الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

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

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 16th of June to 22nd of June. 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 ١٦ يونيو إلى ٢٢ يونيو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- **عالي جدًا: النتيجة الأساسية لCVSS 9.0-10.0**
- **عالي: النتيجة الأساسية لCVSS 7.0-8.9**
- **متوسط: النتيجة الأساسية لCVSS 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-2024-6045 | D-Link | Certain models of D-Link wireless routers contain an undisclosed factory testing backdoor. Unauthenticated attackers on the local area network can force the device to enable Telnet service by accessing a specific URL and can log in by using the administrator credentials obtained from analyzing the firmware. | 2024-06-17 | 8.8 | High |
| CVE-2024-6100 | Google | Type Confusion in V8 in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High) | 2024-06-20 | 8.8 | High |
| CVE-2024-6101 | Google | Inappropriate implementation in V8 in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High) | 2024-06-20 | 8.8 | High |
| CVE-2024-6102 | Google | Out of bounds memory access in Dawn in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) | 2024-06-20 | 8.8 | High |
| CVE-2024-6103 | Google | Use after free in Dawn in Google Chrome prior to 126.0.6478.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High) | 2024-06-20 | 8.8 | High |
| CVE-2024-37532 | IBM | IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to identity spoofing by an authenticated user due to improper signature validation.  IBM X-Force ID:  294721. | 2024-06-20 | 8.8 | High |
| CVE-2024-31890 | IBM | IBM i 7.3, 7.4, and 7.5 product IBM TCP/IP Connectivity Utilities for i contains a local privilege escalation vulnerability. A malicious actor with command line access to the host operating system can elevate privileges to gain root access to the host operating system.  IBM X-Force ID:  288171. | 2024-06-21 | 7.8 | High |
| CVE-2024-36477 | Linux | In the Linux kernel, the following vulnerability has been resolved:<br><br>tpm_tis_spi: Account for SPI header when allocating TPM SPI xfer buffer<br><br>The TPM SPI transfer mechanism uses MAX_SPI_FRAMESIZE for computing the<br>maximum transfer length and the size of the transfer buffer. As such, it<br>does not account for the 4 bytes of header that prepends the SPI data<br>frame. This can result in out-of-bounds accesses and was confirmed with<br>KASAN.<br><br>Introduce SPI_HDRSIZE to account for the header and use to allocate the<br>transfer buffer. | 2024-06-21 | 7.8 | High |
| CVE-2024-39277 | Linux | In the Linux kernel, the following vulnerability has been resolved:<br><br>dma-mapping: benchmark: handle NUMA_NO_NODE correctly | 2024-06-21 | 7.8 | High |

| | | | | | |
|---|---|---|---|---|---|
| | | cpumask_of_node() can be called for NUMA_NO_NODE inside<br>do_map_benchmark()<br>resulting in the following sanitizer report:<br><br>UBSAN: array-index-out-of-bounds in<br>./arch/x86/include/asm/topology.h:72:28<br>index -1 is out of range for type 'cpumask [64][1]'<br>CPU: 1 PID: 990 Comm: dma_map_benchma Not tainted 6.9.0-rc6<br>#29<br>Hardware name: QEMU Standard PC (i440FX + PIIX, 1996)<br>Call Trace:<br> <TASK><br>dump_stack_lvl (lib/dump_stack.c:117)<br>ubsan_epilogue (lib/ubsan.c:232)<br>__ubsan_handle_out_of_bounds (lib/ubsan.c:429)<br>cpumask_of_node (arch/x86/include/asm/topology.h:72) [inline]<br>do_map_benchmark (kernel/dma/map_benchmark.c:104)<br>map_benchmark_ioctl (kernel/dma/map_benchmark.c:246)<br>full_proxy_unlocked_ioctl (fs/debugfs/file.c:333)<br>__x64_sys_ioctl (fs/ioctl.c:890)<br>do_syscall_64 (arch/x86/entry/common.c:83)<br>entry_SYSCALL_64_after_hwframe<br>(arch/x86/entry/entry_64.S:130)<br><br>Use cpumask_of_node() in place when binding a kernel thread to a<br>cpuset<br>of a particular node.<br><br>Note that the provided node id is checked inside<br>map_benchmark_ioctl().<br>It's just a NUMA_NO_NODE case which is not handled properly<br>later.<br><br>Found by Linux Verification Center (linuxtesting.org). | | | |
| CVE-2024-38329 | IBM | IBM Storage Protect for Virtual Environments: Data Protection for VMware 8.1.0.0 through 8.1.22.0 could allow a remote authenticated attacker to bypass security restrictions, caused by improper validation of user permission. By sending a specially crafted request, an attacker could exploit this vulnerability to change its settings, trigger backups, restore backups, and also delete all previous backups via log rotation. IBM X-Force ID: 294994. | 2024-06-19 | 7.7 | High |
| CVE-2024-38319 | IBM | IBM Security SOAR 51.0.2.0 could allow an authenticated user to execute malicious code loaded from a specially crafted script. IBM X-Force ID: 294830. | 2024-06-22 | 7.5 | High |
| CVE-2024-21685 | Atlassian | This High severity Information Disclosure vulnerability was introduced in versions 9.4.0, 9.12.0, and 9.15.0 of Jira Core Data Center.<br><br>This Information Disclosure vulnerability, with a CVSS Score of 7.4, allows an unauthenticated attacker to view sensitive information via an Information Disclosure vulnerability which has high impact to confidentiality, no impact to integrity, no impact to availability, and requires user interaction.<br><br>Atlassian recommends that Jira Core Data Center customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions:<br><br>Jira Core Data Center 9.4: Upgrade to a release greater than or equal to 9.4.21<br><br>Jira Core Data Center 9.12: Upgrade to a release greater than or equal to 9.12.8<br><br>Jira Core Data Center 9.16: Upgrade to a release greater than or equal to 9.16.0 | 2024-06-18 | 7.4 | High |

| | | | | | |
|---|---|---|---|---|---|
| | | See the release notes. You can download the latest version of Jira Core Data Center from the download center.<br>This vulnerability was found internally. | | | |
| CVE-2023-47726 | IBM | IBM QRadar Suite Software 1.10.12.0 through 1.10.21.0 and IBM Cloud Pak for Security 1.10.12.0 through 1.10.21.0 could allow an authenticated user to execute certain arbitrary commands due to improper input validation.  IBM X-Force ID:  272087. | 2024-06-18 | 7.1 | High |
| CVE-2024-6044 | D-Link | Certain models of D-Link wireless routers have a path traversal vulnerability. Unauthenticated attackers on the same local area network can read arbitrary system files by manipulating the URL. | 2024-06-17 | 6.5 | Medium |
| CVE-2024-36288 | Linux | In the Linux kernel, the following vulnerability has been resolved:<br>SUNRPC: Fix loop termination condition in gss_free_in_token_pages()<br>The in_token->pages[] array is not NULL terminated. This results in the following KASAN splat:<br>KASAN: maybe wild-memory-access in range [0x04a2013400000008-0x04a201340000000f] | 2024-06-21 | 5.5 | Medium |
| CVE-2024-36481 | Linux | In the Linux kernel, the following vulnerability has been resolved:<br>tracing/probes: fix error check in parse_btf_field()<br>btf_find_struct_member() might return NULL or an error via the ERR_PTR() macro. However, its caller in parse_btf_field() only checks for the NULL condition. Fix this by using IS_ERR() and returning the error up the stack. | 2024-06-21 | 5.5 | Medium |
| CVE-2024-38780 | Linux | In the Linux kernel, the following vulnerability has been resolved:<br>dma-buf/sw-sync: don't enable IRQ from sync_print_obj()<br>Since commit a6aa8fca4d79 ("dma-buf/sw-sync: Reduce irqsave/irqrestore from known context") by error replaced spin_unlock_irqrestore() with spin_unlock_irq() for both sync_debugfs_show() and sync_print_obj() despite sync_print_obj() is called from sync_debugfs_show(), lockdep complains inconsistent lock state warning.<br>Use plain spin_{lock,unlock}() for sync_print_obj(), for sync_debugfs_show() is already using spin_{lock,unlock}_irq(). | 2024-06-21 | 5.5 | Medium |
| CVE-2024-38082 | Microsoft | Microsoft Edge (Chromium-based) Spoofing Vulnerability | 2024-06-20 | 4.7 | Medium |
| CVE-2024-38662 | Linux | In the Linux kernel, the following vulnerability has been resolved:<br>bpf: Allow delete from sockmap/sockhash only if update is allowed<br>We have seen an influx of syzkaller reports where a BPF program attached to a tracepoint triggers a locking rule violation by performing a map_delete on a sockmap/sockhash.<br>We don't intend to support this artificial use scenario. Extend the existing verifier allowed-program-type check for updating sockmap/sockhash to also cover deleting from a map.<br>From now on only BPF programs which were previously allowed to update sockmap/sockhash can delete from these map types. | 2024-06-21 | 4.7 | Medium |
| CVE-2024-38093 | Microsoft | Microsoft Edge (Chromium-based) Spoofing Vulnerability | 2024-06-20 | 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.