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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٢ مارس إلى ٨ مارس. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 2nd of March to 8th of March. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2024-55532	apache software foundation - Apache Ranger	Improper Neutralization of Formula Elements in Export CSV feature of Apache Ranger in Apache Ranger Version < 2.6.0. Users are recommended to upgrade to version 2.6.0, which fixes this issue.	2025-03-03	9.8
CVE-2025-22224	vmware - multiple products	VMware ESXi, and Workstation contain a TOCTOU (Time-of-Check Time-of-Use) vulnerability that leads to an out-of-bounds write. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.	2025-03-04	9.3
CVE-2025-1941	mozilla - Firefox	Under certain circumstances, a user opt-in setting that Focus should require authentication before use could have been be bypassed (distinct from CVE-2025-0245). This vulnerability affects Firefox < 136.	2025-03-04	9.1
CVE-2024-43169	ibm - multiple products	IBM Engineering Requirements Management DOORS Next 7.0.2, 7.0.3, and 7.1 could allow a user to download a malicious file without verifying the integrity of the code.	2025-03-03	8.8
CVE-2025-1930	mozilla - multiple products	On Windows, a compromised content process could use bad StreamData sent over AudioIPC to trigger a use-after-free in the Browser process. This could have led to a sandbox escape. This vulnerability affects Firefox < 136, Firefox ESR < 115.21, Firefox ESR < 128.8, Thunderbird < 136, and Thunderbird < 128.8.	2025-03-04	8.8
CVE-2025-1914	google - Chrome	Out of bounds read in V8 in Google Chrome prior to 134.0.6998.35 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	2025-03-05	8.8
CVE-2025-1916	google - Chrome	Use after free in Profiles in Google Chrome prior to 134.0.6998.35 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2025-03-05	8.8
CVE-2025-1918	google - Chrome	Out of bounds read in PDFium in Google Chrome prior to 134.0.6998.35 allowed a remote attacker to potentially perform out of bounds memory access via a crafted PDF file. (Chromium security severity: Medium)	2025-03-05	8.8
CVE-2025-1919	google - Chrome	Out of bounds read in Media in Google Chrome prior to 134.0.6998.35 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	2025-03-05	8.8
CVE-2024-58045	huawei - harmonyos	Multi-concurrency vulnerability in the media digital copyright protection module Impact: Successful exploitation of this vulnerability may affect availability.	2025-03-04	8.6
CVE-2024-58044	huawei - multiple products	Permission verification bypass vulnerability in the notification module Impact: Successful exploitation of this vulnerability may affect availability.	2025-03-04	8.4
CVE-2025-22225	vmware - multiple products	VMware ESXi contains an arbitrary write vulnerability. A malicious actor with privileges within the VMX process may trigger an arbitrary kernel write leading to an escape of the sandbox.	2025-03-04	8.2
CVE-2025-1943	mozilla - multiple products	Memory safety bugs present in Firefox 135 and Thunderbird 135. 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 < 136 and Thunderbird < 136.	2025-03-04	8.2
CVE-2025-1723	manageengine - ADSelfService Plus	Zohocorp ManageEngine ADSelfService Plus versions 6510 and below are vulnerable to account takeover due to the session mishandling. Valid account holders in the setup only have the potential to exploit this bug.	2025-03-03	8.1
CVE-2025-1801	red hat - multiple products	A flaw was found in the Ansible aap-gateway. Concurrent requests handled by the gateway grpc service can result in concurrency issues due to race condition requests against the proxy. This issue potentially allows a less privileged user to obtain the JWT of a greater privileged user, enabling the server to be jeopardized. A user session or confidential data might be vulnerable.	2025-03-03	8.1
CVE-2025-23368	red hat - multiple products	A flaw was found in Wildfly Elytron integration. The component does not implement sufficient measures to prevent multiple failed authentication attempts within a short time frame, making it more susceptible to brute force attacks via CLI.	2025-03-04	8.1

CVE-2025-1915	google - Chrome	Improper Limitation of a Pathname to a Restricted Directory in DevTools in Google Chrome on Windows prior to 134.0.6998.35 allowed an attacker who convinced a user to install a malicious extension to bypass file access restrictions via a crafted Chrome Extension. (Chromium security severity: Medium)	2025-03-05	8.1
CVE-2024-43055	qualcomm - fastconnect_6900_firmware	Memory corruption while processing camera use case IOCTL call.	2025-03-03	7.8
CVE-2024-43057	qualcomm - qcn6224_firmware	Memory corruption while processing command in Glink linux.	2025-03-03	7.8
CVE-2024-43059	qualcomm - sa8770p_firmware	Memory corruption while invoking IOCTL calls from the use-space for HGSL memory node.	2025-03-03	7.8
CVE-2024-43060	qualcomm - ar8035_firmware	Memory corruption during voice activation, when sound model parameters are loaded from HLOS to ADSP.	2025-03-03	7.8
CVE-2024-43061	qualcomm - fastconnect_6900_firmware	Memory corruption during voice activation, when sound model parameters are loaded from HLOS, and the received sound model list is empty in HLOS drive.	2025-03-03	7.8
CVE-2024-43062	qualcomm - fastconnect_6900_firmware	Memory corruption caused by missing locks and checks on the DMA fence and improper synchronization.	2025-03-03	7.8
CVE-2024-45580	qualcomm - fastconnect_6900_firmware	Memory corruption while handling multuple IOCTL calls from userspace for remote invocation.	2025-03-03	7.8
CVE-2024-49836	qualcomm - fastconnect_6900_firmware	Memory corruption may occur during the synchronization of the camera`s frame processing pipeline.	2025-03-03	7.8
CVE-2024-53012	qualcomm - qam8255p_firmware	Memory corruption may occur due to improper input validation in clock device.	2025-03-03	7.8
CVE-2024-53014	qualcomm - sm6370_firmware	Memory corruption may occur while validating ports and channels in Audio driver.	2025-03-03	7.8
CVE-2024-53022	qualcomm - qam8255p_firmware	Memory corruption may occur during communication between primary and guest VM.	2025-03-03	7.8
CVE-2024-53023	qualcomm - ar8035_firmware	Memory corruption may occur while accessing a variable during extended back to back tests.	2025-03-03	7.8
CVE-2024-53024	qualcomm - qcs6490_firmware	Memory corruption in display driver while detaching a device.	2025-03-03	7.8
CVE-2024-53028	qualcomm - qam8255p_firmware	Memory corruption may occur while processing message from frontend during allocation.	2025-03-03	7.8
CVE-2024-53029	qualcomm - qam8255p_firmware	Memory corruption while reading a value from a buffer controlled by the Guest Virtual Machine.	2025-03-03	7.8
CVE-2024-53030	qualcomm - msm8996au_firmware	Memory corruption while processing input message passed from FE driver.	2025-03-03	7.8
CVE-2024-53031	qualcomm - qam8255p_firmware	Memory corruption while reading a type value from a buffer controlled by the Guest Virtual Machine.	2025-03-03	7.8
CVE-2024-53032	qualcomm - qam8255p_firmware	Memory corruption may occur in keyboard virtual device due to guest VM interaction.	2025-03-03	7.8
CVE-2024-53033	qualcomm - fastconnect_6900_firmware	Memory corruption while doing Escape call when user provides valid kernel address in the place of valid user buffer address.	2025-03-03	7.8
CVE-2024-53034	qualcomm - fastconnect_6900_firmware	Memory corruption occurs during an Escape call if an invalid Kernel Mode CPU event and sync object handle are passed with the DriverKnownEscape flag reset.	2025-03-03	7.8
CVE-2025-21424	qualcomm - 315_5g_iot_modem_firmware	Memory corruption while calling the NPU driver APIs concurrently.	2025-03-03	7.8
CVE-2024-58060	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: bpf: Reject struct_ops registration that uses module ptr and the module btf_id is missing There is a UAF report in the bpf_struct_ops when CONFIG_MODULES=n. In particular, the report is on tcp_congestion_ops that has a "struct module *owner" member. For struct_ops that has a "struct module *owner" member, it can be extended either by the regular kernel module or by the bpf_struct_ops. bpf_try_module_get() will be used to do the refcounting and different refcount is done based on the owner pointer. When CONFIG_MODULES=n, the btf_id of the "struct module" is missing: WARN: resolve_btfids: unresolved symbol module	2025-03-06	7.8

		Thus, the bpf_try_module_get() cannot do the correct refcounting. Not all subsystem's struct_ops requires the "struct module *owner" member. e.g. the recent sched_ext_ops. This patch is to disable bpf_struct_ops registration if the struct_ops has the "struct module *" member and the "struct module" btf_id is missing. The btf_type_is_fwd() helper is moved to the btf.h header file for this test. This has happened since the beginning of bpf_struct_ops which has gone through many changes. The Fixes tag is set to a recent commit that this patch can apply cleanly. Considering CONFIG_MODULES=n is not common and the age of the issue, targeting for bpf-next also.		
CVE-2025-26331	dell - Wyse Proprietary OS (Modern ThinOS)	Dell ThinOS 2411 and prior, contains an Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary code execution.	2025-03-07	7.8
CVE-2024-53027	qualcomm - qca9367_firmware	Transient DOS may occur while processing the country IE.	2025-03-03	7.5
CVE-2024-41770	ibm - multiple products	IBM Engineering Requirements Management DOORS Next 7.0.2, 7.0.3, and 7.1 could allow a remote attacker to download temporary files which could expose application logic or other sensitive information.	2025-03-03	7.5
CVE-2024-41771	ibm - multiple products	IBM Engineering Requirements Management DOORS Next 7.0.2, 7.0.3, and 7.1 could allow a remote attacker to download temporary files which could expose application logic or other sensitive information.	2025-03-03	7.5
CVE-2025-1937	mozilla - multiple products	Memory safety bugs present in Firefox 135, Thunderbird 135, Firefox ESR 115.20, Firefox ESR 128.7, and Thunderbird 128.7. 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 < 136, Firefox ESR < 115.21, Firefox ESR < 128.8, Thunderbird < 136, and Thunderbird < 128.8.	2025-03-04	7.5
CVE-2024-51476	ibm - Concert Software	IBM Concert Software 1.0.5 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials.	2025-03-06	7.5
CVE-2024-58043	huawei - multiple products	Permission bypass vulnerability in the window module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-03-04	7.3
CVE-2025-22226	vmware - multiple products	VMware ESXi, Workstation, and Fusion contain an information disclosure vulnerability due to an out-of-bounds read in HGFS. A malicious actor with administrative privileges to a virtual machine may be able to exploit this issue to leak memory from the vmx process.	2025-03-04	7.1
CVE-2025-1940	mozilla - Firefox	A select option could partially obscure the confirmation prompt shown before launching external apps. This could be used to trick a user in to launching an external app unexpectedly. *This issue only affects Android versions of Firefox.* This vulnerability affects Firefox < 136.	2025-03-04	7.1
CVE-2025-20206	cisco - Cisco Secure Client	A vulnerability in the interprocess communication (IPC) channel of Cisco Secure Client for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack on an affected device if the Secure Firewall Posture Engine, formerly HostScan, is installed on Cisco Secure Client._x000D_ _x000D_ This vulnerability is due to insufficient validation of resources that are loaded by the application at run time. An attacker could exploit this vulnerability by sending a crafted IPC message to a specific Cisco Secure Client process. A successful exploit could allow the attacker to execute arbitrary code on the affected machine with SYSTEM privileges. To exploit this vulnerability, the attacker must have valid user credentials on the Windows system.	2025-03-05	7.1
CVE-2025-0162	ibm - multiple products	IBM Aspera Shares 1.9.9 through 1.10.0 PL7 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote authenticated attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	2025-03-07	7.1
CVE-2025-1876	d-link - DAP-1562	A vulnerability, which was classified as critical, has been found in D-Link DAP-1562 1.10. Affected by this issue is the function http_request_parse of the component HTTP Header Handler. The manipulation of the argument Authorization leads to stack-based buffer overflow. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2025-03-03	6.9
CVE-2025-1695	f5 - nginx	In NGINX Unit before version 1.34.2 with the Java Language Module in use, undisclosed requests can lead to an infinite loop and cause an increase in CPU resource utilization. This vulnerability allows a remote attacker to cause a degradation that can lead to a limited denial-of-service (DoS). There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2025-03-04	6.9
CVE-2025-27521	huawei - harmonyos	Vulnerability of improper access permission in the process management module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-03-04	6.8
CVE-2025-1121	google - ChromeOS	Privilege escalation in Installer and Recovery image handling in Google ChromeOS 123.0.6312.112 on device allows an attacker with physical access to gain root code execution and potentially unenroll enterprise-managed devices via a specially crafted recovery image.	2025-03-07	6.8
CVE-2024-45780	gnu - grub2	A flaw was found in grub2. When reading tar files, grub2 allocates an internal buffer for the file name. However, it fails to properly verify the allocation against possible integer overflows. It's possible to cause the allocation length to overflow with a crafted tar file, leading to a heap out-of-bounds write. This flaw eventually allows an attacker to circumvent secure boot protections.	2025-03-03	6.7
CVE-2024-45782	gnu - grub2	A flaw was found in the HFS filesystem. When reading an HFS volume's name at grub_fs_mount(), the HFS filesystem driver performs a strcpy() using the user-provided volume name as input without properly validating the volume name's length. This issue may read to a heap-based out-of-bounds writer, impacting grub's sensitive data integrity and eventually leading to a secure boot protection bypass.	2025-03-03	6.7

CVE-2024-58048	huawei - harmonyos	Multi-thread problem vulnerability in the package management module Impact: Successful exploitation of this vulnerability may affect availability.	2025-03-04	6.7
CVE-2024-24778	apache software foundation - Apache StreamPipes	Improper privilege management in a REST interface allowed registered users to access unauthorized resources if the resource ID was know. This issue affects Apache StreamPipes: through 0.95.1. Users are recommended to upgrade to version 0.97.0 which fixes the issue.	2025-03-03	6.5
CVE-2025-1938	mozilla - multiple products	Memory safety bugs present in Firefox 135, Thunderbird 135, Firefox ESR 128.7, and Thunderbird 128.7. 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 < 136, Firefox ESR < 128.8, Thunderbird < 136, and Thunderbird < 128.8.	2025-03-04	6.5
CVE-2025-1921	google - Chrome	Inappropriate implementation in Media Stream in Google Chrome prior to 134.0.6998.35 allowed a remote attacker to obtain information about a peripheral via a crafted HTML page. (Chromium security severity: Medium)	2025-03-05	6.5
CVE-2024-57972	microsoft - multiple products	The pairing API request handler in Microsoft HoloLens 1 (Windows Holographic) through 10.0.17763.3046 and HoloLens 2 (Windows Holographic) through 10.0.22621.1244 allows remote attackers to cause a Denial of Service (resource consumption and device unusability) by sending many requests through the Device Portal framework.	2025-03-06	6.5
CVE-2025-0678	gnu - grub2	A flaw was found in grub2. When reading data from a squash4 filesystem, grub's squash4 fs module uses user-controlled parameters from the filesystem geometry to determine the internal buffer size, however, it improperly checks for integer overflows. A maliciously crafted filesystem may lead some of those buffer size calculations to overflow, causing it to perform a grub_malloc() operation with a smaller size than expected. As a result, the direct_read() will perform a heap based out-of-bounds write during data reading. This flaw may be leveraged to corrupt grub's internal critical data and may result in arbitrary code execution, by-passing secure boot protections.	2025-03-03	6.4
CVE-2024-38311	apache software foundation - Apache Traffic Server	Improper Input Validation vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.11, from 9.0.0 through 9.2.8, from 10.0.0 through 10.0.3. Users are recommended to upgrade to version 9.2.9 or 10.0.4, which fixes the issue.	2025-03-06	6.3
CVE-2024-56195	apache software foundation - Apache Traffic Server	Improper Access Control vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 9.2.0 through 9.2.8, from 10.0.0 through 10.0.3. Users are recommended to upgrade to version 9.2.9 or 10.0.4, which fixes the issue.	2025-03-06	6.3
CVE-2024-56196	apache software foundation - Apache Traffic Server	Improper Access Control vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 10.0.0 through 10.0.3. Users are recommended to upgrade to version 10.0.4, which fixes the issue.	2025-03-06	6.3
CVE-2024-58046	huawei - harmonyos	Permission management vulnerability in the lock screen module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-03-04	6.2
CVE-2024-58050	huawei - harmonyos	Vulnerability of improper access permission in the HDC module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-03-04	6.2
CVE-2024-43051	qualcomm - aqt1000_firmware	Information disclosure while deriving keys for a session for any Widevine use case.	2025-03-03	5.5
CVE-2024-43056	qualcomm - aqt1000_firmware	Transient DOS during hypervisor virtual I/O operation in a virtual machine.	2025-03-03	5.5
CVE-2024-53025	qualcomm - fastconnect_7800_firmware	Transient DOS can occur while processing UCI command.	2025-03-03	5.5
CVE-2025-21843	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: avoid garbage value in panthor_ioctl_dev_query() 'priorities_info' is uninitialized, and the uninitialized value is copied to user object when calling PANTHOR_UOBJ_SET(). Using memset to initialize 'priorities_info' to avoid this garbage value problem.	2025-03-07	5.5
CVE-2024-38426	qualcomm - 315_5g_iot_firmware	While processing the authentication message in UE, improper authentication may lead to information disclosure.	2025-03-03	5.4
CVE-2024-54179	ibm - multiple products	IBM Business Automation Workflow and IBM Business Automation Workflow Enterprise Service Bus 24.0.0, 24.0.1 and earlier unsupported versions are vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2025-03-03	5.4
CVE-2025-27426	mozilla - Firefox for iOS	Malicious websites utilizing a server-side redirect to an internal error page could result in a spoofed website URL This vulnerability affects Firefox for iOS < 136.	2025-03-04	5.4
CVE-2023-35894	ibm - multiple products	IBM Control Center 6.2.1 through 6.3.1 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking.	2025-03-07	5.4
CVE-2025-26643	microsoft - edge_chromium	The UI performs the wrong action in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2025-03-07	5.4

CVE-2019-1815	cisco - Cisco Meraki MX Firmware	A security vulnerability was discovered in the local status page functionality of Cisco Meraki's MX67 and MX68 security appliance models that may allow unauthenticated individuals to access and download logs containing sensitive, privileged device information. The vulnerability is due to improper access control to the files holding debugging and maintenance information, and is only exploitable when the local status page is enabled on the device. An attacker exploiting this vulnerability may obtain access to wireless pre-shared keys, Site-to-Site VPN key and other sensitive information. Under certain circumstances, this information may allow an attacker to obtain administrative-level access to the device.	2025-03-04	5.3
CVE-2020-3122	cisco - multiple products	A vulnerability in the web-based management interface of Cisco AsyncOS for Cisco Content Security Management Appliance (SMA) could allow an unauthenticated, remote attacker to obtain sensitive network information.	2025-03-04	5.3
CVE-2023-43052	ibm - Control Center	IBM Control Center 6.2.1 through 6.3.1 is vulnerable to an external service interaction attack, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability to induce the application to perform server-side DNS lookups or HTTP requests to arbitrary domain names. By submitting suitable payloads, an attacker can cause the application server to attack other systems that it can interact with.	2025-03-07	5.3
CVE-2025-1696	docker - Docker Desktop	A vulnerability exists in Docker Desktop prior to version 4.39.0 that could lead to the unintentional disclosure of sensitive information via application logs. In affected versions, proxy configuration data—potentially including sensitive details—was written to log files in clear text whenever an HTTP GET request was made through a proxy. An attacker with read access to these logs could obtain the proxy information and leverage it for further attacks or unauthorized access. Starting with version 4.39.0, Docker Desktop no longer logs the proxy string, thereby mitigating this risk.	2025-03-06	5.2
CVE-2024-58047	huawei - harmonyos	Permission verification vulnerability in the media library module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-03-04	5
CVE-2024-58049	huawei - harmonyos	Permission verification vulnerability in the media library module Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-03-04	5
CVE-2022-49733	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ALSA: pcm: oss: Fix race at SNDCTL_DSP_SYNC There is a small race window at snd_pcm_oss_sync() that is called from OSS PCM SNDCTL_DSP_SYNC ioctl; namely the function calls snd_pcm_oss_make_ready() at first, then takes the params_lock mutex for the rest. When the stream is set up again by another thread between them, it leads to inconsistency, and may result in unexpected results such as NULL dereference of OSS buffer as a fuzzer spotted recently. The fix is simply to cover snd_pcm_oss_make_ready() call into the same params_lock mutex with snd_pcm_oss_make_ready_locked() variant.	2025-03-02	4.7
CVE-2025-20208	cisco - Cisco TelePresence Management Suite (TMS)	A vulnerability in the web-based management interface of Cisco TelePresence Management Suite (TMS) could allow a low-privileged, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. _x000D_ _x000D_ This vulnerability is due to insufficient input validation by the web-based management interface. An attacker could exploit this vulnerability by inserting malicious data in a specific data field in the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2025-03-05	4.6
CVE-2025-27424	mozilla - Firefox for iOS	Websites redirecting to a non-HTTP scheme URL could allow a website address to be spoofed for a malicious page This vulnerability affects Firefox for iOS < 136.	2025-03-04	4.3
CVE-2025-27425	mozilla - Firefox for iOS	Scanning certain QR codes that included text with a website URL could allow the URL to be opened without presenting the user with a confirmation alert first This vulnerability affects Firefox for iOS < 136.	2025-03-04	4.3
CVE-2025-1917	google - Chrome	Inappropriate implementation in Browser UI in Google Chrome on Android prior to 134.0.6998.35 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2025-03-05	4.3
CVE-2025-1922	google - Chrome	Inappropriate implementation in Selection in Google Chrome on Android prior to 134.0.6998.35 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: Low)	2025-03-05	4.3
CVE-2025-1923	google - Chrome	Inappropriate implementation in Permission Prompts in Google Chrome prior to 134.0.6998.35 allowed an attacker who convinced a user to install a malicious extension to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Low)	2025-03-05	4.3
CVE-2024-56202	apache software foundation - Apache Traffic Server	Expected Behavior Violation vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 9.0.0 through 9.2.8, from 10.0.0 through 10.0.3. Users are recommended to upgrade to versions 9.2.9 or 10.0.4 or newer, which fixes the issue.	2025-03-06	4.3
CVE-2024-45779	gnu - grub2	An integer overflow flaw was found in the BFS file system driver in grub2. When reading a file with an indirect extent map, grub2 fails to validate the number of extent entries to be read. A crafted or corrupted BFS filesystem may cause an integer overflow during the file reading, leading to a heap of bounds read. As a consequence, sensitive data may be leaked, or grub2 will crash.	2025-03-03	4.1
CVE-2024-45778	gnu - grub2	A stack overflow flaw was found when reading a BFS file system. A crafted BFS filesystem may lead to an uncontrolled loop, causing grub2 to crash.	2025-03-03	4.1
CVE-2025-1939	mozilla - Firefox	Android apps can load web pages using the Custom Tabs feature. This feature supports a transition animation that could have been used to trick a user into granting sensitive permissions by hiding what the user was actually clicking. This vulnerability affects Firefox < 136.	2025-03-04	3.9
CVE-2024-11035	symantec - Carbon Black Cloud Windows Sensor	Carbon Black Cloud Windows Sensor, prior to 4.0.3, may be susceptible to an Information Leak vulnerability, which s a type of issue whereby sensitive information may b exposed due to a vulnerability in software.	2025-03-05	2.5

CVE-2025-0895	ibm - Cognos Analytics Mobile	IBM Cognos Analytics Mobile 1.1 for Android could allow a user with physical access to the device, to obtain sensitive information from debugging code log messages.	2025-03-02	2.4
CVE-2024-55907	ibm - Cognos Analytics Mobile	IBM Cognos Analytics Mobile 1.1 for iOS application could allow an attacker to reverse engineer the codebase to gain knowledge about the programming technique, interface, class definitions, algorithms and functions used due to weak obfuscation.	2025-03-02	2

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.