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 ١٩ نوفمبر إلى ٢٥ نوفمبر. 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 19th of November to 25th of November. 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-2022-46337	apache - derby	A cleverly devised username might bypass LDAP authentication checks. In LDAP-authenticated Derby installations, this could let an attacker fill up the disk by creating junk Derby databases. In LDAP-authenticated Derby installations, this could also allow the attacker to execute malware which was visible to and executable by the account which booted the Derby server. In LDAP-protected databases which weren't also protected by SQL GRANT/REVOKE authorization, this vulnerability could also let an attacker view and corrupt sensitive data and run sensitive database functions and procedures. Mitigation: Users should upgrade to Java 21 and Derby 10.17.1.0. Alternatively, users who wish to remain on older Java versions should build their own Derby distribution from one of the release families to which the fix was backported: 10.16, 10.15, and 10.14. Those are the releases which correspond, respectively, with Java LTS versions 17, 11, and 8.	2023-11-20	9.8	Critical
CVE-2023-46302	apache - submarine	Apache Software Foundation Apache Submarine has a bug when serializing against yaml. The bug is caused by snakeyaml https://nvd.nist.gov/vuln/detail/CVE-2022-1471 . Apache Submarine uses JAXRS to define REST endpoints. In order to handle YAML requests (using application/yaml content-type), it defines a YamlEntityProvider entity provider that will process all incoming YAML requests. In order to unmarshal the request, the readFrom method is invoked, passing the entityStream containing the user-supplied data in `submarine-server/server-core/src/main/java/org/apache/submarine/server/utils/YamlUtils.java`. We have now fixed this issue in the new version by replacing to `jackson-dataformat-yaml`. This issue affects Apache Submarine: from 0.7.0 before 0.8.0. Users are recommended to upgrade to version 0.8.0, which	2023-11-20	9.8	Critical

		fixes this issue. If using the version smaller than 0.8.0 and not want to upgrade, you can try cherry-pick PR https://github.com/apache/submarine/pull/1054 and rebuild the submart-server image to fix this.			
CVE-2023-49060	mozilla - firefox	An attacker could have accessed internal pages or data by ex-filtrating a security key from ReaderMode via the `referrerpolicy` attribute. This vulnerability affects Firefox for iOS < 120.	2023-11-21	9.8	Critical
CVE-2023-37924	apache - submarine	Apache Software Foundation Apache Submarine has an SQL injection vulnerability when a user logs in. This issue can result in unauthorized login. Now we have fixed this issue and now user must have the correct login to access workbench. This issue affects Apache Submarine: from 0.7.0 before 0.8.0. We recommend that all submarine users with 0.7.0 upgrade to 0.8.0, which not only fixes the issue, supports the oidc authentication mode, but also removes the case of unauthenticated logins. If using the version lower than 0.8.0 and not want to upgrade, you can try cherry-pick PR https://github.com/apache/submarine/pull/1037 https://github.com/apache/submarine/pull/1054 and rebuild the submarine-server image to fix this.	2023-11-22	9.8	Critical
CVE-2023-28812	hikvision - localservicecomponents	There is a buffer overflow vulnerability in a web browser plug-in could allow an attacker to exploit the vulnerability by sending crafted messages to computers installed with this plug-in, which could lead to arbitrary code execution or cause process exception of the plug-in.	2023-11-23	9.8	Critical
CVE-2023-6207	mozilla - multiple products	Ownership mismanagement led to a use-after-free in ReadableByteStreams This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5.	2023-11-21	8.8	High
CVE-2023-6208	mozilla - multiple products	When using X11, text selected by the page using the Selection API was erroneously copied into the primary selection, a temporary storage not unlike the clipboard. *This bug only affects Firefox on X11. Other systems are unaffected.* This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5.	2023-11-21	8.8	High
CVE-2023-6212	mozilla - multiple products	Memory safety bugs present in Firefox 119, Firefox ESR 115.4, and Thunderbird 115.4. 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 < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5.	2023-11-21	8.8	High
CVE-2023-6213	mozilla - firefox	Memory safety bugs present in Firefox 119. 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 < 120.	2023-11-21	8.8	High
CVE-2023-22516	atlassian - multiple products	This High severity RCE (Remote Code Execution) vulnerability was introduced in versions 8.1.0, 8.2.0, 9.0.0, 9.1.0, 9.2.0, and 9.3.0 of Bamboo 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 Bamboo 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: Bamboo Data Center and Server 9.2: Upgrade to a release greater than or equal to 9.2.7. JDK 1.8u121+ should be used in case Java 8 used to run Bamboo Data Center and Server. See Bamboo 9.2 Upgrade notes (https://confluence.atlassian.com/bambooreleases/bamboo-9-2-upgrade-notes-1207179212.html) Bamboo Data Center and Server 9.3: Upgrade to a release greater than or equal to 9.3.4 See the release notes	2023-11-21	8.8	High

		([https://confluence.atlassian.com/bambooreleases/bamboo-release-notes-1189793869.html]). You can download the latest version of Bamboo Data Center and Server from the download center ([https://www.atlassian.com/software/bamboo/download-archives]). This vulnerability was discovered by a private user and reported via our Bug Bounty program			
CVE-2023-22521	atlassian - multiple products	This High severity RCE (Remote Code Execution) vulnerability was introduced in version 3.4.6 of Crowd Data Center and Server. This RCE (Remote Code Execution) vulnerability, with a CVSS Score of 8.0, 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 Crowd 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: Crowd Data Center and Server 3.4: Upgrade to a release greater than or equal to 5.1.6 Crowd Data Center and Server 5.2: Upgrade to a release greater than or equal to 5.2.1 See the release notes ([https://confluence.atlassian.com/crowd/crowd-release-notes-199094.html]). You can download the latest version of Crowd Data Center and Server from the download center ([https://www.atlassian.com/software/crowd/download-archive]). This vulnerability was discovered by m1sn0w and reported via our Bug Bounty program	2023-11-21	8.8	High
CVE-2023-20272	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Identity Services Engine could allow an authenticated, remote attacker to upload malicious files to the web root of the application. This vulnerability is due to insufficient file input validation. An attacker could exploit this vulnerability by uploading a malicious file to the web interface. A successful exploit could allow the attacker to replace files and gain access to sensitive server-side information.	2023-11-21	8.8	High
CVE-2022-35638	ibm - multiple products	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 230824.	2023-11-22	8.8	High
CVE-2023-6265	draytek - multiple products	Draytek Vigor2960 v1.5.1.4 and v1.5.1.5 are vulnerable to directory traversal via the mainfunction.cgi dumpSyslog 'option' parameter allowing an authenticated attacker with access to the web management interface to delete arbitrary files. Vigor2960 is no longer supported.	2023-11-22	8.1	High
CVE-2023-5593	zyxel - secuextender_ssl_vpn	The out-of-bounds write vulnerability in the Windows-based SecuExtender SSL VPN Client software version 4.0.4.0 could allow an authenticated local user to gain a privilege escalation by sending a crafted CREATE message.	2023-11-20	7.8	High
CVE-2021-38405	siemens - multiple products	The Datalogics APDFL library used in affected products is vulnerable to memory corruption condition while parsing specially crafted PDF files. An attacker could leverage this vulnerability to execute code in the context of the current process.	2023-11-21	7.8	High
CVE-2023-20274	cisco - multiple products	A vulnerability in the installer script of Cisco AppDynamics PHP Agent could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient permissions that are set by the PHP Agent Installer on the PHP Agent install directory. An attacker could exploit this vulnerability by modifying objects in the PHP Agent install directory, which would run with the same	2023-11-21	7.8	High

		privileges as PHP. A successful exploit could allow a lower-privileged attacker to elevate their privileges to root on an affected device.			
CVE-2023-6238	linux - linux_kernel	A buffer overflow vulnerability was found in the NVM Express (NVMe) driver in the Linux kernel. An unprivileged user could specify a small meta buffer and let the device perform larger Direct Memory Access (DMA) into the same buffer, overwriting unrelated kernel memory, causing random kernel crashes and memory corruption.	2023-11-21	7.8	High
CVE-2023-39253	dell - multiple products	Dell OS Recovery Tool, versions 2.2.4013, 2.3.7012.0, and 2.3.7515.0 contain an Improper Access Control Vulnerability. A local authenticated non-administrator user could potentially exploit this vulnerability, leading to the elevation of privilege on the system.	2023-11-23	7.8	High
CVE-2023-43086	dell - command|configure	Dell Command | Configure, versions prior to 4.11.0, contains an improper access control vulnerability. A local malicious user could potentially modify files inside installation folder during application upgrade, leading to privilege escalation.	2023-11-23	7.8	High
CVE-2023-44289	dell - command|configure	Dell Command | Configure versions prior to 4.11.0, contain an improper access control vulnerability. A local malicious standard user could potentially exploit this vulnerability while repairing/changing installation, leading to privilege escalation.	2023-11-23	7.8	High
CVE-2023-44290	dell - command|monitor	Dell Command | Monitor versions prior to 10.10.0, contain an improper access control vulnerability. A local malicious standard user could potentially exploit this vulnerability while repairing/changing installation, leading to privilege escalation.	2023-11-23	7.8	High
CVE-2023-5972	linux - multiple products	A null pointer dereference flaw was found in the nft_inner.c functionality of netfilter in the Linux kernel. This issue could allow a local user to crash the system or escalate their privileges on the system.	2023-11-23	7.8	High
CVE-2023-26279	ibm - qradar_wincollect	IBM QRadar WinCollect Agent 10.0 through 10.1.7 could allow a local user to perform unauthorized actions due to improper encoding. IBM X-Force ID: 248160.	2023-11-24	7.8	High
CVE-2023-45886	f5 - big-ip_next	The BGP daemon (bgpd) in IP Infusion ZebOS through 7.10.6 allow remote attackers to cause a denial of service by sending crafted BGP update messages containing a malformed attribute.	2023-11-21	7.5	High
CVE-2023-28813	hikvision - localservicecomponents	An attacker could exploit a vulnerability by sending crafted messages to computers installed with this plug-in to modify plug-in parameters, which could cause affected computers to download malicious files.	2023-11-23	7.5	High

CVE-2023-48796	apache - dolphinscheduler	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache DolphinScheduler.
		
		The information exposed to unauthorized actors may include sensitive data such as database credentials.
		
		Users who can't upgrade to the fixed version can also set environment variable `MANAGEMENT_ENDPOINTS_WEB_EXPOSURE_INCLUDE=health,metrics,prometheus` to workaround this, or add the following section in the `application.yaml` file
		
		``
		management:
		  endpoints:
		  web:
		  exposure:
		  include: health,metrics,prometheus
		``
		
		This issue affects Apache DolphinScheduler: from 3.0.0 before 3.0.2.
		
		Users are recommended to upgrade to version 3.0.2, which fixes the issue.
			2023-11-24	7.5	High

CVE-2023-48646	zohocorp - multiple products	Zoho ManageEngine RecoveryManager Plus before 6070 allows admin users to execute arbitrary commands via proxy settings.	2023-11-22	7.2	High
CVE-2023-36013	microsoft - multiple products	PowerShell Information Disclosure Vulnerability	2023-11-20	6.5	Medium
CVE-2023-6204	mozilla - multiple products	On some systems—depending on the graphics settings and drivers—it was possible to force an out-of-bounds read and leak memory data into the images created on the canvas element. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5.	2023-11-21	6.5	Medium

CVE-2023-6205	mozilla - multiple products	It was possible to cause the use of a MessagePort after it had already been freed, which could potentially have led to an exploitable crash. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5.	2023-11-21	6.5	Medium
CVE-2023-6209	mozilla - multiple products	Relative URLs starting with three slashes were incorrectly parsed, and a path-traversal "/../" part in the path could be used to override the specified host. This could contribute to security problems in web sites. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5.	2023-11-21	6.5	Medium
CVE-2023-6210	mozilla - firefox	When an https: web page created a pop-up from a "javascript:" URL, that pop-up was incorrectly allowed to load blockable content such as iframes from insecure http: URLs This vulnerability affects Firefox < 120.	2023-11-21	6.5	Medium
CVE-2023-6211	mozilla - firefox	If an attacker needed a user to load an insecure http: page and knew that user had enabled HTTPS-only mode, the attacker could have tricked the user into clicking to grant an HTTPS-only exception if they could get the user to participate in a clicking game. This vulnerability affects Firefox < 120.	2023-11-21	6.5	Medium
CVE-2022-36777	ibm - multiple products	IBM Cloud Pak for Security (CP4S) 1.10.0.0 through 1.10.11.0 and IBM QRadar Suite Software 1.10.12.0 through 1.10.16.0could allow an authenticated user to obtain sensitive version information that could aid in further attacks against the system. IBM X-Force ID: 233665.	2023-11-22	6.5	Medium
CVE-2023-49061	mozilla - firefox	An attacker could have performed HTML template injection via Reader Mode and exfiltrated user information. This vulnerability affects Firefox for iOS < 120.	2023-11-21	6.1	Medium
CVE-2023-43082	dell - multiple products	Dell Unity prior to 5.3 contains a 'man in the middle' vulnerability in the vmadapter component. If a customer has a certificate signed by a third-party public Certificate Authority, the vCenter CA could be spoofed by an attacker who can obtain a CA-signed certificate.	2023-11-22	5.9	Medium
CVE-2023-20240	cisco - multiple products	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system.	2023-11-22	5.5	Medium
CVE-2023-20241	cisco - multiple products	Multiple vulnerabilities in Cisco Secure Client Software, formerly AnyConnect Secure Mobility Client, could allow an authenticated, local attacker to cause a denial of service (DoS) condition on an affected system. These vulnerabilities are due to an out-of-bounds memory read from Cisco Secure Client Software. An attacker could exploit these vulnerabilities by logging in to an affected device at the same time that another user is accessing Cisco Secure Client on the same system, and then sending crafted packets to a port on that local host. A successful exploit could allow the attacker to crash the VPN Agent service, causing it to be unavailable to all users of the system. To exploit these vulnerabilities, the attacker must have valid credentials on a multi-user system.	2023-11-22	5.5	Medium
CVE-2023-25682	ibm - multiple products	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.0.3.8 and 6.1.0.0 through 6.1.2.1 stores potentially sensitive information in log files that could be read by a local user. IBM X-Force ID: 247034.	2023-11-22	5.5	Medium
CVE-2023-43123	apache - storm	On unix-like systems, the temporary directory is shared between all user. As such, writing to this directory using APIs that do not explicitly set the file/directory permissions can lead to information disclosure. Of note, this does not impact modern MacOS Operating Systems. The method File.createTempFile on unix-like systems creates a file with predefined name (so easily identifiable) and by default will create this file with the permissions -rw-r--r--. Thus, if sensitive information is written to this file, other local users can read this information. File.createTempFile(String, String) will create a temporary file in the system temporary directory if the 'java.io.tmpdir' system property is not explicitly set.	2023-11-23	5.5	Medium

		This affects the class https://github.com/apache/storm/blob/master/storm-core/src/jvm/org/apache/storm/utils/TopologySpoutLag.java#L99 and was introduced by https://issues.apache.org/jira/browse/STORM-3123 In practice, this has a very limited impact as this class is used only if ui.disable.spout.lag.monitoring is set to false, but its value is true by default. Moreover, the temporary file gets deleted soon after its creation. The solution is to use Files.createTempFile https://docs.oracle.com/en/java/javase/11/docs/api/java.base/java/nio/file/Files.html#createTempFile(java.lang.String,java.lang.String,java.nio.file.attribute.FileAttribute...) instead. We recommend that all users upgrade to the latest version of Apache Storm.			
CVE-2023-6206	mozilla - multiple products	The black fade animation when exiting fullscreen is roughly the length of the anti-clickjacking delay on permission prompts. It was possible to use this fact to surprise users by luring them to click where the permission grant button would be about to appear. This vulnerability affects Firefox < 120, Firefox ESR < 115.5.0, and Thunderbird < 115.5.	2023-11-21	5.4	Medium
CVE-2023-20265	cisco - ip_dect_110_firmware	A vulnerability in the web-based management interface of a small subset of Cisco IP Phones could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to view a page containing malicious HTML or script content. 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. To exploit this vulnerability, the attacker must have valid credentials to access the web-based management interface of the affected device.	2023-11-21	5.4	Medium
CVE-2021-39008	ibm - qradar_wincollect	IBM QRadar WinCollect Agent 10.0 through 10.1.7 could allow a privileged user to obtain sensitive information due to missing best practices. IBM X-Force ID: 213551.	2023-11-23	4.9	Medium
CVE-2023-20208	cisco - multiple products	A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to conduct an XSS attack against a user of the web-based management interface of an affected device.	2023-11-21	4.8	Medium
CVE-2023-20084	cisco - multiple products	A vulnerability in the endpoint software of Cisco Secure Endpoint for Windows could allow an authenticated, local attacker to evade endpoint protection within a limited time window. This vulnerability is due to a timing issue that occurs between various software components. An attacker could exploit this vulnerability by persuading a user to put a malicious file into a specific folder and then persuading the user to execute the file within a limited time window. A successful exploit could allow the attacker to cause the endpoint software to fail to quarantine the malicious file or kill its process. Note: This vulnerability only applies to deployments that have the Windows Folder Redirection feature enabled.	2023-11-22	4.4	Medium
CVE-2023-43081	dell - powerprotect_agent_for_file_system	PowerProtect Agent for File System Version 19.14 and prior, contains an incorrect default permissions vulnerability in ddfscon component. A low Privileged local attacker could potentially exploit this vulnerability, leading to overwriting of log files.	2023-11-22	3.3	Low