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 ٢٤ سبتمبر إلى ٣٠ سبتمبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 24th of September to 30th of September. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-43135	tp-link - tl-er5120g_firmware	There is an unauthorized access vulnerability in TP-LINK ER5120G 4.0 2.0.0 Build 210817 Rel.80868n, which allows attackers to obtain sensitive information of the device without authentication, obtain user tokens, and ultimately log in to the device backend management.	2023-09-20	9.8	Critical
CVE-2023-41993	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in Safari 17, iOS 16.7 and iPadOS 16.7, macOS Sonoma 14. Processing web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 16.7.	2023-09-21	9.8	Critical
CVE-2023-23363	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect QNAP operating system. If exploited, the vulnerability possibly allows remote users to execute code via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 4.3.6.2441 build 20230621 and later QTS 4.3.3.2420 build 20230621 and later QTS 4.2.6 build 20230621 and later QTS 4.3.4.2451 build 20230621 and later	2023-09-22	9.8	Critical
CVE-2023-23364	qnap - multiple products	A buffer copy without checking size of input vulnerability has been reported to affect QNAP operating systems. If exploited, the vulnerability possibly allows remote users to execute code via unspecified vectors. We have already fixed the vulnerability in the following versions: Multimedia Console 2.1.1 (2023/03/29) and later Multimedia Console 1.4.7 (2023/03/20) and later	2023-09-22	9.8	Critical
CVE-2022-4039	redhat - single_sign-on	A flaw was found in Red Hat Single Sign-On for OpenShift container images, which are configured with an unsecured management interface enabled. This flaw allows an attacker to use this interface to deploy malicious code and access and modify potentially sensitive information in the app server configuration.	2023-09-22	9.8	Critical
CVE-2022-3874	redhat - multiple products	A command injection flaw was found in foreman. This flaw allows an authenticated user with admin privileges on the foreman instance to transpile commands through CoreOS and Fedora CoreOS configurations in templates, possibly resulting in arbitrary command execution on the underlying operating system.	2023-09-22	9.1	Critical
CVE-2023-22513	atlassian - multiple products	This High severity RCE (Remote Code Execution) vulnerability was introduced in version 8.0.0 of Bitbucket Data Center and Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.5, allows an authenticated attacker to execute arbitrary code which has high impact to confidentiality, high impact to integrity, high impact to availability, and requires no user interaction. Atlassian recommends that Bitbucket Data Center and Server customers upgrade to latest version, if you are unable to do so, upgrade your instance to one of the specified supported fixed versions: Bitbucket Data Center and Server 8.9: Upgrade to a	2023-09-19	8.8	High

		release greater than or equal to 8.9.5 Bitbucket Data Center and Server 8.10: Upgrade to a release greater than or equal to 8.10.5 Bitbucket Data Center and Server 8.11: Upgrade to a release greater than or equal to 8.11.4 Bitbucket Data Center and Server 8.12: Upgrade to a release greater than or equal to 8.12.2 Bitbucket Data Center and Server 8.13: Upgrade to a release greater than or equal to 8.13.1 Bitbucket Data Center and Server 8.14: Upgrade to a release greater than or equal to 8.14.0 Bitbucket Data Center and Server version >= 8.0 and < 8.9: Upgrade to any of the listed fix versions. See the release notes (https://confluence.atlassian.com/bitbucketserver/release-notes). You can download the latest version of Bitbucket Data Center and Server from the download center (https://www.atlassian.com/software/bitbucket/download-archives). This vulnerability was discovered by a private user and reported via our Bug Bounty program			
CVE-2023-40933	nagios - nagios_xi	A SQL injection vulnerability in Nagios XI v5.11.1 and below allows authenticated attackers with announcement banner configuration privileges to execute arbitrary SQL commands via the ID parameter sent to the update_banner_message() function.	2023-09-19	8.8	High
CVE-2023-2163	linux - multiple products	Incorrect verifier pruning in BPF in Linux Kernel >=5.4 leads to unsafe code paths being incorrectly marked as safe, resulting in arbitrary read/write in kernel memory, lateral privilege escalation, and container escape.	2023-09-20	8.8	High
CVE-2023-43496	jenkins - multiple products	Jenkins 2.423 and earlier, LTS 2.414.1 and earlier creates a temporary file in the system temporary directory with the default permissions for newly created files when installing a plugin from a URL, potentially allowing attackers with access to the system temporary directory to replace the file before it is installed in Jenkins, potentially resulting in arbitrary code execution.	2023-09-20	8.8	High
CVE-2023-43500	jenkins - build_failure_analyzer	A cross-site request forgery (CSRF) vulnerability in Jenkins Build Failure Analyzer Plugin 2.4.1 and earlier allows attackers to connect to an attacker-specified hostname and port using attacker-specified username and password.	2023-09-20	8.8	High
CVE-2023-43137	tp-link - tl-er5120g_firmware	TPLINK TL-ER5120G 4.0 2.0.0 Build 210817 Rel.80868n has a command injection vulnerability, when an attacker adds ACL rules after authentication, and the rule name parameter has injection points.	2023-09-20	8.8	High
CVE-2023-43138	tp-link - tl-er5120g_firmware	TPLINK TL-ER5120G 4.0 2.0.0 Build 210817 Rel.80868n has a command injection vulnerability, when an attacker adds NAPT rules after authentication, and the rule name has an injection point.	2023-09-20	8.8	High
CVE-2023-23362	qnap - multiple products	An OS command injection vulnerability has been reported to affect QNAP operating systems. If exploited, the vulnerability allows remote authenticated users to execute commands via susceptible QNAP devices. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2376 build 20230421 and later QTS 4.5.4.2374 build 20230416 and later QuTS hero h5.0.1.2376 build 20230421 and later QuTS hero h4.5.4.2374 build 20230417 and later QuTScloud c5.0.1.2374 and later	2023-09-22	8.8	High
CVE-2023-43497	jenkins - multiple products	In Jenkins 2.423 and earlier, LTS 2.414.1 and earlier, processing file uploads using the Stapler web framework creates temporary files in the default system temporary directory with the default permissions for newly created files, potentially allowing attackers with access to the Jenkins controller file system to read and write the files before they are used.	2023-09-20	8.1	High
CVE-2023-43498	jenkins - multiple products	In Jenkins 2.423 and earlier, LTS 2.414.1 and earlier, processing file uploads using MultipartFormDataParser creates temporary files in the default system temporary directory with the default permissions for newly created files, potentially allowing attackers with access to the Jenkins controller file system to read and write the files before they are used.	2023-09-20	8.1	High
CVE-2023-37410	ibm - multiple products	IBM Personal Communications 14.05, 14.06, and 15.0.0 could allow a local user to escalate their privileges to the SYSTEM user due to overly permissive access controls. IBM X-Force ID: 260138.	2023-09-20	7.8	High
CVE-2023-41992	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.7, macOS Ventura 13.6, iOS 16.7 and iPadOS 16.7. A local attacker may be able to elevate their privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 16.7.	2023-09-21	7.8	High
CVE-2022-3596	redhat - multiple products	An information leak was found in OpenStack's undercloud. This flaw allows unauthenticated, remote attackers to inspect sensitive data after discovering the IP address of the undercloud, possibly leading to compromising private information, including administrator access credentials.	2023-09-20	7.5	High

CVE-2023-42482	samsung - exynos_2200_firmware	Samsung Mobile Processor Exynos 2200 allows a GPU Use After Free.	2023-09-21	7.5	High
CVE-2023-38343	ivanti - multiple products	An XXE (XML external entity injection) vulnerability exists in the CSEP component of Ivanti Endpoint Manager before 2022 SU4. External entity references are enabled in the XML parser configuration. Exploitation of this vulnerability can lead to file disclosure or Server Side Request Forgery.	2023-09-21	7.5	High
CVE-2023-41929	samsung - memory_card_\&_ufd_authentication	A DLL hijacking vulnerability in Samsung Memory Card & UFD Authentication Utility PC Software before 1.0.1 could allow a local attacker to escalate privileges. (An attacker must already have user privileges on Windows to exploit this vulnerability.)	2023-09-18	7.3	High
CVE-2023-41179	trendmicro - multiple products	A vulnerability in the 3rd party AV uninstaller module contained in Trend Micro Apex One (on-prem and SaaS), Worry-Free Business Security and Worry-Free Business Security Services could allow an attacker to manipulate the module to execute arbitrary commands on an affected installation. Note that an attacker must first obtain administrative console access on the target system in order to exploit this vulnerability.	2023-09-19	7.2	High
CVE-2023-40934	nagios - nagios_xi	A SQL injection vulnerability in Nagios XI 5.11.1 and below allows authenticated attackers with privileges to manage host escalations in the Core Configuration Manager to execute arbitrary SQL commands via the host escalation notification settings.	2023-09-19	7.2	High
CVE-2022-3916	redhat - multiple products	A flaw was found in the offline_access scope in Keycloak. This issue would affect users of shared computers more (especially if cookies are not cleared), due to a lack of root session validation, and the reuse of session ids across root and user authentication sessions. This enables an attacker to resolve a user session attached to a previously authenticated user; when utilizing the refresh token, they will be issued a token for the original user.	2023-09-20	6.8	Medium
CVE-2023-4527	gnu - glibc	A flaw was found in glibc. When the getaddrinfo function is called with the AF_UNSPEC address family and the system is configured with no-aaaa mode via /etc/resolv.conf, a DNS response via TCP larger than 2048 bytes can potentially disclose stack contents through the function returned address data, and may cause a crash.	2023-09-18	6.5	Medium
CVE-2023-40931	nagios - nagios_xi	A SQL injection vulnerability in Nagios XI from version 5.11.0 up to and including 5.11.1 allows authenticated attackers to execute arbitrary SQL commands via the ID parameter in the POST request to /nagiosxi/admin/banner_message-ajaxhelper.php	2023-09-19	6.5	Medium
CVE-2023-43501	jenkins - build_failure_analyzer	A missing permission check in Jenkins Build Failure Analyzer Plugin 2.4.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified hostname and port using attacker-specified username and password.	2023-09-20	6.5	Medium
CVE-2023-38344	ivanti - multiple products	An issue was discovered in Ivanti Endpoint Manager before 2022 SU4. A file disclosure vulnerability exists in the GetFileContents SOAP action exposed via /landesk/managementsuite/core/core.secure/OsdScript.asmx. The application does not sufficiently restrict user-supplied paths, allowing for an authenticated attacker to read arbitrary files from a remote system, including the private key used to authenticate to agents for remote access.	2023-09-21	6.5	Medium
CVE-2023-41834	apache - flink_stateful_functions	Improper Neutralization of CRLF Sequences in HTTP Headers in Apache Flink Stateful Functions 3.1.0, 3.1.1 and 3.2.0 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via crafted HTTP requests. Attackers could potentially inject malicious content into the HTTP response that is sent to the user's browser. Users should upgrade to Apache Flink Stateful Functions version 3.3.0.	2023-09-19	6.1	Medium
CVE-2023-4806	gnu - glibc	A flaw was found in glibc. In an extremely rare situation, the getaddrinfo function may access memory that has been freed, resulting in an application crash. This issue is only exploitable when a NSS module implements only the _nss_*_gethostbyname2_r and _nss_*_getcanonname_r hooks without implementing the _nss_*_gethostbyname3_r hook. The resolved name should return a large number of IPv6 and IPv4, and the call to the getaddrinfo function should have the AF_INET6 address family with AI_CANONNAME, AI_ALL and AI_V4MAPPED as flags.	2023-09-18	5.9	Medium
CVE-2023-39252	dell - secure_connect_gateway_policy_manager	Dell SCG Policy Manager 5.16.00.14 contains a broken cryptographic algorithm vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by performing MitM attacks and let attackers obtain sensitive information.	2023-09-21	5.9	Medium

CVE-2023-22024	oracle - multiple products	In the Unbreakable Enterprise Kernel (UEK), the RDS module in UEK has two setsockopt(2) options, RDS_CONN_RESET and RDS6_CONN_RESET, that are not re-entrant. A malicious local user with CAP_NET_ADMIN can use this to crash the kernel. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	2023-09-20	5.5	Medium
CVE-2023-41991	apple - multiple products	A certificate validation issue was addressed. This issue is fixed in macOS Ventura 13.6, iOS 16.7 and iPadOS 16.7. A malicious app may be able to bypass signature validation. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 16.7.	2023-09-21	5.5	Medium
CVE-2023-23957	symantec - identity_portal	An authenticated user can see and modify the value for 'next' query parameter in Symantec Identity Portal 14.4	2023-09-19	5.4	Medium
CVE-2023-40932	nagios - nagios_xi	A Cross-site scripting (XSS) vulnerability in Nagios XI version 5.11.1 and below allows authenticated attackers with access to the custom logo component to inject arbitrary javascript or HTML via the alt-text field. This affects all pages containing the navbar including the login page which means the attacker is able to to steal plaintext credentials.	2023-09-19	5.4	Medium
CVE-2023-43495	jenkins - multiple products	Jenkins 2.423 and earlier, LTS 2.414.1 and earlier does not escape the value of the 'caption' constructor parameter of 'ExpandableDetailsNote', resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control this parameter.	2023-09-20	5.4	Medium
CVE-2023-43499	jenkins - build_failure_analyzer	Jenkins Build Failure Analyzer Plugin 2.4.1 and earlier does not escape Failure Cause names in build logs, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to create or update Failure Causes.	2023-09-20	5.4	Medium
CVE-2023-38718	ibm - multiple products	IBM Robotic Process Automation 21.0.0 through 21.0.7.8 could disclose sensitive information from access to RPA scripts, workflows and related data. IBM X-Force ID: 261606.	2023-09-20	5.3	Medium
CVE-2022-1438	redhat - keycloak	A flaw was found in Keycloak. Under specific circumstances, HTML entities are not sanitized during user impersonation, resulting in a Cross-site scripting (XSS) vulnerability.	2023-09-20	4.8	Medium
CVE-2023-40368	ibm - storage_protect	IBM Storage Protect 8.1.0.0 through 8.1.19.0 could allow a privileged user to obtain sensitive information from the administrative command line client. IBM X-Force ID: 263456.	2023-09-20	4.4	Medium
CVE-2023-43494	jenkins - multiple products	Jenkins 2.50 through 2.423 (both inclusive), LTS 2.60.1 through 2.414.1 (both inclusive) does not exclude sensitive build variables (e.g., password parameter values) from the search in the build history widget, allowing attackers with Item/Read permission to obtain values of sensitive variables used in builds by iteratively testing different characters until the correct sequence is discovered.	2023-09-20	4.3	Medium
CVE-2023-43502	jenkins - build_failure_analyzer	A cross-site request forgery (CSRF) vulnerability in Jenkins Build Failure Analyzer Plugin 2.4.1 and earlier allows attackers to delete Failure Causes.	2023-09-20	4.3	Medium
CVE-2020-36766	linux - linux_kernel	An issue was discovered in the Linux kernel before 5.8.6. drivers/media/cec/core/cec-api.c leaks one byte of kernel memory on specific hardware to unprivileged users, because of directly assigning log_addrs with a hole in the struct.	2023-09-18	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.