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 22 سبتمبر إلى 28 سبتمبر. 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 22nd of September to 28th of September. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2024-42505	hewlett packard enterprise (hpe) - Aruba OS	Command injection vulnerabilities in the underlying CLI service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2024-09-25	9.8	Critical
CVE-2024-42506	hewlett packard enterprise (hpe) - Aruba OS	Command injection vulnerabilities in the underlying CLI service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2024-09-25	9.8	Critical
CVE-2024-42507	hewlett packard enterprise (hpe) - Aruba OS	Command injection vulnerabilities in the underlying CLI service could lead to unauthenticated remote code execution by sending specially crafted packets destined to the PAPI (Aruba's Access Point management protocol) UDP port (8211). Successful exploitation of these vulnerabilities results in the ability to execute arbitrary code as a privileged user on the underlying operating system.	2024-09-25	9.8	Critical
CVE-2024-7575	telerik - ui_for_wpf	In Progress Telerik UI for WPF versions prior to 2024 Q3 (2024.3.924), a command injection attack is possible through improper neutralization of hyperlink elements.	2024-09-25	9.8	Critical
CVE-2024-7576	telerik - ui_for_wpf	In Progress Telerik UI for WPF versions prior to 2024 Q3 (2024.3.924), a code execution attack is possible through an insecure deserialization vulnerability.	2024-09-25	9.8	Critical
CVE-2024-7024	google - Chrome	Inappropriate implementation in V8 in Google Chrome prior to 126.0.6478.54 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	2024-09-23	9.3	Critical
CVE-2024-20510	cisco - multiple products	A vulnerability in the Central Web Authentication (CWA) feature of Cisco IOS XE Software for Wireless Controllers could allow an unauthenticated, adjacent attacker to bypass the pre-authentication access control list (ACL), which could allow access to network resources before user authentication. This vulnerability is due to a logic error when activating the pre-authentication ACL that is received from the authentication, authorization, and accounting (AAA) server. An attacker could exploit this vulnerability by connecting to a wireless network that is configured for CWA and sending traffic through an affected device that should be denied by the configured ACL before user authentication. A successful exploit could allow the attacker to bypass configured ACL protections on the affected device before the user authentication is completed, allowing the attacker to access trusted networks that the device might be protecting.	2024-09-25	9.3	Critical
CVE-2024-6592	watchguard - multiple products	Incorrect Authorization vulnerability in the protocol communication between the WatchGuard Authentication Gateway (aka Single Sign-On Agent) on Windows and the WatchGuard Single Sign-On Client on Windows and MacOS allows Authentication Bypass.This issue affects	2024-09-25	9.1	Critical

		the Authentication Gateway: through 12.10.2; Windows Single Sign-On Client: through 12.7; MacOS Single Sign-On Client: through 12.5.4.			
CVE-2024-6593	watchguard - authentication_gateway	Incorrect Authorization vulnerability in WatchGuard Authentication Gateway (aka Single Sign-On Agent) on Windows allows an attacker with network access to execute restricted management commands. This issue affects Authentication Gateway: through 12.10.2.	2024-09-25	9.1	Critical
CVE-2021-38023	google - Chrome	Use after free in Extensions in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-09-23	8.8	High
CVE-2024-7018	google - Chrome	Heap buffer overflow in PDF in Google Chrome prior to 124.0.6367.78 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Medium)	2024-09-23	8.8	High
CVE-2024-7022	google - Chrome	Uninitialized Use in V8 in Google Chrome prior to 123.0.6312.58 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	2024-09-23	8.8	High
CVE-2024-9120	google - Chrome	Use after free in Dawn in Google Chrome on Windows prior to 129.0.6668.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-09-25	8.8	High
CVE-2024-9121	google - Chrome	Inappropriate implementation in V8 in Google Chrome prior to 129.0.6668.70 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	2024-09-25	8.8	High
CVE-2024-9122	google - Chrome	Type Confusion in V8 in Google Chrome prior to 129.0.6668.70 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	2024-09-25	8.8	High
CVE-2024-7479	teamviewer - multiple products	Improper verification of cryptographic signature during installation of a VPN driver via the TeamViewer_service.exe component of TeamViewer Remote Clients prior version 15.58.4 for Windows allows an attacker with local unprivileged access on a Windows system to elevate their privileges and install drivers.	2024-09-25	8.8	High
CVE-2024-7481	teamviewer - multiple products	Improper verification of cryptographic signature during installation of a Printer driver via the TeamViewer_service.exe component of TeamViewer Remote Clients prior version 15.58.4 for Windows allows an attacker with local unprivileged access on a Windows system to elevate their privileges and install drivers.	2024-09-25	8.8	High
CVE-2024-47083	microsoft - power_platform_terraform_provider	Power Platform Terraform Provider allows managing environments and other resources within Power Platform. Versions prior to 3.0.0 have an issue in the Power Platform Terraform Provider where sensitive information, specifically the `client_secret` used in the service principal authentication, may be exposed in logs. This exposure occurs due to an error in the logging code that causes the `client_secret` to not be properly masked when logs are persisted or viewed. Users should upgrade to version 3.0.0 to receive a patched version of the provider that removes all logging of sensitive content. Users who have used this provider with the affected versions should take the following additional steps to mitigate the risk: Immediately rotate the `client_secret` for any service principal that has been configured using this Terraform provider. This will invalidate any potentially exposed secrets. Those who have set the `TF_LOG_PATH` environment variable or configured Terraform to persist logs to a file or an external system, consider disabling this until they have updated to a fixed version of the provider. Those who have existing logs that may contain the `client_secret` should remove or sanitize these logs to prevent unauthorized access. This includes logs on disk, in monitoring systems, or in logging services.	2024-09-25	8.8	High
CVE-2024-20436	cisco - Cisco IOS XE Software	A vulnerability in the HTTP Server feature of Cisco IOS XE Software when the Telephony Service feature is enabled could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to a null pointer dereference when accessing specific URLs. An attacker could exploit this vulnerability by sending crafted HTTP traffic to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, causing a DoS condition on the affected device.	2024-09-25	8.6	High
CVE-2024-20455	cisco - multiple products	A vulnerability in the process that classifies traffic that is going to the Unified Threat Defense (UTD) component of Cisco IOS XE Software in controller mode could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because UTD improperly handles certain packets as those packets egress an SD-WAN IPsec tunnel. An attacker could exploit this vulnerability by sending crafted traffic through an SD-WAN IPsec tunnel that is configured on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: SD-WAN tunnels that are configured with Generic Routing Encapsulation (GRE) are not affected by this vulnerability.	2024-09-25	8.6	High
CVE-2024-20464	cisco - Cisco IOS XE Software	A vulnerability in the Protocol Independent Multicast (PIM) feature of Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of received IPv4 PIMv2	2024-09-25	8.6	High

		packets. An attacker could exploit this vulnerability by sending a crafted PIMv2 packet to a PIM-enabled interface on an affected device. A successful exploit could allow the attacker to cause an affected device to reload, resulting in a DoS condition. Note: This vulnerability can be exploited with either an IPv4 multicast or unicast packet.			
CVE-2024-20467	cisco - multiple products	A vulnerability in the implementation of the IPv4 fragmentation reassembly code in Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper management of resources during fragment reassembly. An attacker could exploit this vulnerability by sending specific sizes of fragmented packets to an affected device or through a Virtual Fragmentation Reassembly (VFR)-enabled interface on an affected device. A successful exploit could allow the attacker to cause the device to reload, resulting in a DoS condition. Note: This vulnerability affects Cisco ASR 1000 Series Aggregation Services Routers and Cisco cBR-8 Converged Broadband Routers if they are running Cisco IOS XE Software Release 17.12.1 or 17.12.1a.	2024-09-25	8.6	High
CVE-2024-20480	cisco - multiple products	A vulnerability in the DHCP Snooping feature of Cisco IOS XE Software on Software-Defined Access (SD-Access) fabric edge nodes could allow an unauthenticated, remote attacker to cause high CPU utilization on an affected device, resulting in a denial of service (DoS) condition that requires a manual reload to recover. This vulnerability is due to improper handling of IPv4 DHCP packets. An attacker could exploit this vulnerability by sending certain IPv4 DHCP packets to an affected device. A successful exploit could allow the attacker to cause the device to exhaust CPU resources and stop processing traffic, resulting in a DoS condition that requires a manual reload to recover.	2024-09-25	8.6	High
CVE-2024-6769	microsoft - multiple products	A DLL Hijacking caused by drive remapping combined with a poisoning of the activation cache in Microsoft Windows 10, Windows 11, Windows Server 2016, Windows Server 2019, and Windows Server 2022 allows a malicious authenticated attacker to elevate from a medium integrity process to a high integrity process without the intervention of a UAC prompt.	2024-09-26	8.4	High
CVE-2023-52946	synology - Synology Drive Client	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in vss service component in Synology Drive Client before 3.5.0-16084 allows remote attackers to overwrite trivial buffers and crash the client via unspecified vectors.	2024-09-26	8.2	High
CVE-2024-20437	cisco - Cisco IOS XE Software	A vulnerability in the web-based management interface of Cisco IOS XE Software could allow an unauthenticated, remote attacker to perform a cross-site request forgery (CSRF) attack and execute commands on the CLI of an affected device. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an already authenticated user to follow a crafted link. A successful exploit could allow the attacker to perform arbitrary actions on the affected device with the privileges of the targeted user.	2024-09-25	8.1	High
CVE-2024-7023	google - Chrome	Insufficient data validation in Updater in Google Chrome prior to 128.0.6537.0 allowed a remote attacker to perform privilege escalation via a malicious file. (Chromium security severity: Medium)	2024-09-23	8	High
CVE-2021-38963	ibm - aspera_console	IBM Aspera Console 3.4.0 through 3.4.4 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by a CSV injection vulnerability. By persuading a victim to open a specially crafted file, an attacker could exploit this vulnerability to execute arbitrary code on the system.	2024-09-25	8	High
CVE-2018-20072	google - chrome	Insufficient data validation in PDF in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform out of bounds memory access via a crafted PDF file. (Chromium security severity: Low)	2024-09-23	7.8	High
CVE-2024-7679	telerik - ui_for_wpf	In Progress Telerik UI for WinForms versions prior to 2024 Q3 (2024.3.924), a command injection attack is possible through improper neutralization of hyperlink elements.	2024-09-25	7.8	High
CVE-2024-8316	telerik - ui_for_wpf	In Progress Telerik UI for WPF versions prior to 2024 Q3 (2024.3.924), a code execution attack is possible through an insecure deserialization vulnerability.	2024-09-25	7.8	High
CVE-2024-8975	grafana - multiple products	Unquoted Search Path or Element vulnerability in Grafana Alloy on Windows allows Privilege Escalation from Local User to SYSTEM This issue affects Alloy: before 1.3.3, from 1.4.0-rc.0 through 1.4.0-rc.1.	2024-09-25	7.8	High
CVE-2024-8996	grafana - agent	Unquoted Search Path or Element vulnerability in Grafana Agent (Flow mode) on Windows allows Privilege Escalation from Local User to SYSTEM This issue affects Agent Flow: before 0.43.2	2024-09-25	7.8	High
CVE-2022-49038	synology - Synology Drive Client	Inclusion of functionality from untrusted control sphere vulnerability in OpenSSL DLL component in Synology Drive Client before 3.3.0-15082 allows local users to execute arbitrary code via unspecified vectors.	2024-09-26	7.8	High

CVE-2024-39435	google - multiple products	In Logmanager service, there is a possible missing verification incorrect input. This could lead to local escalation of privilege with no additional execution privileges needed.	2024-09-27	7.8	High
CVE-2024-46804	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add array index check for hdcp ddc access [Why] Coverity reports OVERRUN warning. Do not check if array index valid. [How] Check msg_id valid and valid array index.	2024-09-27	7.8	High
CVE-2024-46813	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check link_index before accessing dc->links[] [WHY & HOW] dc->links[] has max size of MAX_LINKS and NULL is return when trying to access with out-of-bound index. This fixes 3 OVERRUN and 1 RESOURCE_LEAK issues reported by Coverity.	2024-09-27	7.8	High
CVE-2024-46814	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check msg_id before processing transcation [WHY & HOW] HDCP_MESSAGE_ID_INVALID (-1) is not a valid msg_id nor is it a valid array index, and it needs checking before used. This fixes 4 OVERRUN issues reported by Coverity.	2024-09-27	7.8	High
CVE-2024-46818	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check gpio_id before used as array index [WHY & HOW] GPIO_ID_UNKNOWN (-1) is not a valid value for array index and therefore should be checked in advance. This fixes 5 OVERRUN issues reported by Coverity.	2024-09-27	7.8	High
CVE-2024-46821	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amd/pm: Fix negative array index read Avoid using the negative values for clk_idex as an index into an array pptable->DpmDescriptor. V2: fix clk_index return check (Tim Huang)	2024-09-27	7.8	High
CVE-2024-46831	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: microchip: vcap: Fix use-after-free error in kunit test This is a clear use-after-free error. We remove it, and rely on checking the return code of vcap_del_rule.	2024-09-27	7.8	High
CVE-2024-46844	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: um: line: always fill *error_out in setup_one_line() The pointer isn't initialized by callers, but I have encountered cases where it's still printed; initialize it in all possible cases in setup_one_line().	2024-09-27	7.8	High
CVE-2024-46845	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: tracing/timerlat: Only clear timer if a kthread exists The timerlat tracer can use user space threads to check for osnoise and timer latency. If the program using this is killed via a SIGTERM, the threads are shutdown one at a time and another tracing instance can start up resetting the threads before they are fully closed. That causes the hrtimer assigned to the kthread to be shutdown and freed twice when the dying thread finally closes the file descriptors, causing a use-after-free bug. Only cancel the hrtimer if the associated thread is still around. Also add the interface_lock around the resetting of the tlat_var->kthread. Note, this is just a quick fix that can be backported to stable. A real fix is to have a better synchronization between the shutdown of old threads and the starting of new ones.	2024-09-27	7.8	High
CVE-2024-46849	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ASoC: meson: axg-card: fix 'use-after-free' Buffer 'card->dai_link' is reallocated in 'meson_card_reallocate_links()', so move 'pad' pointer initialization after this function when memory is already reallocated. Kasan bug report: ========== BUG: KASAN: slab-use-after-free in axg_card_add_link+0x76c/0x9bc Read of size 8 at addr ffff000000e8b260 by task modprobe/356 CPU: 0 PID: 356 Comm: modprobe Tainted: G O 6.9.12-sdkernel #1 Call trace: dump_backtrace+0x94/0xec show_stack+0x18/0x24 dump_stack_lvl+0x78/0x90 print_report+0xfc/0x5c0 kasan_report+0xb8/0xfc __asan_load8+0x9c/0xb8 axg_card_add_link+0x76c/0x9bc [snd_soc_meson_axg_sound_card] meson_card_probe+0x344/0x3b8 [snd_soc_meson_card_utils] platform_probe+0x8c/0xf4 really_probe+0x110/0x39c __driver_probe_device+0xb8/0x18c driver_probe_device+0x108/0x1d8 __driver_attach+0xd0/0x25c bus_for_each_dev+0xe0/0x154 driver_attach+0x34/0x44 bus_add_driver+0x134/0x294	2024-09-27	7.8	High

		driver_register+0xa8/0x1e8 __platform_driver_register+0x44/0x54 axg_card_pdrv_init+0x20/0x1000 [snd_soc_meson_axg_sound_card] do_one_initcall+0xdc/0x25c do_init_module+0x10c/0x334 load_module+0x24c4/0x26cc init_module_from_file+0xd4/0x128 __arm64_sys_finit_module+0x1f4/0x41c invoke_syscall+0x60/0x188 el0_svc_common.constprop.0+0x78/0x13c do_el0_svc+0x30/0x40 el0_svc+0x38/0x78 el0t_64_sync_handler+0x100/0x12c el0t_64_sync+0x190/0x194			
CVE-2024-46852	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: dma-buf: heaps: Fix off-by-one in CMA heap fault handler Until VM_DONTEXPAND was added in commit 1c1914d6e8c6 ("dma-buf: heaps: Don't track CMA dma-buf pages under RssFile") it was possible to obtain a mapping larger than the buffer size via mremap and bypass the overflow check in dma_buf_mmap_internal. When using such a mapping to attempt to fault past the end of the buffer, the CMA heap fault handler also checks the fault offset against the buffer size, but gets the boundary wrong by 1. Fix the boundary check so that we don't read off the end of the pages array and insert an arbitrary page in the mapping.	2024-09-27	7.8	High
CVE-2024-46853	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: spi: nxp-fspi: fix the KASAN report out-of-bounds bug Change the memcpy length to fix the out-of-bounds issue when writing the data that is not 4 byte aligned to TX FIFO. To reproduce the issue, write 3 bytes data to NOR chip. dd if=3b of=/dev/mtd0 [36.926103] ========== [36.933409] BUG: KASAN: slab-out-of-bounds in nxp_fspi_exec_op+0x26ec/0x2838 [36.940514] Read of size 4 at addr ffff00081037c2a0 by task dd/455 [36.946721] [36.948235] CPU: 3 UID: 0 PID: 455 Comm: dd Not tainted 6.11.0-rc5-gc7b0e37c8434 #1070 [36.956185] Hardware name: Freescale i.MX8QM MEK (DT) [36.961260] Call trace: [36.963723] dump_backtrace+0x90/0xe8 [36.967414] show_stack+0x18/0x24 [36.970749] dump_stack_lvl+0x78/0x90 [36.974451] print_report+0x114/0x5cc [36.978151] kasan_report+0xa4/0xf0 [36.981670] __asan_report_load_n_noabort+0x1c/0x28 [36.986587] nxp_fspi_exec_op+0x26ec/0x2838 [36.990800] spi_mem_exec_op+0x8ec/0xd30 [36.994762] spi_mem_no_dirmap_read+0x190/0x1e0 [36.999323] spi_mem_dirmap_write+0x238/0x32c [37.003710] spi_nor_write_data+0x220/0x374 [37.007932] spi_nor_write+0x110/0x2e8 [37.011711] mtd_write_oob_std+0x154/0x1f0 [37.015838] mtd_write_oob+0x104/0x1d0 [37.019617] mtd_write+0xb8/0x12c [37.022953] mtdchar_write+0x224/0x47c [37.026732] vfs_write+0x1e4/0x8c8 [37.030163] ksys_write+0xec/0x1d0 [37.033586] __arm64_sys_write+0x6c/0x9c [37.037539] invoke_syscall+0x6c/0x258 [37.041327] el0_svc_common.constprop.0+0x160/0x22c [37.046244] do_el0_svc+0x44/0x5c [37.049589] el0_svc+0x38/0x78 [37.052681] el0t_64_sync_handler+0x13c/0x158 [37.057077] el0t_64_sync+0x190/0x194 [37.060775] [37.062274] Allocated by task 455: [37.065701] kasan_save_stack+0x2c/0x54 [37.069570] kasan_save_track+0x20/0x3c [37.073438] kasan_save_alloc_info+0x40/0x54 [37.077736] __kasan_kmalloc+0xa0/0xb8 [37.081515] __kmalloc_noprof+0x158/0x2f8 [37.085563] mtd_kmalloc_up_to+0x120/0x154 [37.089690] mtdchar_write+0x130/0x47c [37.093469] vfs_write+0x1e4/0x8c8 [37.096901] ksys_write+0xec/0x1d0 [37.100332] __arm64_sys_write+0x6c/0x9c [37.104287] invoke_syscall+0x6c/0x258 [37.108064] el0_svc_common.constprop.0+0x160/0x22c	2024-09-27	7.8	High

		[37.112972] do_el0_svc+0x44/0x5c [37.116319] el0_svc+0x38/0x78 [37.119401] el0t_64_sync_handler+0x13c/0x158 [37.123788] el0t_64_sync+0x190/0x194 [37.127474] [37.128977] The buggy address belongs to the object at ffff00081037c2a0 [37.128977] which belongs to the cache kmalloc-8 of size 8 [37.141177] The buggy address is located 0 bytes inside of [37.141177] allocated 3-byte region [ffff00081037c2a0, ffff00081037c2a3) [37.153465] [37.154971] The buggy address belongs to the physical page: [37.160559] page: refcount:1 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x89037c [37.168596] flags: 0xbfffe0000000000(node=0|zone=2|lastcpupid=0x1ffff) [37.175149] page_type: 0xfdffffff(slab) [37.179021] raw: 0bfffe0000000000 ffff000800002500 dead000000000122 0000000000000000 [37.186788] raw: 0000000000000000 0000000080800080 00000001fdffffff 0000000000000000 [37.194553] page dumped because: kasan: bad access detected [37.200144] [37.201647] Memory state around the buggy address: [37.206460] ffff00081037c180: fa fc fc fc fa fc fc fc fa fc fc fc fa fc fc fc [37.213701] ffff00081037c200: fa fc fc fc 05 fc fc fc 03 fc fc fc 02 fc fc fc [37.220946] >ffff00081037c280: 06 fc fc fc 03 fc fc fc fc fc fc fc fc fc fc fc [37.228186] ^ [37.232473] ffff00081037c300: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [37.239718] ffff00081037c380: fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc fc [37.246962] ========== ---truncated---			
CVE-2024-46859	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: platform/x86: panasonic-laptop: Fix SINF array out of bounds accesses The panasonic laptop code in various places uses the SINF array with index values of 0 - SINF_CUR_BRIGHT(0x0d) without checking that the SINF array is big enough. Not all panasonic laptops have this many SINF array entries, for example the Toughbook CF-18 model only has 10 SINF array entries. So it only supports the AC+DC brightness entries and mute. Check that the SINF array has a minimum size which covers all AC+DC brightness entries and refuse to load if the SINF array is smaller. For higher SINF indexes hide the sysfs attributes when the SINF array does not contain an entry for that attribute, avoiding show()/store() accessing the array out of bounds and add bounds checking to the probe() and resume() code accessing these.	2024-09-27	7.8	High
CVE-2022-43845	ibm - aspera_console	IBM Aspera Console 3.4.0 through 3.4.4 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie.	2024-09-25	7.5	High
CVE-2024-39928	apache software foundation - Apache Linkis Spark EngineConn	In Apache Linkis <= 1.5.0, a Random string security vulnerability in Spark EngineConn, random string generated by the Token when starting Py4j uses the Commons Lang's RandomStringUtils. Users are recommended to upgrade to version 1.6.0, which fixes this issue.	2024-09-25	7.5	High
CVE-2024-6594	watchguard - single_sign-on_client	Improper Handling of Exceptional Conditions vulnerability in the WatchGuard Single Sign-On Client on Windows causes the client to crash while handling malformed commands. An attacker with network access to the client could create a denial of service condition for the Single Sign-On service by repeatedly issuing malformed commands. This issue affects Single Sign-On Client: through 12.7.	2024-09-25	7.5	High
CVE-2024-20350	cisco - Cisco Digital Network Architecture Center (DNA Center)	A vulnerability in the SSH server of Cisco Catalyst Center, formerly Cisco DNA Center, could allow an unauthenticated, remote attacker to impersonate a Cisco Catalyst Center appliance. This vulnerability is due to the presence of a static SSH host key. An attacker could exploit this vulnerability by performing a machine-in-the-middle attack on SSH connections, which could allow the attacker to intercept traffic between SSH clients and a Cisco Catalyst Center appliance. A successful exploit could allow the attacker to impersonate the affected appliance, inject commands into the terminal session, and steal valid user credentials.	2024-09-25	7.5	High
CVE-2024-20433	cisco - multiple products	A vulnerability in the Resource Reservation Protocol (RSVP) feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to cause an affected device to reload unexpectedly, resulting in a denial of service (DoS) condition. This vulnerability is due to a buffer overflow when processing crafted RSVP packets. An attacker could exploit this vulnerability by sending	2024-09-25	7.5	High

		RSVP traffic to an affected device. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.			
CVE-2024-47197	apache - maven_archetype	Exposure of Sensitive Information to an Unauthorized Actor, Insecure Storage of Sensitive Information vulnerability in Maven Archetype Plugin. This issue affects Maven Archetype Plugin: from 3.2.1 before 3.3.0. Users are recommended to upgrade to version 3.3.0, which fixes the issue. Archetype integration testing creates a file called ./target/classes/archetype-it/archetype-settings.xml This file contains all the content from the users ~/.m2/settings.xml file, which often contains information they do not want to publish. We expect that on many developer machines, this also contains credentials. When the user runs mvn verify again (without a mvn clean), this file becomes part of the final artifact. If a developer were to publish this into Maven Central or any other remote repository (whether as a release or a snapshot) their credentials would be published without them knowing.	2024-09-26	7.5	High
CVE-2024-37125	dell - SmartFabric OS10 Software	Dell SmartFabric OS10 Software, versions 10.5.6.x, 10.5.5.x, 10.5.4.x,10.5.3.x, contains an Uncontrolled Resource Consumption vulnerability. A remote unauthenticated host could potentially exploit this vulnerability leading to a denial of service.	2024-09-26	7.5	High
CVE-2024-47293	huawei - multiple products	Out-of-bounds write vulnerability in the HAL-WIFI module Impact: Successful exploitation of this vulnerability may affect availability.	2024-09-27	7.5	High
CVE-2024-47294	huawei - multiple products	Access permission verification vulnerability in the input method framework module Impact: Successful exploitation of this vulnerability may affect availability.	2024-09-27	7.5	High
CVE-2024-9136	huawei - multiple products	Access permission verification vulnerability in the App Multiplier module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-09-27	7.5	High
CVE-2024-43191	ibm - Cloud Pak for Multicloud Management	IBM ManageIQ could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted yaml file request.	2024-09-26	7.2	High
CVE-2024-9123	google - Chrome	Integer overflow in Skia in Google Chrome prior to 129.0.6668.70 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	2024-09-25	7.1	High
CVE-2024-39577	dell - SmartFabric OS10 Software	Dell SmartFabric OS10 Software, versions 10.5.6.x, 10.5.5.x, 10.5.4.x, 10.5.3.x, contains an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability leading to code execution.	2024-09-26	7.1	High
CVE-2024-46854	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: dpaa: Pad packets to ETH_ZLEN When sending packets under 60 bytes, up to three bytes of the buffer following the data may be leaked. Avoid this by extending all packets to ETH_ZLEN, ensuring nothing is leaked in the padding. This bug can be reproduced by running $ ping -s 11 destination	2024-09-27	7.1	High
CVE-2024-46865	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: fou: fix initialization of grc The grc must be initialize first. There can be a condition where if fou is NULL, goto out will be executed and grc would be used uninitialized.	2024-09-27	7.1	High
CVE-2024-9284	tp-link - TL-WR841ND	A vulnerability was found in TP-LINK TL-WR841ND up to 20240920. It has been rated as critical. Affected by this issue is some unknown functionality of the file /userRpm/popupSiteSurveyRpm.htm. The manipulation of the argument ssid leads to stack-based buffer overflow. The attack may 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.	2024-09-27	7.1	High
CVE-2024-46858	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: Fix uaf in __timer_delete_sync There are two paths to access mptcp_pm_del_add_timer, result in a race condition: CPU1 CPU2 ==== ==== net_rx_action napi_poll netlink_sendmsg __napi_poll netlink_unicast process_backlog netlink_unicast_kernel __netif_receive_skb genl_rcv __netif_receive_skb_one_core netlink_rcv_skb NF_HOOK genl_rcv_msg ip_local_deliver_finish genl_family_rcv_msg ip_protocol_deliver_rcu genl_family_rcv_msg_doit tcp_v4_rcv mptcp_pm_nl_flush_addrs_doit tcp_v4_do_rcv mptcp_nl_remove_addrs_list	2024-09-27	7	High

		tcp_rcv_established mptcp_pm_remove_addrs_and_subflows tcp_data_queue remove_anno_list_by_saddr mptcp_incoming_options mptcp_pm_del_add_timer mptcp_pm_del_add_timer kfree(entry) In remove_anno_list_by_saddr(running on CPU2), after leaving the critical zone protected by "pm.lock", the entry will be released, which leads to the occurrence of uaf in the mptcp_pm_del_add_timer(running on CPU1). Keeping a reference to add_timer inside the lock, and calling sk_stop_timer_sync() with this reference, instead of "entry->add_timer". Move list_del(&entry->list) to mptcp_pm_del_add_timer and inside the pm lock, do not directly access any members of the entry outside the pm lock, which can avoid similar "entry->x" uaf.			
CVE-2022-49039	synology - Synology Drive Client	Out-of-bounds write vulnerability in backup task management functionality in Synology Drive Client before 3.4.0-15721 allows local users with administrator privileges to execute arbitrary commands via unspecified vectors.	2024-09-26	6.7	Medium
CVE-2024-38324	ibm - storage_defender	IBM Storage Defender 2.0.0 through 2.0.7 on-prem defender-sensor-cmd CLI does not validate server name during registration and unregistration operations which could expose sensitive information to an attacker with access to the system.	2024-09-25	6.5	Medium
CVE-2024-20414	cisco - multiple products	A vulnerability in the web UI feature of Cisco IOS Software and Cisco IOS XE Software could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system through the web UI. This vulnerability is due to incorrectly accepting configuration changes through the HTTP GET method. An attacker could exploit this vulnerability by persuading a currently authenticated administrator to follow a crafted link. A successful exploit could allow the attacker to change the configuration of the affected device.	2024-09-25	6.5	Medium
CVE-2024-20508	cisco - multiple products	A vulnerability in Cisco Unified Threat Defense (UTD) Snort Intrusion Prevention System (IPS) Engine for Cisco IOS XE Software could allow an unauthenticated, remote attacker to bypass configured security policies or cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient validation of HTTP requests when they are processed by Cisco UTD Snort IPS Engine. An attacker could exploit this vulnerability by sending a crafted HTTP request through an affected device. A successful exploit could allow the attacker to trigger a reload of the Snort process. If the action in case of Cisco UTD Snort IPS Engine failure is set to the default, fail-open, successful exploitation of this vulnerability could allow the attacker to bypass configured security policies. If the action in case of Cisco UTD Snort IPS Engine failure is set to fail-close, successful exploitation of this vulnerability could cause traffic that is configured to be inspected by Cisco UTD Snort IPS Engine to be dropped.	2024-09-25	6.5	Medium
CVE-2022-49037	synology - Synology Drive Client	Insertion of sensitive information into log file vulnerability in proxy settings component in Synology Drive Client before 3.3.0-15082 allows remote authenticated users to obtain sensitive information via unspecified vectors.	2024-09-26	6.5	Medium
CVE-2024-20496	cisco - multiple products	A vulnerability in the UDP packet validation code of Cisco SD-WAN vEdge Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected system. This vulnerability is due to incorrect handling of a specific type of malformed UDP packet. An attacker in a machine-in-the-middle position could exploit this vulnerability by sending crafted UDP packets to an affected device. A successful exploit could allow the attacker to cause the device to reboot, resulting in a DoS condition on the affected system.	2024-09-25	6.1	Medium
CVE-2024-20465	cisco - IOS	A vulnerability in the access control list (ACL) programming of Cisco IOS Software running on Cisco Industrial Ethernet 4000, 4010, and 5000 Series Switches could allow an unauthenticated, remote attacker to bypass a configured ACL. This vulnerability is due to the incorrect handling of IPv4 ACLs on switched virtual interfaces when an administrator enables and disables Resilient Ethernet Protocol (REP). An attacker could exploit this vulnerability by attempting to send traffic through an affected device. A successful exploit could allow the attacker to bypass an ACL on the affected device.	2024-09-25	5.8	Medium
CVE-2024-40703	ibm - multiple products	IBM Cognos Analytics 11.2.0, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 12.0.0, 12.0.1, 12.0.2, 12.0.3, and IBM Cognos Analytics Reports for iOS 11.0.0.7 could allow a local attacker to obtain sensitive information in the form of an API key. An attacker could use this information to launch further attacks against affected applications.	2024-09-22	5.5	Medium
CVE-2023-52949	synology - active_backup_for_business_agent	Missing authentication for critical function vulnerability in proxy settings functionality in Synology Active Backup for Business Agent before 2.7.0-3221 allows local users to obtain user credential via unspecified vectors.	2024-09-26	5.5	Medium

CVE-2024-47290	huawei - multiple products	Input validation vulnerability in the USB service module Impact: Successful exploitation of this vulnerability may affect availability.	2024-09-27	5.5	Medium
CVE-2024-47291	huawei - multiple products	Permission vulnerability in the ActivityManagerService (AMS) module Impact: Successful exploitation of this vulnerability may affect availability.	2024-09-27	5.5	Medium
CVE-2024-47292	huawei - multiple products	Path traversal vulnerability in the Bluetooth module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-09-27	5.5	Medium
CVE-2024-46803	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amdkfd: Check debug trap enable before write dbg_ev_file In interrupt context, write dbg_ev_file will be run by work queue. It will cause write dbg_ev_file execution after debug_trap_disable, which will cause NULL pointer access. v2: cancel work "debug_event_workarea" before set dbg_ev_file as NULL.	2024-09-27	5.5	Medium
CVE-2024-46805	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: fix the waring dereferencing hive Check the amdgpu_hive_info *hive that maybe is NULL.	2024-09-27	5.5	Medium
CVE-2024-46806	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix the warning division or modulo by zero Checks the partition mode and returns an error for an invalid mode.	2024-09-27	5.5	Medium
CVE-2024-46807	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amd/amdgpu: Check tbo resource pointer Validate tbo resource pointer, skip if NULL	2024-09-27	5.5	Medium
CVE-2024-46808	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Add missing NULL pointer check within dpcd_extend_address_range [Why & How] ASSERT if return NULL from kcalloc.	2024-09-27	5.5	Medium
CVE-2024-46809	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Check BIOS images before it is used BIOS images may fail to load and null checks are added before they are used. This fixes 6 NULL_RETURNS issues reported by Coverity.	2024-09-27	5.5	Medium
CVE-2024-46810	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/bridge: tc358767: Check if fully initialized before signalling HPD event via IRQ Make sure the connector is fully initialized before signalling any HPD events via drm_kms_helper_hotplug_event(), otherwise this may lead to NULL pointer dereference.	2024-09-27	5.5	Medium
CVE-2024-46819	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: the warning dereferencing obj for nbio_v7_4 if ras_manager obj null, don't print NBIO err data	2024-09-27	5.5	Medium
CVE-2024-46822	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: arm64: acpi: Harden get_cpu_for_acpi_id() against missing CPU entry In a review discussion of the changes to support vCPU hotplug where a check was added on the GICC being enabled if was online, it was noted that there is need to map back to the cpu and use that to index into a cpumask. As such, a valid ID is needed. If an MPIDR check fails in acpi_map_gic_cpu_interface() it is possible for the entry in cpu_madt_gicc[cpu] == NULL. This function would then cause a NULL pointer dereference. Whilst a path to trigger this has not been established, harden this caller against the possibility.	2024-09-27	5.5	Medium
CVE-2024-46824	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: iommufd: Require drivers to supply the cache_invalidate_user ops If drivers don't do this then iommufd will oops invalidation ioctls with something like: Unable to handle kernel NULL pointer dereference at virtual address 0000000000000000 Mem abort info: ESR = 0x0000000086000004 EC = 0x21: IABT (current EL), IL = 32 bits SET = 0, FnV = 0 EA = 0, S1PTW = 0 FSC = 0x04: level 0 translation fault user pgtable: 4k pages, 48-bit VAs, pgdp=0000000101059000 [0000000000000000] pgd=0000000000000000, p4d=0000000000000000 Internal error: Oops: 0000000086000004 [#1] PREEMPT SMP Modules linked in: CPU: 2 PID: 371 Comm: qemu-system-aar Not tainted 6.8.0-rc7-gde77230ac23a #9 Hardware name: linux,dummy-virt (DT) pstate: 81400809 (Nzcv daif +PAN -UAO -TCO +DIT -SSBS BTYPE=-c) pc : 0x0 lr : iommufd_hwpt_invalidate+0xa4/0x204 sp : ffff800080f3bcc0 x29: ffff800080f3bcf0 x28: ffff0000c369b300 x27: 0000000000000000 x26: 0000000000000000 x25: 0000000000000000 x24:	2024-09-27	5.5	Medium

		0000000000000000 x23: 0000000000000000 x22: 00000000c1e334a0 x21: ffff0000c1e334a0 x20: ffff800080f3bd38 x19: ffff800080f3bd58 x18: 0000000000000000 x17: 0000000000000000 x16: 0000000000000000 x15: 0000ffff8240d6d8 x14: 0000000000000000 x13: 0000000000000000 x12: 0000000000000000 x11: 0000000000000000 x10: 0000000000000000 x9 : 0000000000000000 x8 : 0000001000000002 x7 : 0000fffeac1ec950 x6 : 0000000000000000 x5 : ffff800080f3bd78 x4 : 0000000000000003 x3 : 0000000000000002 x2 : 0000000000000000 x1 : ffff800080f3bcc8 x0 : ffff0000c6034d80 Call trace: 0x0 iommufd_fops_ioctl+0x154/0x274 __arm64_sys_ioctl+0xac/0xf0 invoke_syscall+0x48/0x110 el0_svc_common.constprop.0+0x40/0xe0 do_el0_svc+0x1c/0x28 el0_svc+0x34/0xb4 el0t_64_sync_handler+0x120/0x12c el0t_64_sync+0x190/0x194 All existing drivers implement this op for nesting, this is mostly a bisection aid.			
CVE-2024-46829	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: rtmutex: Drop rt_mutex::wait_lock before scheduling rt_mutex_handle_deadlock() is called with rt_mutex::wait_lock held. In the good case it returns with the lock held and in the deadlock case it emits a warning and goes into an endless scheduling loop with the lock held, which triggers the 'scheduling in atomic' warning. Unlock rt_mutex::wait_lock in the dead lock case before issuing the warning and dropping into the schedule for ever loop. [tglx: Moved unlock before the WARN(), removed the pointless comment, massaged changelog, added Fixes tag]	2024-09-27	5.5	Medium
CVE-2024-46835	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu: Fix smatch static checker warning adev->gfx.imu.funcs could be NULL	2024-09-27	5.5	Medium
CVE-2024-46847	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mm: vmalloc: ensure vmap_block is initialised before adding to queue Commit 8c61291fd850 ("mm: fix incorrect vbq reference in purge_fragmented_block") extended the 'vmap_block' structure to contain a 'cpu' field which is set at allocation time to the id of the initializing CPU. When a new 'vmap_block' is being instantiated by new_vmap_block(), the partially initialised structure is added to the local 'vmap_block_queue' xarray before the 'cpu' field has been initialised. If another CPU is concurrently walking the xarray (e.g. via vm_unmap_aliases()), then it may perform an out-of-bounds access to the remote queue thanks to an uninitialised index. This has been observed as UBSAN errors in Android: | Internal error: UBSAN: array index out of bounds: 00000000f2005512 [#1] PREEMPT SMP | | Call trace: | purge_fragmented_block+0x204/0x21c | _vm_unmap_aliases+0x170/0x378 | vm_unmap_aliases+0x1c/0x28 | change_memory_common+0x1dc/0x26c | set_memory_ro+0x18/0x24 | module_enable_ro+0x98/0x238 | do_init_module+0x1b0/0x310 Move the initialisation of 'vb->cpu' in new_vmap_block() ahead of the addition to the xarray.	2024-09-27	5.5	Medium
CVE-2024-46848	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: perf/x86/intel: Limit the period on Haswell Running the ltp test cve-2015-3290 concurrently reports the following warnings. perfevents: irq loop stuck! WARNING: CPU: 31 PID: 32438 at arch/x86/events/intel/core.c:3174 intel_pmu_handle_irq+0x285/0x370 Call Trace: <NMI> ? __warn+0xa4/0x220 ? intel_pmu_handle_irq+0x285/0x370 ? __report_bug+0x123/0x130 ? intel_pmu_handle_irq+0x285/0x370 ? __report_bug+0x123/0x130 ? intel_pmu_handle_irq+0x285/0x370 ? report_bug+0x3e/0xa0 ? handle_bug+0x3c/0x70	2024-09-27	5.5	Medium

		? exc_invalid_op+0x18/0x50 ? asm_exc_invalid_op+0x1a/0x20 ? irq_work_claim+0x1e/0x40 ? intel_pmu_handle_irq+0x285/0x370 perf_event_nmi_handler+0x3d/0x60 nmi_handle+0x104/0x330 Thanks to Thomas Gleixner's analysis, the issue is caused by the low initial period (1) of the frequency estimation algorithm, which triggers the defects of the HW, specifically erratum HSW11 and HSW143. (For the details, please refer https://lore.kernel.org/lkml/87plq9l5d2.ffs@tglx/) The HSW11 requires a period larger than 100 for the INST_RETIRED.ALL event, but the initial period in the freq mode is 1. The erratum is the same as the BDM11, which has been supported in the kernel. A minimum period of 128 is enforced as well on HSW. HSW143 is regarding that the fixed counter 1 may overcount 32 with the Hyper-Threading is enabled. However, based on the test, the hardware has more issues than it tells. Besides the fixed counter 1, the message 'interrupt took too long' can be observed on any counter which was armed with a period < 32 and two events expired in the same NMI. A minimum period of 32 is enforced for the rest of the events. The recommended workaround code of the HSW143 is not implemented. Because it only addresses the issue for the fixed counter. It brings extra overhead through extra MSR writing. No related overcounting issue has been reported so far.			
CVE-2024-46855	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_socket: fix sk refcount leaks We must put 'sk' reference before returning.	2024-09-27	5.5	Medium
CVE-2024-46856	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: phy: dp83822: Fix NULL pointer dereference on DP83825 devices The probe() function is only used for DP83822 and DP83826 PHY, leaving the private data pointer uninitialized for the DP83825 models which causes a NULL pointer dereference in the recently introduced/changed functions dp8382x_config_init() and dp83822_set_wol(). Add the dp8382x_probe() function, so all PHY models will have a valid private data pointer to fix this issue and also prevent similar issues in the future.	2024-09-27	5.5	Medium
CVE-2024-46857	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net/mlx5: Fix bridge mode operations when there are no VFs Currently, trying to set the bridge mode attribute when numvfs=0 leads to a crash: bridge link set dev eth2 hwmode vepa [168.967392] BUG: kernel NULL pointer dereference, address: 0000000000000030 [...] [168.969989] RIP: 0010:mlx5_add_flow_rules+0x1f/0x300 [mlx5_core] [...] [168.976037] Call Trace: [168.976188] <TASK> [168.978620] _mlx5_eswitch_set_vepa_locked+0x113/0x230 [mlx5_core] [168.979074] mlx5_eswitch_set_vepa+0x7f/0xa0 [mlx5_core] [168.979471] rtnl_bridge_setlink+0xe9/0x1f0 [168.979714] rtnetlink_rcv_msg+0x159/0x400 [168.980451] netlink_rcv_skb+0x54/0x100 [168.980675] netlink_unicast+0x241/0x360 [168.980918] netlink_sendmsg+0x1f6/0x430 [168.981162] ____sys_sendmsg+0x3bb/0x3f0 [168.982155] ___sys_sendmsg+0x88/0xd0 [168.985036] __sys_sendmsg+0x59/0xa0 [168.985477] do_syscall_64+0x79/0x150 [168.987273] entry_SYSCALL_64_after_hwframe+0x76/0x7e [168.987773] RIP: 0033:0x7f8f7950f917 (esw->fdb_table.legacy.vepa_fdb is null) The bridge mode is only relevant when there are multiple functions per port. Therefore, prevent setting and getting this setting when there are no VFs. Note that after this change, there are no settings to change on the PF interface using `bridge link` when there are no VFs, so the interface no longer appears in the `bridge link` output.	2024-09-27	5.5	Medium
CVE-2024-46860	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: wifi: mt76: mt7921: fix NULL pointer access in mt7921_ipv6_addr_change When disabling wifi mt7921_ipv6_addr_change() is called as a notifier. At this point mvif->phy is already NULL so we cannot use it here.	2024-09-27	5.5	Medium
CVE-2024-46861	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: usbnet: ipheth: do not stop RX on failing RX callback RX callbacks can fail for multiple reasons: * Payload too short	2024-09-27	5.5	Medium

		* Payload formatted incorrecly (e.g. bad NCM framing) * Lack of memory None of these should cause the driver to seize up. Make such failures non-critical and continue processing further incoming URBs.			
CVE-2024-46862	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: soc-acpi-intel-mtl-match: add missing empty item There is no links_num in struct snd_soc_acpi_mach {}, and we test !link->num_adr as a condition to end the loop in hda_sdw_machine_select(). So an empty item in struct snd_soc_acpi_link_adr array is required.	2024-09-27	5.5	Medium
CVE-2024-46863	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ASoC: Intel: soc-acpi-intel-lnl-match: add missing empty item There is no links_num in struct snd_soc_acpi_mach {}, and we test !link->num_adr as a condition to end the loop in hda_sdw_machine_select(). So an empty item in struct snd_soc_acpi_link_adr array is required.	2024-09-27	5.5	Medium
CVE-2024-46864	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: x86/hyperv: fix kexec crash due to VP assist page corruption commit 9636be85cc5b ("x86/hyperv: Fix hyperv_pcpu_input_arg handling when CPUs go online/offline") introduces a new cpuhp state for hyperv initialization. cpuhp_setup_state() returns the state number if state is CPUHP_AP_ONLINE_DYN or CPUHP_BP_PREPARE_DYN and 0 for all other states. For the hyperv case, since a new cpuhp state was introduced it would return 0. However, in hv_machine_shutdown(), the cpuhp_remove_state() call is conditioned upon "hyperv_init_cpuhp > 0". This will never be true and so hv_cpu_die() won't be called on all CPUs. This means the VP assist page won't be reset. When the kexec kernel tries to setup the VP assist page again, the hypervisor corrupts the memory region of the old VP assist page causing a panic in case the kexec kernel is using that memory elsewhere. This was originally fixed in commit dfe94d4086e4 ("x86/hyperv: Fix kexec panic/hang issues"). Get rid of hyperv_init_cpuhp entirely since we are no longer using a dynamic cpuhp state and use CPUHP_AP_HYPERV_ONLINE directly with cpuhp_remove_state().	2024-09-27	5.5	Medium
CVE-2024-46866	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/xe/client: add missing bo locking in show_meminfo() bo_meminfo() wants to inspect bo state like tt and the ttm resource, however this state can change at any point leading to stuff like NPD and UAF, if the bo lock is not held. Grab the bo lock when calling bo_meminfo(), ensuring we drop any spinlocks first. In the case of object_idr we now also need to hold a ref. v2 (MattB) - Also add xe_bo_assert_held() (cherry picked from commit 4f63d712fa104c3ebefcb289d1e733e86d8698c7)	2024-09-27	5.5	Medium
CVE-2024-46867	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/xe/client: fix deadlock in show_meminfo() There is a real deadlock as well as sleeping in atomic() bug in here, if the bo put happens to be the last ref, since bo destruction wants to grab the same spinlock and sleeping locks. Fix that by dropping the ref using xe_bo_put_deferred(), and moving the final commit outside of the lock. Dropping the lock around the put is tricky since the bo can go out of scope and delete itself from the list, making it difficult to navigate to the next list entry. (cherry picked from commit 0083b8e6f11d7662283a267d4ce7c966812ffd8a)	2024-09-27	5.5	Medium
CVE-2024-46868	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: firmware: qcom: uefisecapp: Fix deadlock in qcuefi_acquire() If the __qcuefi pointer is not set, then in the original code, we would hold onto the lock. That means that if we tried to set it later, then it would cause a deadlock. Drop the lock on the error path. That's what all the callers are expecting.	2024-09-27	5.5	Medium
CVE-2024-20475	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Catalyst SD-WAN Manager, formerly Cisco SD-WAN vManage, could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious data into a specific data field in an affected interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface.	2024-09-25	5.4	Medium
CVE-2024-40761	apache software foundation - Apache Answer	Inadequate Encryption Strength vulnerability in Apache Answer. This issue affects Apache Answer: through 1.3.5. Using the MD5 value of a user's email to access Gravatar is insecure and can lead to the leakage of user email. The official recommendation is to use SHA256 instead. Users are recommended to upgrade to version 1.4.0, which fixes the issue.	2024-09-25	5.3	Medium

CVE-2023-52950	synology - active_backup_for_business_agent	Missing encryption of sensitive data vulnerability in login component in Synology Active Backup for Business Agent before 2.7.0-3221 allows adjacent man-in-the-middle attackers to obtain user credential via unspecified vectors.	2024-09-26	5.3	Medium
CVE-2024-8118	grafana - Grafana	In Grafana, the wrong permission is applied to the alert rule write API endpoint, allowing users with permission to write external alert instances to also write alert rules.	2024-09-26	5.1	Medium
CVE-2023-52948	synology - active_backup_for_business_agent	Missing encryption of sensitive data vulnerability in settings functionality in Synology Active Backup for Business Agent before 2.7.0-3221 allows local users to obtain user credential via unspecified vectors.	2024-09-26	5	Medium
CVE-2024-38266	zyxel - VMG8825-T50K firmware	An improper restriction of operations within the bounds of a memory buffer in the parameter type parser of the Zyxel VMG8825-T50K firmware versions through 5.50(ABOM.8)C0 could allow an authenticated attacker with administrator privileges to cause potential memory corruptions, resulting in a thread crash on an affected device.	2024-09-24	4.9	Medium
CVE-2024-38267	zyxel - wx5600-t0_firmware	An improper restriction of operations within the bounds of a memory buffer in the IPv6 address parser of the Zyxel VMG8825-T50K firmware versions through 5.50(ABOM.8)C0 could allow an authenticated attacker with administrator privileges to cause potential memory corruptions, resulting in a thread crash on an affected device.	2024-09-24	4.9	Medium
CVE-2024-38268	zyxel - wx5600-t0_firmware	An improper restriction of operations within the bounds of a memory buffer in the MAC address parser of the Zyxel VMG8825-T50K firmware versions through 5.50(ABOM.8)C0 could allow an authenticated attacker with administrator privileges to cause potential memory corruptions, resulting in a thread crash on an affected device.	2024-09-24	4.9	Medium
CVE-2024-38269	zyxel - wx5600-t0_firmware	An improper restriction of operations within the bounds of a memory buffer in the USB file-sharing handler of the Zyxel VMG8825-T50K firmware versions through 5.50(ABOM.8)C0 could allow an authenticated attacker with administrator privileges to cause potential memory corruptions, resulting in a thread crash on an affected device.	2024-09-24	4.9	Medium
CVE-2024-46850	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid race between dcn35_set_drr() and dc_state_destruct() dc_state_destruct() nulls the resource context of the DC state. The pipe context passed to dcn35_set_drr() is a member of this resource context. If dc_state_destruct() is called parallel to the IRQ processing (which calls dcn35_set_drr() at some point), we can end up using already nulled function callback fields of struct stream_resource. The logic in dcn35_set_drr() already tries to avoid this, by checking tg against NULL. But if the nulling happens exactly after the NULL check and before the next access, then we get a race. Avoid this by copying tg first to a local variable, and then use this variable for all the operations. This should work, as long as nobody frees the resource pool where the timing generators live. (cherry picked from commit 0607a50c004798a96e62c089a4c34c220179dcb5)	2024-09-27	4.7	Medium
CVE-2024-46851	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Avoid race between dcn10_set_drr() and dc_state_destruct() dc_state_destruct() nulls the resource context of the DC state. The pipe context passed to dcn10_set_drr() is a member of this resource context. If dc_state_destruct() is called parallel to the IRQ processing (which calls dcn10_set_drr() at some point), we can end up using already nulled function callback fields of struct stream_resource. The logic in dcn10_set_drr() already tries to avoid this, by checking tg against NULL. But if the nulling happens exactly after the NULL check and before the next access, then we get a race. Avoid this by copying tg first to a local variable, and then use this variable for all the operations. This should work, as long as nobody frees the resource pool where the timing generators live. (cherry picked from commit a3cc326a43bdc48fbdf53443e1027a03e309b643)	2024-09-27	4.7	Medium
CVE-2024-39431	google - multiple products	In UMTS RLC driver, there is a possible out of bounds write due to a missing bounds check. This could lead to remote denial of service with System execution privileges needed.	2024-09-27	4.5	Medium
CVE-2024-39432	google - multiple products	In UMTS RLC driver, there is a possible out of bounds read due to a missing bounds check. This could lead to remote denial of service with System execution privileges needed.	2024-09-27	4.5	Medium
CVE-2022-49040	synology - Synology Drive Client	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in connection management functionality in Synology Drive Client before 3.4.0-15721 allows local users with administrator privileges to crash the client via unspecified vectors.	2024-09-26	4.4	Medium
CVE-2022-49041	synology - Synology Drive Client	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in backup task management functionality in Synology Drive Client before 3.4.0-15721 allows local users with administrator privileges to crash the client via unspecified vectors.	2024-09-26	4.4	Medium

CVE-2023-46175	ibm - Cloud Pak for Multicloud Management	IBM Cloud Pak for Multicloud Management 2.3 through 2.3 FP8 stores user credentials in a log file plain clear text which can be read by a privileged user.	2024-09-26	4.4	Medium
CVE-2024-7259	red hat - Red Hat Virtualization 4	A flaw was found in oVirt. A user with administrator privileges, including users with the ReadOnlyAdmin permission, may be able to use browser developer tools to view Provider passwords in cleartext.	2024-09-26	4.4	Medium
CVE-2024-39433	google - multiple products	In drm service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2024-09-27	4.4	Medium
CVE-2024-39434	google - multiple products	In drm service, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed.	2024-09-27	4.4	Medium
CVE-2023-7281	google - Chrome	Inappropriate implementation in Compositing in Google Chrome prior to 119.0.6045.105 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2024-09-23	4.3	Medium
CVE-2023-7282	google - Chrome	Inappropriate implementation in Navigation in Google Chrome prior to 113.0.5672.63 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	2024-09-23	4.3	Medium
CVE-2024-7019	google - Chrome	Inappropriate implementation in UI in Google Chrome prior to 124.0.6367.60 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2024-09-23	4.3	Medium
CVE-2024-7020	google - Chrome	Inappropriate implementation in Autofill in Google Chrome prior to 124.0.6367.60 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2024-09-23	4.3	Medium
CVE-2024-20434	cisco - Cisco IOS XE Software	A vulnerability in Cisco IOS XE Software could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on the control plane of an affected device. This vulnerability is due to improper handling of frames with VLAN tag information. An attacker could exploit this vulnerability by sending crafted frames to an affected device. A successful exploit could allow the attacker to render the control plane of the affected device unresponsive. The device would not be accessible through the console or CLI, and it would not respond to ping requests, SNMP requests, or requests from other control plane protocols. Traffic that is traversing the device through the data plane is not affected. A reload of the device is required to restore control plane services.	2024-09-25	4.3	Medium
CVE-2024-31899	ibm - Cognos Command Center	IBM Cognos Command Center 10.2.4.1 and 10.2.5 could disclose highly sensitive user information to an authenticated user with physical access to the device.	2024-09-26	4.3	Medium
CVE-2023-52947	synology - active_backup_for_business_agent	Missing authentication for critical function vulnerability in logout functionality in Synology Active Backup for Business Agent before 2.6.3-3101 allows local users to logout the client via unspecified vectors. The backup functionality will continue to operate and will not be affected by the logout.	2024-09-26	3.3	Low

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.