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

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

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 September to 7th 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**

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 سبتمبر إلى ٧ 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**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2024-45076	IBM	IBM webMethods Integration 10.15 could allow an authenticated user to upload and execute arbitrary files which could be executed on the underlying operating system.	2024-09-04	9.9	Critical
CVE-2024-38650	Veeam	An authentication bypass vulnerability can allow a low privileged attacker to access the NTLM hash of service account on the VSPC server.	2024-09-07	9.9	Critical
CVE-2024-39714	Veeam	A code injection vulnerability that permits a low-privileged user to upload arbitrary files to the server, leading to remote code execution on VSPC server.	2024-09-07	9.9	Critical
CVE-2024-7261	Zyxel	The improper neutralization of special elements in the parameter "host" in the CGI program of Zyxel NWA1123ACv3 firmware version 6.70(ABVT.4) and earlier, WAC500 firmware version 6.70(ABVS.4) and earlier, WAX655E firmware version 7.00(ACDO.1) and earlier, WBE530 firmware version 7.00(ACLE.1) and earlier, and USG LITE 60AX firmware version V2.00(ACIP.2) could allow an unauthenticated attacker to execute OS commands by sending a crafted cookie to a vulnerable device.	2024-09-03	9.8	Critical
CVE-2024-8381	Mozilla	A potentially exploitable type confusion could be triggered when looking up a property name on an object being used as the `with` environment. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15.	2024-09-03	9.8	Critical
CVE-2024-8384	Mozilla	The JavaScript garbage collector could mis-color cross-compartment objects if OOM conditions were detected at the right point between two passes. This could have led to memory corruption. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15.	2024-09-03	9.8	Critical
CVE-2024-8385	Mozilla	A difference in the handling of StructFields and ArrayTypes in WASM could be used to trigger an exploitable type confusion vulnerability. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Thunderbird < 128.2.	2024-09-03	9.8	Critical
CVE-2024-8387	Mozilla	Memory safety bugs present in Firefox 129, Firefox ESR 128.1, and Thunderbird 128.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Thunderbird < 128.2.	2024-09-03	9.8	Critical
CVE-2024-8389	Mozilla	Memory safety bugs present in Firefox 129. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 130.	2024-09-03	9.8	Critical
CVE-2024-20439	Cisco	A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to log in to an affected system by using a static administrative credential.	2024-09-04	9.8	Critical

		This vulnerability is due to an undocumented static user credential for an administrative account. An attacker could exploit this vulnerability by using the static credentials to log in to the affected system. A successful exploit could allow the attacker to log in to the affected system with administrative privileges over the API of the Cisco Smart Licensing Utility application.			
CVE-2024-40711	Veeam	A deserialization of untrusted data vulnerability with a malicious payload can allow an unauthenticated remote code execution (RCE).	2024-09-07	9.8	Critical
CVE-2024-45443	Huawei	Directory traversal vulnerability in the cust module Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	2024-09-04	9.1	Critical
CVE-2024-42024	Veeam	A vulnerability that allows an attacker in possession of the Veeam ONE Agent service account credentials to perform remote code execution on the machine where the Veeam ONE Agent is installed.	2024-09-07	9.1	Critical
CVE-2024-42019	Veeam	A vulnerability that allows an attacker to access the NTLM hash of the Veeam Reporter Service service account. This attack requires user interaction and data collected from Veeam Backup & Replication.	2024-09-07	9	Critical
CVE-2024-8382	Mozilla	Internal browser event interfaces were exposed to web content when privileged EventHandler listener callbacks ran for those events. Web content that tried to use those interfaces would not be able to use them with elevated privileges, but their presence would indicate certain browser features had been used, such as when a user opened the Dev Tools console. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, Firefox ESR < 115.15, Thunderbird < 128.2, and Thunderbird < 115.15.	2024-09-03	8.8	High
CVE-2024-7970	Google	Out of bounds write in V8 in Google Chrome prior to 128.0.6613.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-09-03	8.8	High
CVE-2024-8362	Google	Use after free in WebAudio in Google Chrome prior to 128.0.6613.119 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2024-09-03	8.8	High
CVE-2024-45075	IBM	IBM webMethods Integration 10.15 could allow an authenticated user to create scheduler tasks that would allow them to escalate their privileges to administrator due to missing authentication.	2024-09-04	8.8	High
CVE-2024-38486	Dell	Dell SmartFabric OS10 Software, version(s) 10.5.5.4 through 10.5.5.10 and 10.5.6.x , contain(s) 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 Command execution.	2024-09-06	8.8	High
CVE-2024-40710	Veeam	A series of related high-severity vulnerabilities, the most notable enabling remote code execution (RCE) as the service account and extraction of sensitive information (savedcredentials and passwords). Exploiting these vulnerabilities requires a user who has been assigned a low-privileged role within Veeam Backup & Replication.	2024-09-07	8.8	High
CVE-2024-40718	Veeam	A server side request forgery vulnerability allows a low-privileged user to perform local privilege escalation through exploiting an SSRF vulnerability.	2024-09-07	8.8	High
CVE-2024-38651	Veeam	A code injection vulnerability can allow a low-privileged user to overwrite files on that VSPC server, which can lead to remote code execution on VSPC server.	2024-09-07	8.5	High
CVE-2024-39715	Veeam	A code injection vulnerability that allows a low-privileged user with REST API access granted to remotely upload arbitrary files to the VSPC server using REST API, leading to remote code execution on VSPC server.	2024-09-07	8.5	High
CVE-2024-40714	Veeam	An improper certificate validation vulnerability in TLS certificate validation allows an attacker on the same network to intercept sensitive credentials during restore operations.	2024-09-07	8.3	High
CVE-2024-42057	Zyxel	A command injection vulnerability in the IPSec VPN feature of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an unauthenticated attacker to execute some OS commands on an affected device by sending a crafted username to the vulnerable device. Note that this attack could be successful only if the device was configured in User-Based-PSK authentication mode and a valid user with a long username exceeding 28 characters exists.	2024-09-03	8.1	High

CVE-2024-45098	IBM	IBM Aspera Faspex 5.0.0 through 5.0.9 could allow a user to bypass intended access restrictions and conduct resource modification.	2024-09-05	8.1	High
CVE-2024-39585	Dell	Dell SmartFabric OS10 Software, version(s) 10.5.5.4 through 10.5.5.10 and 10.5.6.x, contain(s) an Use of Hard-coded Password vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Client-side request forgery and Information disclosure.	2024-09-06	8.1	High
CVE-2024-39718	Veeam	An improper input validation vulnerability that allows a low-privileged user to remotely remove files on the system with permissions equivalent to those of the service account.	2024-09-07	8.1	High
CVE-2024-44964	Linux	In the Linux kernel, the following vulnerability has been resolved: idpf: fix memory leaks and crashes while performing a soft reset The second tagged commit introduced a UAF, as it removed restoring q_vector->vport pointers after reinitializating the structures. This is due to that all queue allocation functions are performed here with the new temporary vport structure and those functions rewrite the backpointers to the vport. Then, this new struct is freed and the pointers start leading to nowhere. But generally speaking, the current logic is very fragile. It claims to be more reliable when the system is low on memory, but in fact, it consumes two times more memory as at the moment of running this function, there are two vports allocated with their queues and vectors. Moreover, it claims to prevent the driver from running into "bad state", but in fact, any error during the rebuild leaves the old vport in the partially allocated state. Finally, if the interface is down when the function is called, it always allocates a new queue set, but when the user decides to enable the interface later on, vport_open() allocates them once again, IOW there's a clear memory leak here. Just don't allocate a new queue set when performing a reset, that solves crashes and memory leaks. Readd the old queue number and reopen the interface on rollback - that solves limbo states when the device is left disabled and/or without HW queues enabled.	2024-09-04	7.8	High
CVE-2024-44974	Linux	In the Linux kernel, the following vulnerability has been resolved: mptcp: pm: avoid possible UaF when selecting endp select_local_address() and select_signal_address() both select an endpoint entry from the list inside an RCU protected section, but return a reference to it, to be read later on. If the entry is dereferenced after the RCU unlock, reading info could cause a Use-after-Free. A simple solution is to copy the required info while inside the RCU protected section to avoid any risk of UaF later. The address ID might need to be modified later to handle the ID0 case later, so a copy seems OK to deal with.	2024-09-04	7.8	High
CVE-2024-44978	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe: Free job before xe_exec_queue_put Free job depends on job->vm being valid, the last xe_exec_queue_put can destroy the VM. Prevent UAF by freeing job before xe_exec_queue_put. (cherry picked from commit 32a42c93b74c8ca6d0915ea3eba21bceff53042f)	2024-09-04	7.8	High
CVE-2024-44985	Linux	In the Linux kernel, the following vulnerability has been resolved:	2024-09-04	7.8	High

		ipv6: prevent possible UAF in ip6_xmit() If skb_expand_head() returns NULL, skb has been freed and the associated dst/idev could also have been freed. We must use rcu_read_lock() to prevent a possible UAF.			
CVE-2024-44986	Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: fix possible UAF in ip6_finish_output2() If skb_expand_head() returns NULL, skb has been freed and associated dst/idev could also have been freed. We need to hold rcu_read_lock() to make sure the dst and associated idev are alive.	2024-09-04	7.8	High
CVE-2024-44987	Linux	In the Linux kernel, the following vulnerability has been resolved: ipv6: prevent UAF in ip6_send_skb() syzbot reported an UAF in ip6_send_skb() [1] After ip6_local_out() has returned, we no longer can safely dereference rt, unless we hold rcu_read_lock(). A similar issue has been fixed in commit a688caa34beb ("ipv6: take rcu lock in rawv6_send_hdrinc()") Another potential issue in ip6_finish_output2() is handled in a separate patch. [1] BUG: KASAN: slab-use-after-free in ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 Read of size 8 at addr ffff88806dde4858 by task syz.1.380/6530 CPU: 1 UID: 0 PID: 6530 Comm: syz.1.380 Not tainted 6.11.0-rc3- syzkaller-00306-gdf6cbc62cc9b #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 08/06/2024 Call Trace: <TASK> __dump_stack lib/dump_stack.c:93 [inline] dump_stack_lvl+0x241/0x360 lib/dump_stack.c:119 print_address_description mm/kasan/report.c:377 [inline] print_report+0x169/0x550 mm/kasan/report.c:488 kasan_report+0x143/0x180 mm/kasan/report.c:601 ip6_send_skb+0x18d/0x230 net/ipv6/ip6_output.c:1964 rawv6_push_pending_frames+0x75c/0x9e0 net/ipv6/raw.c:588 rawv6_sendmsg+0x19c7/0x23c0 net/ipv6/raw.c:926 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 sock_write_iter+0x2dd/0x400 net/socket.c:1160 do_iter_readv_writev+0x60a/0x890 vfs_writev+0x37c/0xbb0 fs/read_write.c:971 do_writev+0x1b1/0x350 fs/read_write.c:1018 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f936bf79e79 Code: ff ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 40 00 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 a8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007f936cd7f038 EFLAGS: 00000246 ORIG_RAX: 0000000000000014 RAX: ffffffffffffffda RBX: 00007f936c115f80 RCX: 00007f936bf79e79 RDX: 0000000000000001 RSI: 0000000020000040 RDI: 0000000000000004 RBP: 00007f936bfe7916 R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 0000000000000000 R14: 00007f936c115f80 R15: 00007fff2860a7a8 </TASK> Allocated by task 6530: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 unpoison_slab_object mm/kasan/common.c:312 [inline]	2024-09-04	7.8	High

		__kasan_slab_alloc+0x66/0x80 mm/kasan/common.c:338 kasan_slab_alloc include/linux/kasan.h:201 [inline] slab_post_alloc_hook mm/slub.c:3988 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_noprof+0x135/0x2a0 mm/slub.c:4044 dst_alloc+0x12b/0x190 net/core/dst.c:89 ip6_blackhole_route+0x59/0x340 net/ipv6/route.c:2670 make_blackhole net/xfrm/xfrm_policy.c:3120 [inline] xfrm_lookup_route+0xd1/0x1c0 net/xfrm/xfrm_policy.c:3313 ip6_dst_lookup_flow+0x13e/0x180 net/ipv6/ip6_output.c:1257 rawv6_sendmsg+0x1283/0x23c0 net/ipv6/raw.c:898 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x1a6/0x270 net/socket.c:745 ____sys_sendmsg+0x525/0x7d0 net/socket.c:2597 ___sys_sendmsg net/socket.c:2651 [inline] __sys_sendmsg+0x2b0/0x3a0 net/socket.c:2680 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xf3/0x230 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Freed by task 45: kasan_save_stack mm/kasan/common.c:47 [inline] kasan_save_track+0x3f/0x80 mm/kasan/common.c:68 kasan_save_free_info+0x40/0x50 mm/kasan/generic.c:579 poison_slab_object+0xe0/0x150 mm/kasan/common.c:240 __kasan_slab_free+0x37/0x60 mm/kasan/common.c:256 kasan_slab_free include/linux/kasan.h:184 [inline] slab_free_hook mm/slub.c:2252 [inline] slab_free mm/slub.c:4473 [inline] kmem_cache_free+0x145/0x350 mm/slub.c:4548 dst_destroy+0x2ac/0x460 net/core/dst.c:124 rcu_do_batch kernel/rcu/tree.c:2569 [inline] rcu_core+0xafd/0x1830 kernel/rcu/tree. ---truncated---			
CVE-2024-44997	Linux	In the Linux kernel, the following vulnerability has been resolved: net: ethernet: mtk_wed: fix use-after-free panic in mtk_wed_setup_tc_block_cb() When there are multiple ap interfaces on one band and with WED on, turning the interface down will cause a kernel panic on MT798X. Previously, cb_priv was freed in mtk_wed_setup_tc_block() without marking NULL,and mtk_wed_setup_tc_block_cb() didn't check the value, too. Assign NULL after free cb_priv in mtk_wed_setup_tc_block() and check NULL in mtk_wed_setup_tc_block_cb(). ---------- Unable to handle kernel paging request at virtual address 0072460bca32b4f5 Call trace: mtk_wed_setup_tc_block_cb+0x4/0x38 0xffffffc0794084bc tcf_block_playback_offloads+0x70/0x1e8 tcf_block_unbind+0x6c/0xc8 ... ---------	2024-09-04	7.8	High
CVE-2024-44998	Linux	In the Linux kernel, the following vulnerability has been resolved: atm: idt77252: prevent use after free in dequeue_rx() We can't dereference "skb" after calling vcc->push() because the skb is released.	2024-09-04	7.8	High
CVE-2024-40709	Veeam	A missing authorization vulnerability allows a local low-privileged user on the machine to escalate their privileges to root level.	2024-09-07	7.8	High
CVE-2024-40712	Veeam	A path traversal vulnerability allows an attacker with a low-privileged account and local access to the system to perform local privilege escalation (LPE).	2024-09-07	7.8	High
CVE-2024-40713	Veeam	A vulnerability that allows a user who has been assigned a low-privileged role within Veeam Backup & Replication to alter Multi-Factor Authentication (MFA) settings and bypass MFA.	2024-09-07	7.8	High
CVE-2024-42023	Veeam	An improper access control vulnerability allows low-privileged users to execute code with Administrator privileges remotely.	2024-09-07	7.8	High

CVE-2024-42058	Zyxel	A null pointer dereference vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V5.20 through V5.38, and USG20(W)-VPN series firmware versions from V5.20 through V5.38 could allow an unauthenticated attacker to cause DoS conditions by sending crafted packets to a vulnerable device.	2024-09-03	7.5	High
CVE-2024-5412	Zyxel	A buffer overflow vulnerability in the library "libclinkc" of the Zyxel VMG8825-T50K firmware version 5.50(ABOM.8)C0 could allow an unauthenticated attacker to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device.	2024-09-03	7.5	High
CVE-2024-8383	Mozilla	Firefox normally asks for confirmation before asking the operating system to find an application to handle a scheme that the browser does not support. It did not ask before doing so for the Usenet-related schemes news: and snews:. Since most operating systems don't have a trusted newsreader installed by default, an unscrupulous program that the user downloaded could register itself as a handler. The website that served the application download could then launch that application at will. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Firefox ESR < 115.15.	2024-09-03	7.5	High
CVE-2024-6119	OpenSSL	Issue summary: Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address resulting in abnormal termination of the application process. Impact summary: Abnormal termination of an application can a cause a denial of service. Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address when comparing the expected name with an `otherName` subject alternative name of an X.509 certificate. This may result in an exception that terminates the application program. Note that basic certificate chain validation (signatures, dates, ...) is not affected, the denial of service can occur only when the application also specifies an expected DNS name, Email address or IP address. TLS servers rarely solicit client certificates, and even when they do, they generally don't perform a name check against a reference identifier (expected identity), but rather extract the presented identity after checking the certificate chain. So TLS servers are generally not affected and the severity of the issue is Moderate. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.	2024-09-03	7.5	High
CVE-2024-42039	Huawei	Access control vulnerability in the SystemUI module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-09-04	7.5	High
CVE-2024-45441	huawei	Input verification vulnerability in the system service module Impact: Successful exploitation of this vulnerability will affect availability.	2024-09-04	7.5	High
CVE-2024-45442	Huawei	Vulnerability of permission verification for APIs in the DownloadProviderMain module Impact: Successful exploitation of this vulnerability will affect availability.	2024-09-04	7.5	High
CVE-2024-45450	Huawei	Permission control vulnerability in the software update module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-09-04	7.5	High
CVE-2024-20440	Cisco	A vulnerability in Cisco Smart Licensing Utility could allow an unauthenticated, remote attacker to access sensitive information. This vulnerability is due to excessive verbosity in a debug log file.	2024-09-04	7.5	High

		An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain log files that contain sensitive data, including credentials that can be used to access the API.			
CVE-2024-20505	Cisco	A vulnerability in the PDF parsing module of Clam AntiVirus (ClamAV) versions 1.4.0, 1.3.2 and prior versions, all 1.2.x versions, 1.0.6 and prior versions, all 0.105.x versions, all 0.104.x versions, and 0.103.11 and all prior versions could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to an out of bounds read. An attacker could exploit this vulnerability by submitting a crafted PDF file to be scanned by ClamAV on an affected device. An exploit could allow the attacker to terminate the scanning process.	2024-09-04	7.5	High
CVE-2024-5957	Trellix	This vulnerability allows unauthenticated remote attackers to bypass authentication and gain APIs access of the Manager.	2024-09-05	7.5	High
CVE-2024-7652	Mozilla	An error in the ECMA-262 specification relating to Async Generators could have resulted in a type confusion, potentially leading to memory corruption and an exploitable crash. This vulnerability affects Firefox < 128, Firefox ESR < 115.13, Thunderbird < 115.13, and Thunderbird < 128.	2024-09-06	7.5	High
CVE-2024-37068	IBM	IBM Maximo Application Suite - Manage Component 8.10, 8.11, and 9.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	2024-09-07	7.5	High
CVE-2024-40681	IBM	IBM MQ Operator 2.0.26 and 3.2.4 could allow an authenticated user in a specifically defined role, to bypass security restrictions and execute actions against the queue manager.	2024-09-07	7.5	High
CVE-2024-42021	Veeam	An improper access control vulnerability allows an attacker with valid access tokens to access saved credentials.	2024-09-07	7.5	High
CVE-2024-42022	Veeam	An incorrect permission assignment vulnerability allows an attacker to modify product configuration files.	2024-09-07	7.5	High
CVE-2024-42020	Veeam	A Cross-site-scripting (XSS) vulnerability exists in the Reporter Widgets that allows HTML injection.	2024-09-07	7.3	High
CVE-2024-42059	Zyxel	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V5.00 through V5.38, USG FLEX series firmware versions from V5.00 through V5.38, USG FLEX 50(W) series firmware versions from V5.00 through V5.38, and USG20(W)-VPN series firmware versions from V5.00 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted compressed language file via FTP.	2024-09-03	7.2	High
CVE-2024-42060	Zyxel	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to execute some OS commands on an affected device by uploading a crafted internal user agreement file to the vulnerable device.	2024-09-03	7.2	High
CVE-2024-7203	Zyxel	A post-authentication command injection vulnerability in Zyxel ATP series firmware versions from V4.60 through V5.38 and USG FLEX series firmware versions from V4.60 through V5.38 could allow an authenticated attacker with administrator privileges to execute some operating system (OS) commands on an affected device by executing a crafted CLI command.	2024-09-03	7.2	High
CVE-2024-44983	Linux	In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: validate vlan header Ensure there is sufficient room to access the protocol field of the VLAN header, validate it once before the flowtable lookup. === BUG: KMSAN: uninit-value in nf_flow_offload_inet_hook+0x45a/0x5f0 net/netfilter/nf_flow_table_inet.c:32 nf_flow_offload_inet_hook+0x45a/0x5f0 net/netfilter/nf_flow_table_inet.c:32 nf_hook_entry_hookfn include/linux/netfilter.h:154 [inline] nf_hook_slow+0xf4/0x400 net/netfilter/core.c:626 nf_hook_ingress include/linux/netfilter_netdev.h:34 [inline] nf_ingress net/core/dev.c:5440 [inline]	2024-09-04	7.1	High
CVE-2024-44993	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/v3d: Fix out-of-bounds read in `v3d_csd_job_run()`	2024-09-04	7.1	High

		When enabling UBSAN on Raspberry Pi 5, we get the following warning: [387.894977] UBSAN: array-index-out-of-bounds in drivers/gpu/drm/v3d/v3d_sched.c:320:3 [387.903868] index 7 is out of range for type '__u32 [7]' [387.909692] CPU: 0 PID: 1207 Comm: kworker/u16:2 Tainted: G WC 6.10.3-v8-16k-numa #151 [387.919166] Hardware name: Raspberry Pi 5 Model B Rev 1.0 (DT) [387.925961] Workqueue: v3d_csd drm_sched_run_job_work [gpu_sched] [387.932525] Call trace: [387.935296] dump_backtrace+0x170/0x1b8 [387.939403] show_stack+0x20/0x38 [387.942907] dump_stack_lvl+0x90/0xd0 [387.946785] dump_stack+0x18/0x28 [387.950301] __ubsan_handle_out_of_bounds+0x98/0xd0 [387.955383] v3d_csd_job_run+0x3a8/0x438 [v3d] [387.960707] drm_sched_run_job_work+0x520/0x6d0 [gpu_sched] [387.966862] process_one_work+0x62c/0xb48 [387.971296] worker_thread+0x468/0x5b0 [387.975317] kthread+0x1c4/0x1e0 [387.978818] ret_from_fork+0x10/0x20 [387.983014] ---[end trace]--- This happens because the UAPI provides only seven configuration registers and we are reading the eighth position of this u32 array. Therefore, fix the out-of-bounds read in `v3d_csd_job_run()` by accessing only seven positions on the '__u32 [7]' array. The eighth register exists indeed on V3D 7.1, but it isn't currently used. That being so, let's guarantee that it remains unused and add a note that it could be set in a future patch.			
CVE-2024-44999	Linux	In the Linux kernel, the following vulnerability has been resolved: gtp: pull network headers in gtp_dev_xmit() syzbot/KMSAN reported use of uninit-value in get_dev_xmit() [1] We must make sure the IPv4 or Ipv6 header is pulled in skb->head before accessing fields in them. Use pskb_inet_may_pull() to fix this issue. [1] BUG: KMSAN: uninit-value in ipv6_pdp_find drivers/net/gtp.c:220 [inline] BUG: KMSAN: uninit-value in gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] BUG: KMSAN: uninit-value in gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 ipv6_pdp_find drivers/net/gtp.c:220 [inline] gtp_build_skb_ip6 drivers/net/gtp.c:1229 [inline] gtp_dev_xmit+0x1424/0x2540 drivers/net/gtp.c:1281 __netdev_start_xmit include/linux/netdevice.h:4913 [inline] netdev_start_xmit include/linux/netdevice.h:4922 [inline] xmit_one net/core/dev.c:3580 [inline] dev_hard_start_xmit+0x247/0xa20 net/core/dev.c:3596 __dev_queue_xmit+0x358c/0x5610 net/core/dev.c:4423 dev_queue_xmit include/linux/netdevice.h:3105 [inline] packet_xmit+0x9c/0x6c0 net/packet/af_packet.c:276 packet_snd net/packet/af_packet.c:3145 [inline] packet_sendmsg+0x90e3/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f Uninit was created at:	2024-09-04	7.1	High

		slab_post_alloc_hook mm/slub.c:3994 [inline] slab_alloc_node mm/slub.c:4037 [inline] kmem_cache_alloc_node_noprof+0x6bf/0xb80 mm/slub.c:4080 kmalloc_reserve+0x13d/0x4a0 net/core/skbuff.c:583 __alloc_skb+0x363/0x7b0 net/core/skbuff.c:674 alloc_skb include/linux/skbuff.h:1320 [inline] alloc_skb_with_frags+0xc8/0xbf0 net/core/skbuff.c:6526 sock_alloc_send_pskb+0xa81/0xbf0 net/core/sock.c:2815 packet_alloc_skb net/packet/af_packet.c:2994 [inline] packet_snd net/packet/af_packet.c:3088 [inline] packet_sendmsg+0x749c/0xa3a0 net/packet/af_packet.c:3177 sock_sendmsg_nosec net/socket.c:730 [inline] __sock_sendmsg+0x30f/0x380 net/socket.c:745 __sys_sendto+0x685/0x830 net/socket.c:2204 __do_sys_sendto net/socket.c:2216 [inline] __se_sys_sendto net/socket.c:2212 [inline] __x64_sys_sendto+0x125/0x1d0 net/socket.c:2212 x64_sys_call+0x3799/0x3c10 arch/x86/include/generated/asm/syscalls_64.h:45 do_syscall_x64 arch/x86/entry/common.c:52 [inline] do_syscall_64+0xcd/0x1e0 arch/x86/entry/common.c:83 entry_SYSCALL_64_after_hwframe+0x77/0x7f CPU: 0 UID: 0 PID: 7115 Comm: syz.1.515 Not tainted 6.11.0-rc1-syzkaller-00043-g94ede2a3e913 #0 Hardware name: Google Google Compute Engine/Google Compute Engine, BIOS Google 06/27/2024			
CVE-2024-45097	IBM	IBM Aspera Faspex 5.0.0 through 5.0.9 could allow a user to bypass intended access restrictions and conduct resource modification.	2024-09-05	7.1	High
CVE-2024-8461	D-Link	A vulnerability, which was classified as problematic, was found in D-Link DNS-320 2.02b01. This affects an unknown part of the file /cgi-bin/discovery.cgi of the component Web Management Interface. The manipulation leads to information disclosure. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-09-05	6.9	Medium
CVE-2024-45074	IBM	IBM webMethods Integration 10.15 could allow an authenticated user to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system.	2024-09-04	6.5	Medium
CVE-2024-45096	IBM	IBM Aspera Faspex 5.0.0 through 5.0.9 could allow a user with access to the package to obtain sensitive information through a directory listing.	2024-09-05	6.5	Medium
CVE-2024-8394	Mozilla	When aborting the verification of an OTR chat session, an attacker could have caused a use-after-free bug leading to a potentially exploitable crash. This vulnerability affects Thunderbird < 128.2.	2024-09-06	6.5	Medium
CVE-2024-8460	D-Link	A vulnerability, which was classified as problematic, has been found in D-Link DNS-320 2.02b01. Affected by this issue is some unknown functionality of the file /cgi-bin/widget_api.cgi of the component Web Management Interface. The manipulation of the argument getHD/getSer/getSys leads to information disclosure. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	2024-09-05	6.3	Medium
CVE-2024-42061	Zyxel	A reflected cross-site scripting (XSS) vulnerability in the CGI program "dynamic_script.cgi" of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an attacker to trick a user into visiting a crafted URL with the XSS payload. The attacker could obtain browser-based information if the malicious script is executed on the victim’s browser.	2024-09-03	6.1	Medium
CVE-2024-8386	Mozilla	If a site had been granted the permission to open popup windows, it could cause Select elements to appear on top of another site to perform a spoofing attack. This vulnerability affects Firefox < 130, Firefox ESR < 128.2, and Thunderbird < 128.2.	2024-09-03	6.1	Medium
CVE-2024-20506	Cisco	A vulnerability in the ClamD service module of Clam AntiVirus (ClamAV) versions 1.4.0, 1.3.2 and prior versions, all 1.2.x versions, 1.0.6 and prior versions, all 0.105.x versions, all 0.104.x versions, and 0.103.11 and all prior versions could allow an authenticated, local attacker to corrupt critical system files.	2024-09-04	6.1	Medium

		The vulnerability is due to allowing the ClamD process to write to its log file while privileged without checking if the logfile has been replaced with a symbolic link. An attacker could exploit this vulnerability if they replace the ClamD log file with a symlink to a critical system file and then find a way to restart the ClamD process. An exploit could allow the attacker to corrupt a critical system file by appending ClamD log messages after restart.			
CVE-2024-20469	Cisco	A vulnerability in specific CLI commands in Cisco Identity Services Engine (ISE) could allow an authenticated, local attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit this vulnerability, the attacker must have valid Administrator privileges on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	2024-09-04	6	Medium
CVE-2024-45444	Huawei	Access permission verification vulnerability in the WMS module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-09-04	5.5	Medium
CVE-2024-45445	Huawei	Vulnerability of resources not being closed or released in the keystore module Impact: Successful exploitation of this vulnerability will affect availability.	2024-09-04	5.5	Medium
CVE-2024-45446	Huawei	Access permission verification vulnerability in the camera driver module Impact: Successful exploitation of this vulnerability will affect availability.	2024-09-04	5.5	Medium
CVE-2024-45447	Huawei	Access control vulnerability in the camera framework module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-09-04	5.5	Medium
CVE-2024-45448	Huawei	Page table protection configuration vulnerability in the trusted firmware module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-09-04	5.5	Medium
CVE-2024-45449	Huawei	Access permission verification vulnerability in the ringtone setting module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-09-04	5.5	Medium
CVE-2024-8298	Huawei	Memory request vulnerability in the memory management module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2024-09-04	5.5	Medium
CVE-2024-20503	Cisco	A vulnerability in Cisco Duo Epic for Hyperdrive could allow an authenticated, local attacker to view sensitive information in cleartext on an affected system. This vulnerability is due to improper storage of an unencrypted registry key. A low-privileged attacker could exploit this vulnerability by viewing or querying the registry key on the affected system. A successful exploit could allow the attacker to view sensitive information in cleartext.	2024-09-04	5.5	Medium
CVE-2024-44952	Linux	In the Linux kernel, the following vulnerability has been resolved: driver core: Fix uevent_show() vs driver detach race uevent_show() wants to de-reference dev->driver->name. There is no clean way for a device attribute to de-reference dev->driver unless that attribute is defined via (struct device_driver).dev_groups. Instead, the anti-pattern of taking the device_lock() in the attribute handler risks deadlocks with code paths that remove device attributes while holding the lock. This deadlock is typically invisible to lockdep given the device_lock() is marked lockdep_set_novalidate_class(), but some subsystems allocate a local lockdep key for @dev->mutex to reveal reports of the form:	2024-09-04	5.5	Medium

		== WARNING: possible circular locking dependency detected 6.10.0-rc7+ #275 Tainted: G OE N -- modprobe/2374 is trying to acquire lock: ffff8c2270070de0 (kn->active#6){++++}-{0:0}, at: __kernfs_remove+0xde/0x220 but task is already holding lock: ffff8c22016e88f8 (&cxl_root_key){+.+.}-{3:3}, at: device_release_driver_internal+0x39/0x210 which lock already depends on the new lock. the existing dependency chain (in reverse order) is: -> #1 (&cxl_root_key){+.+.}-{3:3}: __mutex_lock+0x99/0xc30 uevent_show+0xac/0x130 dev_attr_show+0x18/0x40 sysfs_kf_seq_show+0xac/0xf0 seq_read_iter+0x110/0x450 vfs_read+0x25b/0x340 ksys_read+0x67/0xf0 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e -> #0 (kn->active#6){++++}-{0:0}: __lock_acquire+0x121a/0x1fa0 lock_acquire+0xd6/0x2e0 kernfs_drain+0x1e9/0x200 __kernfs_remove+0xde/0x220 kernfs_remove_by_name_ns+0x5e/0xa0 device_del+0x168/0x410 device_unregister+0x13/0x60 devres_release_all+0xb8/0x110 device_unbind_cleanup+0xe/0x70 device_release_driver_internal+0x1c7/0x210 driver_detach+0x47/0x90 bus_remove_driver+0x6c/0xf0 cxl_acpi_exit+0xc/0x11 [cxl_acpi] __do_sys_delete_module.isra.0+0x181/0x260 do_syscall_64+0x75/0x190 entry_SYSCALL_64_after_hwframe+0x76/0x7e The observation though is that driver objects are typically much longer lived than device objects. It is reasonable to perform lockless de-reference of a @driver pointer even if it is racing detach from a device. Given the infrequency of driver unregistration, use synchronize_rcu() in module_remove_driver() to close any potential races. It is potentially overkill to suffer synchronize_rcu() just to handle the rare module removal racing uevent_show() event. Thanks to Tetsuo Handa for the debug analysis of the syzbot report [1].			
CVE-2024-44953	Linux	In the Linux kernel, the following vulnerability has been resolved: scsi: ufs: core: Fix deadlock during RTC update There is a deadlock when runtime suspend waits for the flush of RTC work, and the RTC work calls ufshcd_rpm_get_sync() to wait for runtime resume. Here is deadlock backtrace: kworker/0:1 D 4892.876354 10 10971 4859 0x4208060 0x8 10 0 120 670730152367 ptr f0ffff80c2e40000 0 1 0x00000001 0x000000ff 0x000000ff 0x000000ff <ffffffee5e71ddb0> __switch_to+0x1a8/0x2d4 <ffffffee5e71e604> __schedule+0x684/0xa98 <ffffffee5e71ea60> schedule+0x48/0xc8 <ffffffee5e725f78> schedule_timeout+0x48/0x170 <ffffffee5e71fb74> do_wait_for_common+0x108/0x1b0 <ffffffee5e71efe0> wait_for_completion+0x44/0x60 <ffffffee5d6de968> __flush_work+0x39c/0x424 <ffffffee5d6decc0> __cancel_work_sync+0xd8/0x208	2024-09-04	5.5	Medium

		<ffffffee5d6dee2c> cancel_delayed_work_sync+0x14/0x28 <ffffffee5e2551b8> __ufshcd_wl_suspend+0x19c/0x480 <ffffffee5e255fb8> ufshcd_wl_runtime_suspend+0x3c/0x1d4 <ffffffee5dffd80c> scsi_runtime_suspend+0x78/0xc8 <ffffffee5df93580> __rpm_callback+0x94/0x3e0 <ffffffee5df90b0c> rpm_suspend+0x2d4/0x65c <ffffffee5df91448> __pm_runtime_suspend+0x80/0x114 <ffffffee5dffd95c> scsi_runtime_idle+0x38/0x6c <ffffffee5df912f4> rpm_idle+0x264/0x338 <ffffffee5df90f14> __pm_runtime_idle+0x80/0x110 <ffffffee5e24ce44> ufshcd_rtc_work+0x128/0x1e4 <ffffffee5d6e3a40> process_one_work+0x26c/0x650 <ffffffee5d6e65c8> worker_thread+0x260/0x3d8 <ffffffee5d6edec8> kthread+0x110/0x134 <ffffffee5d616b18> ret_from_fork+0x10/0x20 Skip updating RTC if RPM state is not RPM_ACTIVE.			
[CVE-2024-44956]()	Linux	In the Linux kernel, the following vulnerability has been resolved: drm/xe/preempt_fence: enlarge the fence critical section It is really easy to introduce subtle deadlocks in preempt_fence_work_func() since we operate on single global ordered-wq for signalling our preempt fences behind the scenes, so even though we signal a particular fence, everything in the callback should be in the fence critical section, since blocking in the callback will prevent other published fences from signalling. If we enlarge the fence critical section to cover the entire callback, then lockdep should be able to understand this better, and complain if we grab a sensitive lock like vm->lock, which is also held when waiting on preempt fences.	2024-09-04	5.5	Medium
[CVE-2024-44957]()	Linux	In the Linux kernel, the following vulnerability has been resolved: xen: privcmd: Switch from mutex to spinlock for irqfds irqfd_wakeup() gets EPOLLHUP, when it is called by eventfd_release() by way of wake_up_poll(&ctx->wqh, EPOLLHUP), which gets called under spin_lock_irqsave(). We can't use a mutex here as it will lead to a deadlock. Fix it by switching over to a spin lock.	2024-09-04	5.5	Medium
[CVE-2024-44971]()	Linux	In the Linux kernel, the following vulnerability has been resolved: net: dsa: bcm_sf2: Fix a possible memory leak in bcm_sf2_mdio_register() bcm_sf2_mdio_register() calls of_phy_find_device() and then phy_device_remove() in a loop to remove existing PHY devices. of_phy_find_device() eventually calls bus_find_device(), which calls get_device() on the returned struct device * to increment the refcount. The current implementation does not decrement the refcount, which causes memory leak. This commit adds the missing phy_device_free() call to decrement the refcount via put_device() to balance the refcount.	2024-09-04	5.5	Medium
[CVE-2024-44981]()	Linux	In the Linux kernel, the following vulnerability has been resolved: workqueue: Fix UBSAN 'subtraction overflow' error in shift_and_mask() UBSAN reports the following 'subtraction overflow' error when booting in a virtual machine on Android: | Internal error: UBSAN: integer subtraction overflow: 00000000f2005515 [#1] PREEMPT SMP | Modules linked in: | CPU: 0 PID: 1 Comm: swapper/0 Not tainted 6.10.0-00006-g3cbe9e5abd46-dirty #4 | Hardware name: linux,dummy-virt (DT)	2024-09-04	5.5	Medium

		| pstate: 600000c5 (nZCv daIF -PAN -UAO -TCO -DIT -SSBS BTYPE=--) | pc : cancel_delayed_work+0x34/0x44 | lr : cancel_delayed_work+0x2c/0x44 | sp : ffff80008002ba60 | x29: ffff80008002ba60 x28: 0000000000000000 x27: 0000000000000000 | x26: 0000000000000000 x25: 0000000000000000 x24: 0000000000000000 | x23: 0000000000000000 x22: 0000000000000000 x21: ffff1f65014cd3c0 | x20: ffffc0e84c9d0da0 x19: ffffc0e84cab3558 x18: ffff800080009058 | x17: 00000000247ee1f8 x16: 00000000247ee1f8 x15: 00000000bdcb279d | x14: 0000000000000001 x13: 0000000000000075 x12: 00000a0000000000 | x11: ffff1f6501499018 x10: 00984901651fffff x9 : ffff5e7cc35af000 | x8 : 0000000000000001 x7 : 3d4d455453595342 x6 : 000000004e514553 | x5 : ffff1f6501499265 x4 : ffff1f650ff60b10 x3 : 0000000000000620 | x2 : ffff80008002ba78 x1 : 0000000000000000 x0 : 0000000000000000 | Call trace: | cancel_delayed_work+0x34/0x44 | deferred_probe_extend_timeout+0x20/0x70 | driver_register+0xa8/0x110 | __platform_driver_register+0x28/0x3c | syscon_init+0x24/0x38 | do_one_initcall+0xe4/0x338 | do_initcall_level+0xac/0x178 | do_initcalls+0x5c/0xa0 | do_basic_setup+0x20/0x30 | kernel_init_freeable+0x8c/0xf8 | kernel_init+0x28/0x1b4 | ret_from_fork+0x10/0x20 | Code: f9000fbf 97fffa2f 39400268 37100048 (d42aa2a0) | ---[end trace 0000000000000000]--- | Kernel panic - not syncing: UBSAN: integer subtraction overflow: Fatal exception This is due to shift_and_mask() using a signed immediate to construct the mask and being called with a shift of 31 (WORK_OFFQ_POOL_SHIFT) so that it ends up decrementing from INT_MIN. Use an unsigned constant '1U' to generate the mask in shift_and_mask().			
CVE-2024-44989	Linux	In the Linux kernel, the following vulnerability has been resolved: bonding: fix xfrm real_dev null pointer dereference We shouldn't set real_dev to NULL because packets can be in transit and xfrm might call xdo_dev_offload_ok() in parallel. All callbacks assume real_dev is set. Example trace: kernel: BUG: unable to handle page fault for address: 0000000000001030 kernel: bond0: (slave eni0np1): making interface the new active one kernel: #PF: supervisor write access in kernel mode kernel: #PF: error_code(0x0002) - not-present page kernel: PGD 0 P4D 0 kernel: Oops: 0002 [#1] PREEMPT SMP kernel: CPU: 4 PID: 2237 Comm: ping Not tainted 6.7.7+ #12 kernel: Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-2.fc40 04/01/2014 kernel: RIP: 0010:nsim_ipsec_offload_ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: Code: e0 0f 0b 48 83 7f 38 00 74 de 0f 0b 48 8b 47 08 48 8b 37 48 8b 78 40 e9 b2 e5 9a d7 66 90 0f 1f 44 00 00 48 8b 86 80 02 00 00 <83> 80 30 10 00 00 01 b8 01 00 00 00 c3 0f 1f 80 00 00 00 00 0f 1f	2024-09-04	5.5	Medium

		kernel: bond0: (slave eni0np1): making interface the new active one kernel: RSP: 0018:ffffabde81553b98 EFLAGS: 00010246 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: kernel: RAX: 0000000000000000 RBX: ffff9eb404e74900 RCX: ffff9eb403d97c60 kernel: RDX: ffffffffc090de10 RSI: ffff9eb404e74900 RDI: ffff9eb3c5de9e00 kernel: RBP: ffff9eb3c0a42000 R08: 0000000000000010 R09: 0000000000000014 kernel: R10: 7974203030303030 R11: 3030303030303030 R12: 0000000000000000 kernel: R13: ffff9eb3c5de9e00 R14: ffffabde81553cc8 R15: ffff9eb404c53000 kernel: FS: 00007f2a77a3ad00(0000) GS:ffff9eb43bd00000(0000) knlGS:0000000000000000 kernel: CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 kernel: CR2: 0000000000001030 CR3: 00000001122ab000 CR4: 0000000000350ef0 kernel: bond0: (slave eni0np1): making interface the new active one kernel: Call Trace: kernel: <TASK> kernel: ? __die+0x1f/0x60 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ? page_fault_oops+0x142/0x4c0 kernel: ? do_user_addr_fault+0x65/0x670 kernel: ? kvm_read_and_reset_apf_flags+0x3b/0x50 kernel: bond0: (slave eni0np1): making interface the new active one kernel: ? exc_page_fault+0x7b/0x180 kernel: ? asm_exc_page_fault+0x22/0x30 kernel: ? nsim_bpf_uninit+0x50/0x50 [netdevsim] kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ? nsim_ipsec_offload_ok+0xc/0x20 [netdevsim] kernel: bond0: (slave eni0np1): making interface the new active one kernel: bond_ipsec_offload_ok+0x7b/0x90 [bonding] kernel: xfrm_output+0x61/0x3b0 kernel: bond0: (slave eni0np1): bond_ipsec_add_sa_all: failed to add SA kernel: ip_push_pending_frames+0x56/0x80			
CVE-2024-44990	Linux	In the Linux kernel, the following vulnerability has been resolved: bonding: fix null pointer deref in bond_ipsec_offload_ok We must check if there is an active slave before dereferencing the pointer.	2024-09-04	5.5	Medium
CVE-2024-44992	Linux	In the Linux kernel, the following vulnerability has been resolved: smb/client: avoid possible NULL dereference in cifs_free_subrequest() Clang static checker (scan-build) warning: cifsglob.h:line 890, column 3 Access to field 'ops' results in a dereference of a null pointer. Commit 519be989717c ("cifs: Add a tracepoint to track credits involved in R/W requests") adds a check for 'rdata->server', and let clang throw this warning about NULL dereference. When 'rdata->credits.value != 0 && rdata->server == NULL' happens, add_credits_and_wake_if() will call rdata->server->ops->add_credits(). This will cause NULL dereference problem. Add a check for 'rdata->server' to avoid NULL dereference.	2024-09-04	5.5	Medium
CVE-2024-44995	Linux	In the Linux kernel, the following vulnerability has been resolved: net: hns3: fix a deadlock problem when config TC during resetting When config TC during the reset process, may cause a deadlock, the flow is	2024-09-04	5.5	Medium

		as below: pf reset start ? ? ...... setup tc ? ? ? ? DOWN: napi_disable() napi_disable()(skip) ? ? ? ? ? .... ? ? ? ? napi_enable() ? ? UINIT: netif_napi_del() ? ? ...... ? ? INIT: netif_napi_add() ? ? ...... global reset start ? ? ? ? UP: napi_enable()(skip) ...... ? ? ? ? ...... napi_disable() In reset process, the driver will DOWN the port and then UINIT, in this case, the setup tc process will UP the port before UINIT, so cause the problem. Adds a DOWN process in UINIT to fix it.			
CVE-2024-45000	Linux	In the Linux kernel, the following vulnerability has been resolved: fs/netfs/fscache_cookie: add missing "n_accesses" check This fixes a NULL pointer dereference bug due to a data race which looks like this: BUG: kernel NULL pointer dereference, address: 0000000000000008 #PF: supervisor read access in kernel mode #PF: error_code(0x0000) - not-present page PGD 0 P4D 0 Oops: 0000 [#1] SMP PTI CPU: 33 PID: 16573 Comm: kworker/u97:799 Not tainted 6.8.7-cm4all1-hp+ #43 Hardware name: HP ProLiant DL380 Gen9/ProLiant DL380 Gen9, BIOS P89 10/17/2018 Workqueue: events_unbound netfs_rreq_write_to_cache_work RIP: 0010:cachefiles_prepare_write+0x30/0xa0 Code: 57 41 56 45 89 ce 41 55 49 89 cd 41 54 49 89 d4 55 53 48 89 fb 48 83 ec 08 48 8b 47 08 48 83 7f 10 00 48 89 34 24 48 8b 68 20 <48> 8b 45 08 4c 8b 38 74 45 49 8b 7f 50 e8 4e a9 b0 ff 48 8b 73 10 RSP: 0018:ffffb4e78113bde0 EFLAGS: 00010286 RAX: ffff976126be6d10 RBX: ffff97615cdb8438 RCX: 0000000000020000 RDX: ffff97605e6c4c68 RSI: ffff97605e6c4c60 RDI: ffff97615cdb8438 RBP: 0000000000000000 R08: 0000000000278333 R09: 0000000000000001 R10: ffff97605e6c4600 R11: 0000000000000001 R12: ffff97605e6c4c68 R13: 0000000000020000 R14: 0000000000000001 R15: ffff976064fe2c00 FS: 0000000000000000(0000) GS:ffff9776dfd40000(0000) knlGS:0000000000000000 CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 CR2: 0000000000000008 CR3: 000000005942c002 CR4: 00000000001706f0 Call Trace: <TASK> ? __die+0x1f/0x70	2024-09-04	5.5	Medium

		? page_fault_oops+0x15d/0x440
		? search_module_extables+0xe/0x40
		? fixup_exception+0x22/0x2f0
		? exc_page_fault+0x5f/0x100
		? asm_exc_page_fault+0x22/0x30
		? cachefiles_prepare_write+0x30/0xa0
		netfs_rreq_write_to_cache_work+0x135/0x2e0
		process_one_work+0x137/0x2c0
		worker_thread+0x2e9/0x400
		? __pfx_worker_thread+0x10/0x10
		kthread+0xcc/0x100
		? __pfx_kthread+0x10/0x10
		ret_from_fork+0x30/0x50
		? __pfx_kthread+0x10/0x10
		ret_from_fork_asm+0x1b/0x30
		</TASK>
		Modules linked in:
		CR2: 0000000000000008
		---[end trace 0000000000000000]---
		
		This happened because fscache_cookie_state_machine() was slow and was still running while another process invoked fscache_unuse_cookie(); this led to a fscache_cookie_lru_do_one() call, setting the FSCACHE_COOKIE_DO_LRU_DISCARD flag, which was picked up by fscache_cookie_state_machine(), withdrawing the cookie via cachefiles_withdraw_cookie(), clearing cookie->cache_priv.
		
		At the same time, yet another process invoked cachefiles_prepare_write(), which found a NULL pointer in this code line:
		
		struct cachefiles_object *object = cachefiles_cres_object(cres);
		
		The next line crashes, obviously:
		
		struct cachefiles_cache *cache = object->volume->cache;
		
		During cachefiles_prepare_write(), the "n_accesses" counter is non-zero (via fscache_begin_operation()). The cookie must not be withdrawn until it drops to zero.
		
		The counter is checked by fscache_cookie_state_machine() before switching to FSCACHE_COOKIE_STATE_RELINQUISHING and FSCACHE_COOKIE_STATE_WITHDRAWING (in "case FSCACHE_COOKIE_STATE_FAILED"), but not for FSCACHE_COOKIE_STATE_LRU_DISCARDING ("case FSCACHE_COOKIE_STATE_ACTIVE").
		
		This patch adds the missing check. With a non-zero access counter, the function returns and the next fscache_end_cookie_access() call will queue another fscache_cookie_state_machine() call to handle the still-pending FSCACHE_COOKIE_DO_LRU_DISCARD.			

CVE-2024-45002	Linux	In the Linux kernel, the following vulnerability has been resolved: rtla/osnoise: Prevent NULL dereference in error handling If the "tool->data" allocation fails then there is no need to call osnoise_free_top() and, in fact, doing so will lead to a NULL dereference.	2024-09-04	5.5	Medium
CVE-2024-45006	Linux	In the Linux kernel, the following vulnerability has been resolved: xhci: Fix Panther point NULL pointer deref at full-speed re-enumeration re-enumerating full-speed devices after a failed address device command can trigger a NULL pointer dereference. Full-speed devices may need to reconfigure the endpoint 0 Max Packet Size value during enumeration. Usb core calls usb_ep0_reinit() in this case, which ends up calling xhci_configure_endpoint().	2024-09-04	5.5	Medium

		On Panther point xHC the xhci_configure_endpoint() function will additionally check and reserve bandwidth in software. Other hosts do this in hardware If xHC address device command fails then a new xhci_virt_device structure is allocated as part of re-enabling the slot, but the bandwidth table pointers are not set up properly here. This triggers the NULL pointer dereference the next time usb_ep0_reinit() is called and xhci_configure_endpoint() tries to check and reserve bandwidth [46710.713538] usb 3-1: new full-speed USB device number 5 using xhci_hcd [46710.713699] usb 3-1: Device not responding to setup address. [46710.917684] usb 3-1: Device not responding to setup address. [46711.125536] usb 3-1: device not accepting address 5, error -71 [46711.125594] BUG: kernel NULL pointer dereference, address: 0000000000000008 [46711.125600] #PF: supervisor read access in kernel mode [46711.125603] #PF: error_code(0x0000) - not-present page [46711.125606] PGD 0 P4D 0 [46711.125610] Oops: Oops: 0000 [#1] PREEMPT SMP PTI [46711.125615] CPU: 1 PID: 25760 Comm: kworker/1:2 Not tainted 6.10.3_2 #1 [46711.125620] Hardware name: Gigabyte Technology Co., Ltd. [46711.125623] Workqueue: usb_hub_wq hub_event [usbcore] [46711.125668] RIP: 0010:xhci_reserve_bandwidth (drivers/usb/host/xhci.c Fix this by making sure bandwidth table pointers are set up correctly after a failed address device command, and additionally by avoiding checking for bandwidth in cases like this where no actual endpoints are added or removed, i.e. only context for default control endpoint 0 is evaluated.			
CVE-2024-45107	Adobe	Acrobat Reader versions 20.005.30636, 24.002.20964, 24.001.30123, 24.002.20991 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2024-09-05	5.5	Medium
CVE-2023-52915	Linux	In the Linux kernel, the following vulnerability has been resolved: media: dvb-usb-v2: af9035: Fix null-ptr-deref in af9035_i2c_master_xfer In af9035_i2c_master_xfer, msg is controlled by user. When msg[i].buf is null and msg[i].len is zero, former checks on msg[i].buf would be passed. Malicious data finally reach af9035_i2c_master_xfer. If accessing msg[i].buf[0] without sanity check, null ptr deref would happen. We add check on msg[i].len to prevent crash. Similar commit: commit 0ed554fd769a ("media: dvb-usb: az6027: fix null-ptr-deref in az6027_i2c_xfer()")	2024-09-06	5.5	Medium
CVE-2024-40680	IBM	IBM MQ Operator 2.0.26 and 3.2.4 could allow a local user to cause a denial of service due to improper memory allocation causing a segmentation fault.	2024-09-07	5.5	Medium
CVE-2024-8388	Mozilla	Multiple prompts and panels from both Firefox and the Android OS could be used to obscure the notification announcing the transition to fullscreen mode after the fix for CVE-2023-6870 in Firefox 121. This could lead to spoofing the browser UI if the sudden appearance of the prompt distracted the user from noticing the visual transition happening behind the prompt. These notifications now use the Android Toast feature. *This bug only affects Firefox on Android. Other operating systems are unaffected.* This vulnerability affects Firefox < 130.	2024-09-03	5.3	Medium
CVE-2024-5956	Trellix	This vulnerability allows unauthenticated remote attackers to bypass authentication and gain partial data access to the vulnerable Trellix IPS Manager with garbage data in response mostly	2024-09-05	5.3	Medium

CVE-2024-6343	Zyxel	A buffer overflow vulnerability in the CGI program of Zyxel ATP series firmware versions from V4.32 through V5.38, USG FLEX series firmware versions from V4.50 through V5.38, USG FLEX 50(W) series firmware versions from V4.16 through V5.38, and USG20(W)-VPN series firmware versions from V4.16 through V5.38 could allow an authenticated attacker with administrator privileges to cause denial of service (DoS) conditions by sending a crafted HTTP request to a vulnerable device.	2024-09-03	4.9	Medium
CVE-2024-37136	Dell	Dell Path to PowerProtect, versions 1.1, 1.2, contains an Exposure of Private Personal Information to an Unauthorized Actor vulnerability. A remote high privileged attacker could potentially exploit this vulnerability, leading to information exposure.	2024-09-03	4.9	Medium
CVE-2024-8399	Mozilla	Websites could utilize Javascript links to spoof URL addresses in the Focus navigation bar This vulnerability affects Focus for iOS < 130.	2024-09-03	4.7	Medium
CVE-2024-20497	Cisco	A vulnerability in Cisco Expressway Edge (Expressway-E) could allow an authenticated, remote attacker to masquerade as another user on an affected system. This vulnerability is due to inadequate authorization checks for Mobile and Remote Access (MRA) users. An attacker could exploit this vulnerability by running a series of crafted commands. A successful exploit could allow the attacker to intercept calls that are destined for a particular phone number or to make phone calls and have that phone number appear on the caller ID. To successfully exploit this vulnerability, the attacker must be an MRA user on an affected system.	2024-09-04	4.3	Medium

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.