800 x8 : 34d77febe173e800 x7 : 0000000000000001 x6 : 0000000000000001 x5 : feff800082ea74b8 x4 : ffff800082870a90 x3 : ffff80008018d3c4 x2 : 0000000000000001 x1 : ffff800082858810 x0 : 0000000000000050 Call trace: __debug_object_init+0x330/0x364 debug_object_init_on_stack+0x30/0x3c schedule_hrtimeout_range_clock+0xac/0x26c schedule_hrtimeout+0x1c/0x30 wait_task_inactive+0x1d4/0x25c kthread_bind_mask+0x28/0x98 init_rescuer+0x1e8/0x280 workqueue_init+0x1a0/0x3cc kernel_init_freeable+0x118/0x200 kernel_init+0x28/0x1f0 ret_from_fork+0x10/0x20 ---[end trace 0000000000000000]---	2024-12-04	5.5

		ODEBUG: object 3eff800082ea7bb0 is NOT on stack ffff800082ea0000, but annotated. ------------[cut here]------------		
CVE-2024-53129	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/rockchip: vop: Fix a dereferenced before check warning The 'state' can't be NULL, we should check crtc_state. Fix warning: drivers/gpu/drm/rockchip/rockchip_drm_vop.c:1096 vop_plane_atomic_async_check() warn: variable dereferenced before check 'state' (see line 1077)	2024-12-04	5.5
CVE-2024-53130	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix null-ptr-deref in block_dirty_buffer tracepoint When using the "block:block_dirty_buffer" tracepoint, mark_buffer_dirty() may cause a NULL pointer dereference, or a general protection fault when KASAN is enabled. This happens because, since the tracepoint was added in mark_buffer_dirty(), it references the dev_t member bh->b_bdev->bd_dev regardless of whether the buffer head has a pointer to a block_device structure. In the current implementation, nilfs_grab_buffer(), which grabs a buffer to read (or create) a block of metadata, including b-tree node blocks, does not set the block device, but instead does so only if the buffer is not in the "uptodate" state for each of its caller block reading functions. However, if the uptodate flag is set on a folio/page, and the buffer heads are detached from it by try_to_free_buffers(), and new buffer heads are then attached by create_empty_buffers(), the uptodate flag may be restored to each buffer without the block device being set to bh->b_bdev, and mark_buffer_dirty() may be called later in that state, resulting in the bug mentioned above. Fix this issue by making nilfs_grab_buffer() always set the block device of the super block structure to the buffer head, regardless of the state of the buffer's uptodate flag.	2024-12-04	5.5
CVE-2024-53131	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: nilfs2: fix null-ptr-deref in block_touch_buffer tracepoint Patch series "nilfs2: fix null-ptr-deref bugs on block tracepoints". This series fixes null pointer dereference bugs that occur when using nilfs2 and two block-related tracepoints. This patch (of 2): It has been reported that when using "block:block_touch_buffer" tracepoint, touch_buffer() called from __nilfs_get_folio_block() causes a NULL pointer dereference, or a general protection fault when KASAN is enabled. This happens because since the tracepoint was added in touch_buffer(), it references the dev_t member bh->b_bdev->bd_dev regardless of whether the buffer head has a pointer to a block_device structure. In the current implementation, the block_device structure is set after the function returns to the caller. Here, touch_buffer() is used to mark the folio/page that owns the buffer head as accessed, but the common search helper for folio/page used by the caller function was optimized to mark the folio/page as accessed when it was reimplemented a long time ago, eliminating the need to call touch_buffer() here in the first place. So this solves the issue by eliminating the touch_buffer() call itself.	2024-12-04	5.5
CVE-2024-53132	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/xe/oa: Fix "Missing outer runtime PM protection" warning Fix the following drm_WARN: [953.586396] xe 0000:00:02.0: [drm] Missing outer runtime PM protection ... <4> [953.587090] ? xe_pm_runtime_get_noresume+0x8d/0xa0 [xe] <4> [953.587208] guc_exec_queue_add_msg+0x28/0x130 [xe] <4> [953.587319] guc_exec_queue_fini+0x3a/0x40 [xe]	2024-12-04	5.5

		<4> [953.587425] xe_exec_queue_destroy+0xb3/0xf0 [xe] <4> [953.587515] xe_oa_release+0x9c/0xc0 [xe] (cherry picked from commit b107c63d2953907908fd0cafb0e543b3c3167b75)		
CVE-2024-53134	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: pmdomain: imx93-blk-ctrl: correct remove path The check condition should be 'i < bc->onecell_data.num_domains', not 'bc->onecell_data.num_domains' which will make the look never finish and cause kernel panic. Also disable runtime to address "imx93-blk-ctrl 4ac10000.system-controller: Unbalanced pm_runtime_enable!"	2024-12-04	5.5
CVE-2024-53137	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ARM: fix cacheflush with PAN It seems that the cacheflush syscall got broken when PAN for LPAE was implemented. User access was not enabled around the cache maintenance instructions, causing them to fault.	2024-12-04	5.5
CVE-2024-53138	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: kTLS, Fix incorrect page refcounting The kTLS tx handling code is using a mix of get_page() and page_ref_inc() APIs to increment the page reference. But on the release path (mlx5e_ktls_tx_handle_resync_dump_comp()), only put_page() is used. This is an issue when using pages from large folios: the get_page() references are stored on the folio page while the page_ref_inc() references are stored directly in the given page. On release the folio page will be dereferenced too many times. This was found while doing kTLS testing with sendfile() + ZC when the served file was read from NFS on a kernel with NFS large folios support (commit 49b29a573da8 ("nfs: add support for large folios")).	2024-12-04	5.5
CVE-2024-53140	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netlink: terminate outstanding dump on socket close Netlink supports iterative dumping of data. It provides the families the following ops: - start - (optional) kicks off the dumping process - dump - actual dump helper, keeps getting called until it returns 0 - done - (optional) pairs with .start, can be used for cleanup The whole process is asynchronous and the repeated calls to .dump don't actually happen in a tight loop, but rather are triggered in response to recvmsg() on the socket. This gives the user full control over the dump, but also means that the user can close the socket without getting to the end of the dump. To make sure .start is always paired with .done we check if there is an ongoing dump before freeing the socket, and if so call .done. The complication is that sockets can get freed from BH and .done is allowed to sleep. So we use a workqueue to defer the call, when needed. Unfortunately this does not work correctly. What we defer is not the cleanup but rather releasing a reference on the socket. We have no guarantee that we own the last reference, if someone else holds the socket they may release it in BH and we're back to square one. The whole dance, however, appears to be unnecessary. Only the user can interact with dumps, so we can clean up when socket is closed. And close always happens in process context. Some async code may still access the socket after close, queue notification skbs to it etc. but no dumps can start, end or otherwise make progress. Delete the workqueue and flush the dump state directly from the release handler. Note that further cleanup is possible in -next, for instance we now always call .done before releasing the main module reference, so dump doesn't have to take a reference of its own.	2024-12-04	5.5
CVE-2018-9408	google - Android	In m3326_gps_write and m3326_gps_read of gps.s, there is a possible Out Of Bounds Read due to a missing bounds check. This could lead to a local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.	2024-12-05	5.5

CVE-2024-25035	ibm - multiple products	IBM Cognos Controller 11.0.0 and 11.0.1 exposes server details that could allow an attacker to obtain information of the application environment to conduct further attacks.	2024-12-03	5.3
CVE-2024-53702	sonicwall - SMA100	Use of cryptographically weak pseudo-random number generator (PRNG) vulnerability in the SonicWall SMA100 SSLVPN backup code generator that, in certain cases, can be predicted by an attacker, potentially exposing the generated secret.	2024-12-05	5.3
CVE-2024-37071	ibm - Db2 for Linux, UNIX and Windows	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 could allow an authenticated user to cause a denial of service with a specially crafted query due to improper memory allocation.	2024-12-07	5.3
CVE-2024-41762	ibm - Db2 for Linux, UNIX and Windows	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to a denial of service as the server may crash under certain conditions with a specially crafted query.	2024-12-07	5.3
CVE-2024-20397	cisco - multiple products	A vulnerability in the bootloader of Cisco NX-OS Software could allow an unauthenticated attacker with physical access to an affected device, or an authenticated, local attacker with administrative credentials, to bypass NX-OS image signature verification._x000D_ _x000D_ This vulnerability is due to insecure bootloader settings. An attacker could exploit this vulnerability by executing a series of bootloader commands. A successful exploit could allow the attacker to bypass NX-OS image signature verification and load unverified software.	2024-12-04	5.2
CVE-2024-9197	zyxel - VMG3625-T50B firmware	A post-authentication buffer overflow vulnerability in the parameter "action" of the CGI program in Zyxel VMG3625-T50B firmware versions through V5.50(ABPM.9.2)C0 could allow an authenticated attacker with administrator privileges to cause a temporary denial of service (DoS) condition against the web management interface by sending a crafted HTTP GET request to a vulnerable device if the function ZyEE is enabled.	2024-12-03	4.9
CVE-2024-51773	HPE - HPE Aruba Networking ClearPass Policy Manager	A vulnerability in the HPE Aruba Networking ClearPass Policy Manager web-based management interface could allow an authenticated remote Attacker to conduct a stored cross-site scripting (XSS) attack. Successful exploitation could enable a threat actor to perform any actions the user is authorized to do, including accessing the user's data and altering information within the user's permissions. This could lead to data modification, deletion, or theft, including unauthorized access to files, file deletion, or the theft of session cookies, which an attacker could use to hijack a user's session.	2024-12-03	4.8
CVE-2024-53124	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: fix data-races around sk->sk_forward_alloc Syzkaller reported this warning: ------------[cut here]------------ WARNING: CPU: 0 PID: 16 at net/ipv4/af_inet.c:156 inet_sock_destruct+0x1c5/0x1e0 Modules linked in: CPU: 0 UID: 0 PID: 16 Comm: ksoftirqd/0 Not tainted 6.12.0-rc5 #26 Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS 1.15.0-1 04/01/2014 RIP: 0010:inet_sock_destruct+0x1c5/0x1e0 Code: 24 12 4c 89 e2 5b 48 c7 c7 98 ec bb 82 41 5c e9 d1 18 17 ff 4c 89 e6 5b 48 c7 c7 d0 ec bb 82 41 5c e9 bf 18 17 ff 0f 0b eb 83 <0f> 0b eb 97 0f 0b eb 87 0f 0b e9 68 ff ff ff 66 66 2e 0f 1f 84 00 RSP: 0018:ffffc9000008bd90 EFLAGS: 00010206 RAX: 0000000000000300 RBX: ffff88810b172a90 RCX: 0000000000000007 RDX: 0000000000000002 RSI: 0000000000000300 RDI: ffff88810b172a00 RBP: ffff88810b172a00 R08: ffff888104273c00 R09: 0000000000100007 R10: 0000000000020000 R11: 0000000000000006 R12: ffff88810b172a00 R13: 0000000000000004 R14: 0000000000000000 R15: ffff888237c31f78 FS: 0000000000000000(0000) GS:ffff888237c00000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 00007ffc63fecac8 CR3: 000000000342e000 CR4: 00000000000006f0 DR0: 0000000000000000 DR1: 0000000000000000 DR2: 0000000000000000 DR3: 0000000000000000 DR6: 00000000fffe0ff0 DR7: 0000000000000400 Call Trace: <TASK> ? __warn+0x88/0x130 ? inet_sock_destruct+0x1c5/0x1e0 ? report_bug+0x18e/0x1a0 ? handle_bug+0x53/0x90 ? exc_invalid_op+0x18/0x70 ? asm_exc_invalid_op+0x1a/0x20 ? inet_sock_destruct+0x1c5/0x1e0 __sk_destruct+0x2a/0x200 rcu_do_batch+0x1aa/0x530 ? rcu_do_batch+0x13b/0x530 rcu_core+0x159/0x2f0 handle_softirqs+0xd3/0x2b0 ? __pfx_smpboot_thread_fn+0x10/0x10 run_ksoftirqd+0x25/0x30 smpboot_thread_fn+0xdd/0x1d0 kthread+0xd3/0x100 ? __pfx_kthread+0x10/0x10 ret_from_fork+0x34/0x50 ? __pfx_kthread+0x10/0x10 ret_from_fork_asm+0x1a/0x30 </TASK> ---[end trace 0000000000000000]--- Its possible that two threads call tcp_v6_do_rcv()/sk_forward_alloc_add()	2024-12-02	4.7

		concurrently when sk->sk_state == TCP_LISTEN with sk->sk_lock unlocked, which triggers a data-race around sk->sk_forward_alloc: tcp_v6_rcv tcp_v6_do_rcv skb_clone_and_charge_r sk_rmem_schedule __sk_mem_schedule sk_forward_alloc_add() skb_set_owner_r sk_mem_charge sk_forward_alloc_add() __kfree_skb skb_release_all skb_release_head_state sock_rfree sk_mem_uncharge sk_forward_alloc_add() sk_mem_reclaim // set local var reclaimable __sk_mem_reclaim sk_forward_alloc_add() In this syzkaller testcase, two threads call tcp_v6_do_rcv() with skb->truesize=768, the sk_forward_alloc changes like this: (cpu 1) | (cpu 2) | sk_forward_alloc ... | ... | 0 __sk_mem_schedule() | | +4096 = 4096 | __sk_mem_schedule() | +4096 = 8192 sk_mem_charge() | | -768 = 7424 | sk_mem_charge() | -768 = 6656 ... | ... | sk_mem_uncharge() | | +768 = 7424 reclaimable=7424 | | | sk_mem_uncharge() | +768 = 8192 | reclaimable=8192 | __sk_mem_reclaim() | | -4096 = 4096 | __sk_mem_reclaim() | -8192 = -4096 != 0 The skb_clone_and_charge_r() should not be called in tcp_v6_do_rcv() when sk->sk_state is TCP_LISTEN, it happens later in tcp_v6_syn_recv_sock(). Fix the same issue in dccp_v6_do_rcv().		
CVE-2024-53672	HPE - HPE Aruba Networking ClearPass Policy Manager	A vulnerability in the ClearPass Policy Manager web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. Successful exploit could allow an attacker to execute arbitrary commands as a lower privileged user on the underlying operating system.	2024-12-03	4.7
CVE-2024-53136	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mm: revert "mm: shmem: fix data-race in shmem_getattr()" Revert d949d1d14fa2 ("mm: shmem: fix data-race in shmem_getattr()") as suggested by Chuck [1]. It is causing deadlocks when accessing tmpfs over NFS. As Hugh commented, "added just to silence a syzbot sanitizer splat: added where there has never been any practical problem".	2024-12-04	4.7
CVE-2024-25036	ibm - multiple products	IBM Cognos Controller 11.0.0 and 11.0.1 could allow an authenticated user with local access to bypass security allowing users to circumvent restrictions imposed on input fields.	2024-12-03	4.3
CVE-2024-45676	ibm - multiple products	IBM Cognos Controller 11.0.0 and 11.0.1 could allow an authenticated user to upload insecure files, due to insufficient file type distinction.	2024-12-03	4.3
CVE-2023-52943	synology - Surveillance Station	Incorrect authorization vulnerability in Alert.Setting webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to to perform limited actions on the alerting function via unspecified vectors.	2024-12-04	4.3
CVE-2023-52944	synology - Surveillance Station	Incorrect authorization vulnerability in ActionRule webapi component in Synology Surveillance Station before 9.2.0-11289 and 9.2.0-9289 allows remote authenticated users to perform limited actions on the set action rules function via unspecified vectors.	2024-12-04	4.3
CVE-2024-54127	tp-link - Archer C50 Wireless Router	This vulnerability exists in the TP-Link Archer C50 due to presence of terminal access on a serial interface without proper access control. An attacker with physical access could exploit this by accessing the UART shell on the vulnerable device. Successful exploitation of this vulnerability could allow the attacker to obtain Wi-Fi credentials of the targeted system.	2024-12-05	4.3
CVE-2024-49041	microsoft - Microsoft Edge	Microsoft Edge (Chromium-based) Spoofing Vulnerability	2024-12-06	4.3
CVE-2024-10933	openbsd - OpenBSD	In OpenBSD 7.5 before errata 009 and OpenBSD 7.4 before errata 022, exclude any '/' in readdir name validation to avoid unexpected directory traversal on untrusted file systems.	2024-12-05	4.1