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

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٢٢ اكتوبر إلى ٢٨ اكتوبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 22nd of October to 28th of October. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2022-22466	ibm - security_verify_governance	IBM Security Verify Governance 10.0 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 225222.	2023-10-23	9.8	Critical
CVE-2023-34048	vmware - multiple products	vCenter Server contains an out-of-bounds write vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger an out-of-bounds write potentially leading to remote code execution.	2023-10-25	9.8	Critical
CVE-2023-46158	ibm - websphere_application_server_liberty	IBM WebSphere Application Server Liberty 23.0.0.9 through 23.0.0.10 could provide weaker than expected security due to improper resource expiration handling. IBM X-Force ID: 268775.	2023-10-25	9.8	Critical
CVE-2023-46371	tp-link - tl-wdr7660_firmware	TP-Link device TL-WDR7660 2.0.30 has a stack overflow vulnerability via the function upgradeInfoJsonToBin.	2023-10-25	9.8	Critical
CVE-2023-46373	tp-link - tl-wdr7660_firmware	TP-Link TL-WDR7660 2.0.30 has a stack overflow vulnerability via the function deviceInfoJsonToBincauses.	2023-10-25	9.8	Critical
CVE-2023-46520	tp-link - tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function uninstallPluginReqHandle.	2023-10-25	9.8	Critical
CVE-2023-46521	tp-link - tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function RegisterRegister.	2023-10-25	9.8	Critical
CVE-2023-46522	tp-link - tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function deviceInfoRegister.	2023-10-25	9.8	Critical
CVE-2023-46523	tp-link - tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function upgradeInfoRegister.	2023-10-25	9.8	Critical
CVE-2023-46525	tp-link - tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function loginRegister.	2023-10-25	9.8	Critical
CVE-2023-46526	tp-link - tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function resetCloudPwdRegister.	2023-10-25	9.8	Critical
CVE-2023-46527	tp-link - tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function bindRequestHandle.	2023-10-25	9.8	Critical
CVE-2023-46534	tp-link - tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function modifyAccPwdRegister.	2023-10-25	9.8	Critical
CVE-2023-46535	tp-link - tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function getResetVeriRegister.	2023-10-25	9.8	Critical
CVE-2023-46536	tp-link - tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function chkRegVeriRegister.	2023-10-25	9.8	Critical

CVE-2023-46537	tp-link - tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function getRegVeriRegister.	2023-10-25	9.8	Critical
CVE-2023-46538	tp-link - tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function chkResetVeriRegister.	2023-10-25	9.8	Critical
CVE-2023-46539	tp-link - tl-wr886n_firmware	TP-LINK TL-WR886N V7.0_3.0.14_Build_221115_Rel.56908n.bin was discovered to contain a stack overflow via the function registerRequestHandle.	2023-10-25	9.8	Critical
CVE-2023-5730	mozilla - multiple products	Memory safety bugs present in Firefox 118, Firefox ESR 115.3, and Thunderbird 115.3. 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 < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	9.8	Critical
CVE-2023-5731	mozilla - firefox	Memory safety bugs present in Firefox 118. 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 < 119.	2023-10-25	9.8	Critical
CVE-2023-5746	synology - bc500_firmware	A vulnerability regarding use of externally-controlled format string is found in the cgi component. This allows remote attackers to execute arbitrary code via unspecified vectors. The following models with Synology Camera Firmware versions before 1.0.5-0185 may be affected: BC500 and TC500.	2023-10-25	9.8	Critical
CVE-2023-33839	ibm - multiple products	IBM Security Verify Governance 10.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 256036.	2023-10-23	8.8	High
CVE-2023-43507	arubanetworks - multiple products	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit this vulnerability to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster.	2023-10-25	8.8	High
CVE-2023-5472	google - chrome	Use after free in Profiles in Google Chrome prior to 118.0.5993.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-10-25	8.8	High
CVE-2023-40447	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution.	2023-10-25	8.8	High
CVE-2023-41976	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution.	2023-10-25	8.8	High
CVE-2023-42852	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Sonoma 14.1, Safari 17.1, tvOS 17.1. Processing web content may lead to arbitrary code execution.	2023-10-25	8.8	High
CVE-2023-40129	google - multiple products	In build_read_multi_rsp of gatt_sr.cc, there is a possible out of bounds write due to a heap buffer overflow. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	8.8	High
CVE-2023-46654	jenkins - cloudbees_cd	Jenkins CloudBees CD Plugin 1.1.32 and earlier follows symbolic links to locations outside of the expected directory during the cleanup process of the 'CloudBees CD - Publish Artifact' post-build step, allowing attackers able to configure jobs to delete arbitrary files on the Jenkins controller file system.	2023-10-25	8.1	High
CVE-2023-43066	dell - multiple products	Dell Unity prior to 5.3 contains a Restricted Shell Bypass vulnerability. This could allow an authenticated, local attacker to exploit this vulnerability by authenticating to the device CLI and issuing certain commands.	2023-10-23	7.8	High
CVE-2023-5633	linux - multiple products	The reference count changes made as part of the CVE-2023-33951 and CVE-2023-33952 fixes exposed a use-after-free flaw in the way memory objects were handled when they were being used to store a surface. When running inside a VMware guest with 3D acceleration enabled, a local, unprivileged user could potentially use this flaw to escalate their privileges.	2023-10-23	7.8	High
CVE-2022-3699	lenovo - multiple products	A privilege escalation vulnerability was reported in the Lenovo HardwareScanPlugin prior to version 1.3.1.2 and Lenovo Diagnostics prior to version 4.45 that could allow a local user to execute code with elevated privileges.	2023-10-25	7.8	High
CVE-2023-43506	arubanetworks - multiple products	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges to those of a higher role. A successful exploit allows malicious	2023-10-25	7.8	High

		users to execute arbitrary code with root level privileges on the Linux instance.			
CVE-2023-4692	gnu - grub2	An out-of-bounds write flaw was found in grub2's NTFS filesystem driver. This issue may allow an attacker to present a specially crafted NTFS filesystem image, leading to grub's heap metadata corruption. In some circumstances, the attack may also corrupt the UEFI firmware heap metadata. As a result, arbitrary code execution and secure boot protection bypass may be achieved.	2023-10-25	7.8	High
CVE-2023-5717	linux - multiple products	A heap out-of-bounds write vulnerability in the Linux kernel's Linux Kernel Performance Events (perf) component can be exploited to achieve local privilege escalation. If perf_read_group() is called while an event's sibling_list is smaller than its child's sibling_list, it can increment or write to memory locations outside of the allocated buffer. We recommend upgrading past commit 32671e3799ca2e4590773fd0e63aaa4229e50c06.	2023-10-25	7.8	High
CVE-2023-40404	apple - macos	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges.	2023-10-25	7.8	High
CVE-2023-40423	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to execute arbitrary code with kernel privileges.	2023-10-25	7.8	High
CVE-2023-42841	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1. An app may be able to execute arbitrary code with kernel privileges.	2023-10-25	7.8	High
CVE-2023-42856	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. Processing a file may lead to unexpected app termination or arbitrary code execution.	2023-10-25	7.8	High
CVE-2023-40116	google - multiple products	In onTaskAppeared of PipTaskOrganizer.java, there is a possible way to bypass background activity launch restrictions due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	7.8	High
CVE-2023-40117	google - multiple products	In resetSettingsLocked of SettingsProvider.java, there is a possible lockscreen bypass due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	7.8	High
CVE-2023-40120	google - multiple products	In multiple locations, there is a possible way to bypass user notification of foreground services due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	7.8	High
CVE-2023-40125	google - multiple products	In onCreate of ApnEditor.java, there is a possible way for a Guest user to change the APN due to a permission bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	7.8	High
CVE-2023-40128	google - multiple products	In several functions of xmlregexp.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	7.8	High
CVE-2023-40130	google - multiple products	In onBindingDied of CallRedirectionProcessor.java, there is a possible permission bypass due to a logic error in the code. This could lead to local escalation of privilege and background activity launch with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	7.8	High
CVE-2023-38275	ibm - cognos_dashboards_on_cloud_pak_for_data	IBM Cognos Dashboards on Cloud Pak for Data 4.7.0 exposes sensitive information in container images which could lead to further attacks against the system. IBM X-Force ID: 260730.	2023-10-22	7.5	High
CVE-2023-38276	ibm - cognos_dashboards_on_cloud_pak_for_data	IBM Cognos Dashboards on Cloud Pak for Data 4.7.0 exposes sensitive information in environment variables which could aid in further attacks against the system. IBM X-Force ID: 260736.	2023-10-22	7.5	High
CVE-2023-31122	apache - http_server	Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.This issue affects Apache HTTP Server: through 2.4.57.	2023-10-23	7.5	High
CVE-2023-43622	apache - http_server	An attacker, opening a HTTP/2 connection with an initial window size of 0, was able to block handling of that connection indefinitely in Apache HTTP Server. This could be used to exhaust worker resources in the server, similar to the well known "slow loris" attack pattern. This has been fixed in version 2.4.58, so that such connection are terminated properly after the configured connection timeout.	2023-10-23	7.5	High

		This issue affects Apache HTTP Server: from 2.4.55 through 2.4.57. Users are recommended to upgrade to version 2.4.58, which fixes the issue.			
CVE-2023-43074	dell - multiple products	Dell Unity 5.3 contain(s) an Arbitrary File Creation vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability by crafting arbitrary files through a request to the server.	2023-10-23	7.5	High
CVE-2023-43045	ibm - multiple products	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 could allow a remote user to perform unauthorized actions due to improper authentication. IBM X-Force ID: 266896.	2023-10-23	7.5	High
CVE-2023-33837	ibm - security_verify_governance	IBM Security Verify Governance 10.0 does not encrypt sensitive or critical information before storage or transmission. IBM X-Force ID: 256020.	2023-10-23	7.5	High
CVE-2023-46120	vmware - rabbitmq_java_client	The RabbitMQ Java client library allows Java and JVM-based applications to connect to and interact with RabbitMQ nodes. `maxBodyLebgth` was not used when receiving Message objects. Attackers could send a very large Message causing a memory overflow and triggering an OOM Error. Users of RabbitMQ may suffer from DoS attacks from RabbitMQ Java client which will ultimately exhaust the memory of the consumer. This vulnerability was patched in version 5.18.0.	2023-10-25	7.5	High
CVE-2023-5724	mozilla - multiple products	Drivers are not always robust to extremely large draw calls and in some cases this scenario could have led to a crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	7.5	High
CVE-2023-5728	mozilla - multiple products	During garbage collection extra operations were performed on a object that should not be. This could have led to a potentially exploitable crash. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	7.5	High
CVE-2023-32359	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in iOS 16.7.2 and iPadOS 16.7.2. A user's password may be read aloud by VoiceOver.	2023-10-25	7.5	High
CVE-2023-40401	apple - macos	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.6.1. An attacker may be able to access passkeys without authentication.	2023-10-25	7.5	High
CVE-2023-40445	apple - multiple products	The issue was addressed with improved UI handling. This issue is fixed in iOS 17.1 and iPadOS 17.1. A device may persistently fail to lock.	2023-10-25	7.5	High
CVE-2023-42844	apple - multiple products	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. A website may be able to access sensitive user data when resolving symlinks.	2023-10-25	7.5	High
CVE-2023-42847	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An attacker may be able to access passkeys without authentication.	2023-10-25	7.5	High
CVE-2023-20273	cisco - multiple products	A vulnerability in the web UI feature of Cisco IOS XE Software could allow an authenticated, remote attacker to inject commands with the privileges of root. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted input to the web UI. A successful exploit could allow the attacker to inject commands to the underlying operating system with root privileges.	2023-10-25	7.2	High
CVE-2023-38041	ivanti - secure_access_client	A logged in user may elevate its permissions by abusing a Time-of-Check to Time-of-Use (TOCTOU) race condition. When a particular process flow is initiated, an attacker can exploit this condition to gain unauthorized elevated privileges on the affected system.	2023-10-25	7	High
CVE-2023-40131	google - multiple products	In GpuService of GpuService.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	7	High
CVE-2023-41988	apple - multiple products	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data.	2023-10-25	6.8	Medium
CVE-2023-41989	apple - macos	The issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1. An attacker may be able to execute arbitrary code as root from the Lock Screen.	2023-10-25	6.8	Medium
CVE-2023-38735	ibm - cognos_dashboards_on_cloud_pak_for_data	IBM Cognos Dashboards on Cloud Pak for Data 4.7.0 could allow a remote attacker to bypass security restrictions, caused by a reverse tabnabbing flaw. An attacker could exploit this vulnerability and redirect a victim to a phishing site. IBM X-Force ID: 262482.	2023-10-22	6.5	Medium
CVE-2023-43067	dell - multiple products	Dell Unity prior to 5.3 contains an XML External Entity injection	2023-10-23	6.5	Medium

		vulnerability. An XXE attack could potentially exploit this vulnerability disclosing local files in the file system.			
CVE-2023-43508	arubanetworks - multiple products	Vulnerabilities in the web-based management interface of ClearPass Policy Manager allow an attacker with read-only privileges to perform actions that change the state of the ClearPass Policy Manager instance. Successful exploitation of these vulnerabilities allow an attacker to complete state-changing actions in the web-based management interface that should not be allowed by their current level of authorization on the platform.	2023-10-25	6.5	Medium
CVE-2023-46651	jenkins - warnings	Jenkins Warnings Plugin 10.5.0 and earlier does not set the appropriate context for credentials lookup, allowing attackers with Item/Configure permission to access and capture credentials they are not entitled to. This fix has been backported to 10.4.1.	2023-10-25	6.5	Medium
CVE-2023-46653	jenkins - lambdatest-automation	Jenkins lambdatest-automation Plugin 1.20.10 and earlier logs LAMBDATEST Credentials access token at the INFO level, potentially resulting in its exposure.	2023-10-25	6.5	Medium
CVE-2023-46655	jenkins - cloudbees_cd	Jenkins CloudBees CD Plugin 1.1.32 and earlier follows symbolic links to locations outside of the directory from which artifacts are published during the 'CloudBees CD - Publish Artifact' post-build step, allowing attackers able to configure jobs to publish arbitrary files from the Jenkins controller file system to the previously configured CloudBees CD server.	2023-10-25	6.5	Medium
CVE-2023-5568	samba - samba	A heap-based Buffer Overflow flaw was discovered in Samba. It could allow a remote, authenticated attacker to exploit this vulnerability to cause a denial of service.	2023-10-25	6.5	Medium
CVE-2023-5727	mozilla - multiple products	The executable file warning was not presented when downloading .msix, .msixbundle, .appx, and .appxbundle files, which can run commands on a user's computer. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	6.5	Medium
CVE-2023-5732	mozilla - multiple products	An attacker could have created a malicious link using bidirectional characters to spoof the location in the address bar when visited. This vulnerability affects Firefox < 117, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	6.5	Medium
CVE-2023-40416	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. Processing an image may result in disclosure of process memory.	2023-10-25	6.5	Medium
CVE-2023-41983	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.1, Safari 17.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Processing web content may lead to a denial-of-service.	2023-10-25	6.5	Medium
CVE-2023-42849	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An attacker that has already achieved kernel code execution may be able to bypass kernel memory mitigations.	2023-10-25	6.5	Medium
CVE-2023-42861	apple - macos	A logic issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1. An attacker with knowledge of a standard user's credentials can unlock another standard user's locked screen on the same Mac.	2023-10-25	6.5	Medium
CVE-2023-43510	arubanetworks - multiple products	A vulnerability in the ClearPass Policy Manager web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as a non-privileged user on the underlying operating system leading to partial system compromise.	2023-10-25	6.3	Medium
CVE-2023-3010	grafana - worldmap_panel	Grafana is an open-source platform for monitoring and observability. The WorldMap panel plugin, versions before 1.0.4 contains a DOM XSS vulnerability.	2023-10-25	6.1	Medium
CVE-2023-5758	mozilla - firefox	When opening a page in reader mode, the redirect URL could have caused attacker-controlled script to execute in a reflected Cross-Site Scripting (XSS) attack. This vulnerability affects Firefox for iOS < 119.	2023-10-25	6.1	Medium
CVE-2023-45802	apache - http_server	When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources were not reclaimed immediately. Instead, de-allocation was deferred to connection close. A client could send new requests and resets, keeping the connection busy and open and causing the memory footprint to keep on growing. On connection close, all resources were reclaimed, but the process might run out of memory before that.	2023-10-23	5.9	Medium

		This was found by the reporter during testing of CVE-2023-44487 (HTTP/2 Rapid Reset Exploit) with their own test client. During "normal" HTTP/2 use, the probability to hit this bug is very low. The kept memory would not become noticeable before the connection closes or times out. Users are recommended to upgrade to version 2.4.58, which fixes the issue.			
CVE-2023-43509	arubanetworks - multiple products	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an unauthenticated remote attacker to send notifications to computers that are running ClearPass OnGuard. These notifications can then be used to phish users or trick them into downloading malicious software.	2023-10-25	5.8	Medium
CVE-2023-40413	apple - multiple products	The issue was addressed with improved handling of caches. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to read sensitive location information.	2023-10-25	5.5	Medium
CVE-2023-40421	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to access sensitive user data.	2023-10-25	5.5	Medium
CVE-2023-40444	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sonoma 14.1. An app may be able to access user-sensitive data.	2023-10-25	5.5	Medium
CVE-2023-40449	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 17.1 and iPadOS 17.1, macOS Monterey 12.7.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to cause a denial-of-service.	2023-10-25	5.5	Medium
CVE-2023-41072	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data.	2023-10-25	5.5	Medium
CVE-2023-41077	apple - macos	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.6.1. An app may be able to access protected user data.	2023-10-25	5.5	Medium
CVE-2023-41254	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in iOS 17.1 and iPadOS 17.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, macOS Ventura 13.6.1, macOS Sonoma 14.1. An app may be able to access sensitive user data.	2023-10-25	5.5	Medium
CVE-2023-42842	apple - macos	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14.1. An app may be able to access sensitive user data.	2023-10-25	5.5	Medium
CVE-2023-42850	apple - macos	The issue was addressed with improved permissions logic. This issue is fixed in macOS Sonoma 14.1. An app may be able to access sensitive user data.	2023-10-25	5.5	Medium
CVE-2023-42854	apple - multiple products	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. An app may be able to cause a denial-of-service to Endpoint Security clients.	2023-10-25	5.5	Medium
CVE-2023-40121	google - multiple products	In appendEscapedSQLString of DatabaseUtils.java, there is a possible SQL injection due to unsafe deserialization. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	5.5	Medium
CVE-2023-40123	google - multiple products	In updateActionViews of PipMenuView.java, there is a possible bypass of a multi user security boundary due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	5.5	Medium
CVE-2023-40133	google - multiple products	In multiple locations of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	5.5	Medium
CVE-2023-43065	dell - multiple products	Dell Unity prior to 5.3 contains a Cross-site scripting vulnerability. A low-privileged authenticated attacker can exploit these issues to obtain escalated privileges.	2023-10-23	5.4	Medium
CVE-2023-38722	ibm - multiple products	IBM Sterling Partner Engagement Manager 6.1.2, 6.2.0, and 6.2.2 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 262174.	2023-10-23	5.4	Medium
CVE-2023-46650	jenkins - github	Jenkins GitHub Plugin 1.37.3 and earlier does not escape the GitHub project URL on the build page when showing changes, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	2023-10-25	5.4	Medium

CVE-2023-46659	jenkins - edgewall_trac	Jenkins Edgewall Trac Plugin 1.13 and earlier does not escape the Trac website URL on the build page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	2023-10-25	5.4	Medium
CVE-2023-46656	jenkins - multibranch_scan_ webhook_trigger	Jenkins Multibranch Scan Webhook Trigger Plugin 1.0.9 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	2023-10-25	5.3	Medium
CVE-2023-46657	jenkins - gogs	Jenkins Gogs Plugin 1.0.15 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	2023-10-25	5.3	Medium
CVE-2023-46658	jenkins - multiple products	Jenkins MSTeams Webhook Trigger Plugin 0.1.1 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	2023-10-25	5.3	Medium
CVE-2023-46660	jenkins - zanata	Jenkins Zanata Plugin 0.6 and earlier uses a non-constant time comparison function when checking whether the provided and expected webhook token hashes are equal, potentially allowing attackers to use statistical methods to obtain a valid webhook token.	2023-10-25	5.3	Medium
CVE-2023-5722	mozilla - firefox	Using iterative requests an attacker was able to learn the size of an opaque response, as well as the contents of a server-supplied Vary header. This vulnerability affects Firefox < 119.	2023-10-25	5.3	Medium
CVE-2023-5723	mozilla - firefox	An attacker with temporary script access to a site could have set a cookie containing invalid characters using `document.cookie` that could have led to unknown errors. This vulnerability affects Firefox < 119.	2023-10-25	5.3	Medium
CVE-2023-40408	apple - multiple products	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. Hide My Email may be deactivated unexpectedly.	2023-10-25	5.3	Medium
CVE-2023-42845	apple - multiple products	An authentication issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. Photos in the Hidden Photos Album may be viewed without authentication.	2023-10-25	5.3	Medium
CVE-2023-42846	apple - multiple products	This issue was addressed by removing the vulnerable code. This issue is fixed in watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, tvOS 17.1, iOS 17.1 and iPadOS 17.1. A device may be passively tracked by its Wi-Fi MAC address.	2023-10-25	5.3	Medium
CVE-2023-42031	ibm - multiple products	IBM TXSeries for Multiplatforms, 8.1, 8.2, and 9.1, CICS TX Standard CICS TX Advanced 10.1 and 11.1 could allow a privileged user to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 266016.	2023-10-25	4.9	Medium
CVE-2023-46118	vmware - multiple products	RabbitMQ is a multi-protocol messaging and streaming broker. HTTP API did not enforce an HTTP request body limit, making it vulnerable for denial of service (DoS) attacks with very large messages. An authenticated user with sufficient credentials can publish a very large messages over the HTTP API and cause target node to be terminated by an "out-of-memory killer"-like mechanism. This vulnerability has been patched in versions 3.11.24 and 3.12.7.	2023-10-25	4.9	Medium
CVE-2023-33840	ibm - multiple products	IBM Security Verify Governance 10.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 256037.	2023-10-23	4.8	Medium
CVE-2023-4693	gnu - grub2	An out-of-bounds read flaw was found on grub2's NTFS filesystem driver. This issue may allow a physically present attacker to present a specially crafted NTFS file system image to read arbitrary memory locations. A successful attack allows sensitive data cached in memory or EFI variable values to be leaked, presenting a high Confidentiality risk.	2023-10-25	4.6	Medium
CVE-2023-41982	apple - multiple products	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data.	2023-10-25	4.6	Medium
CVE-2023-41997	apple - multiple products	This issue was addressed by restricting options offered on a locked device. This issue is fixed in macOS Sonoma 14.1, watchOS 10.1, iOS 16.7.2 and iPadOS 16.7.2, iOS 17.1 and iPadOS 17.1. An attacker with physical access may be able to use Siri to access sensitive user data.	2023-10-25	4.6	Medium
CVE-2022-0353	lenovo - multiple products	A denial of service vulnerability was reported in the Lenovo HardwareScanPlugin versions prior to	2023-10-25	4.4	Medium

		1.3.1.2 and Lenovo Diagnostics versions prior to 4.45 that could allow a local user with administrative access to trigger a system crash.			
CVE-2022-3698	lenovo - multiple products	A denial of service vulnerability was reported in the Lenovo HardwareScanPlugin versions prior to 1.3.1.2 and Lenovo Diagnostics versions prior to 4.45 that could allow a local user with administrative access to trigger a system crash.	2023-10-25	4.4	Medium
CVE-2023-40425	apple - macos	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Monterey 12.7.1. An app with root privileges may be able to access private information.	2023-10-25	4.4	Medium
CVE-2023-46288	apache - airflow	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Airflow.This issue affects Apache Airflow from 2.4.0 to 2.7.0. Sensitive configuration information has been exposed to authenticated users with the ability to read configuration via Airflow REST API for configuration even when the expose_config option is set to non-sensitive-only. The expose_config option is False by default. It is recommended to upgrade to a version that is not affected if you set expose_config to non-sensitive-only configuration. This is a different error than CVE-2023-45348 which allows authenticated user to retrieve individual configuration values in 2.7.* by specially crafting their request (solved in 2.7.2). Users are recommended to upgrade to version 2.7.2, which fixes the issue and additionally fixes CVE-2023-45348.	2023-10-23	4.3	Medium
CVE-2023-34056	vmware - multiple products	vCenter Server contains a partial information disclosure vulnerability. A malicious actor with non-administrative privileges to vCenter Server may leverage this issue to access unauthorized data.	2023-10-25	4.3	Medium
CVE-2023-46652	jenkins - lambdatest-automation	A missing permission check in Jenkins lambdatest-automation Plugin 1.20.9 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of LAMBDATEST credentials stored in Jenkins.	2023-10-25	4.3	Medium
CVE-2023-5721	mozilla - multiple products	It was possible for certain browser prompts and dialogs to be activated or dismissed unintentionally by the user due to an insufficient activation-delay. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	4.3	Medium
CVE-2023-5725	mozilla - multiple products	A malicious installed WebExtension could open arbitrary URLs, which under the right circumstance could be leveraged to collect sensitive user data. This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	4.3	Medium
CVE-2023-5726	mozilla - multiple products	A website could have obscured the full screen notification by using the file open dialog. This could have led to user confusion and possible spoofing attacks. *Note: This issue only affected macOS operating systems. Other operating systems are unaffected.* This vulnerability affects Firefox < 119, Firefox ESR < 115.4, and Thunderbird < 115.4.1.	2023-10-25	4.3	Medium
CVE-2023-5729	mozilla - firefox	A malicious web site can enter fullscreen mode while simultaneously triggering a WebAuthn prompt. This could have obscured the fullscreen notification and could have been leveraged in a spoofing attack. This vulnerability affects Firefox < 119.	2023-10-25	4.3	Medium
CVE-2023-41975	apple - multiple products	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sonoma 14.1, macOS Monterey 12.7.1, macOS Ventura 13.6.1. A website may be able to access the microphone without the microphone use indicator being shown.	2023-10-25	4.3	Medium
CVE-2023-41977	apple - multiple products	The issue was addressed with improved handling of caches. This issue is fixed in macOS Sonoma 14.1, iOS 16.7.2 and iPadOS 16.7.2. Visiting a malicious website may reveal browsing history.	2023-10-25	4.3	Medium
CVE-2023-42438	apple - macos	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in macOS Sonoma 14.1. Visiting a malicious website may lead to user interface spoofing.	2023-10-25	4.3	Medium

CVE-2023-40405	apple - macos	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1. An app may be able to read sensitive location information.	2023-10-25	3.3	Low
CVE-2023-42857	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Sonoma 14.1, iOS 17.1 and iPadOS 17.1. An app may be able to access sensitive user data.	2023-10-25	3.3	Low
CVE-2023-40127	google - multiple products	In multiple locations, there is a possible way to access screenshots due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	3.3	Low
CVE-2023-40134	google - multiple products	In isFullScreen of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	3.3	Low
CVE-2023-40135	google - multiple products	In applyCustomDescription of SaveUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	3.3	Low
CVE-2023-40136	google - multiple products	In setHeader of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	3.3	Low
CVE-2023-40137	google - multiple products	In multiple functions of DialogFillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	3.3	Low
CVE-2023-40138	google - multiple products	In FillUi of FillUi.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-10-27	3.3	Low

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

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