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 ١١ يونيو إلى ١٧ يونيو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- عالي جدًا: النتيجة الأساسية لـ CVSS 9.0-10.0
- عالي: النتيجة الأساسية لـ CVSS 7.0-8.9
- متوسط: النتيجة الأساسية لـ CVSS 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 11th of June to 17th of June. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-26295	hp - multiple products	Previous versions of HP Device Manager (prior to HPDM 5.0.10) could potentially allow command injection and/or elevation of privileges.	2023-06-12	9.8	Critical
CVE-2023-32673	hp - multiple products	Certain versions of HP PC Hardware Diagnostics Windows, HP Image Assistant, and HP Thunderbolt Dock G2 Firmware are potentially vulnerable to elevation of privilege.	2023-06-12	9.8	Critical
CVE-2023-32674	hp - pc_hardware_diagnostics	Certain versions of HP PC Hardware Diagnostics Windows are potentially vulnerable to buffer overflow.	2023-06-12	9.8	Critical
CVE-2023-26204	fortinet - multiple products	A plaintext storage of a password vulnerability [CWE-256] in FortiSIEM 6.7 all versions, 6.6 all versions, 6.5 all versions, 6.4 all versions, 6.3 all versions, 6.2 all versions, 6.1 all versions, 5.4 all versions, 5.3 all versions may allow an attacker able to access user DB content to impersonate any admin user on the device GUI.	2023-06-13	9.8	Critical
CVE-2023-27997	fortinet - multiple products	A heap-based buffer overflow vulnerability [CWE-122] in FortiOS version 7.2.4 and below, version 7.0.11 and below, version 6.4.12 and below, version 6.0.16 and below and FortiProxy version 7.2.3 and below, version 7.0.9 and below, version 2.0.12 and below, version 1.2 all versions, version 1.1 all versions SSL-VPN may allow a remote attacker to execute arbitrary code or commands via specifically crafted requests.	2023-06-13	9.8	Critical
CVE-2023-27837	tp-link - tl-wpa8630p_firmware	TP-Link TL-WPA8630P (US)_ V2_ Version 171011 was discovered to contain a command injection vulnerability via the key parameter in the function sub_ 40A774.	2023-06-13	9.8	Critical
CVE-2023-27836	tp-link - tl-wpa8630p_firmware	TP-Link TL-WPA8630P (US)_ V2_ Version 171011 was discovered to contain a command injection vulnerability via the devicePwd parameter in the function sub_ 40A80C.	2023-06-13	9.8	Critical
CVE-2023-29562	tp-link - tl-wpa7510_firmware	TP-Link TL-WPA7510 (EU)_V2_190125 was discovered to contain a stack overflow via the operation parameter at /admin/locale.	2023-06-13	9.8	Critical
CVE-2023-29357	microsoft - sharepoint_server	Microsoft SharePoint Server Elevation of Privilege Vulnerability	2023-06-14	9.8	Critical
CVE-2023-29363	microsoft - multiple products	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	2023-06-14	9.8	Critical
CVE-2023-32014	microsoft - multiple products	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	2023-06-14	9.8	Critical
CVE-2023-32015	microsoft - multiple products	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	2023-06-14	9.8	Critical
CVE-2021-0701	google - android	Product: AndroidVersions: Android SoCAndroid ID: A-277775870	2023-06-15	9.8	Critical
CVE-2021-0945	google - android	Product: AndroidVersions: Android SoCAndroid ID: A-278156680	2023-06-15	9.8	Critical
CVE-2023-21130	google - android	In btm_ble_periodic_adv_sync_lost of btm_ble_gap.cc, there is a possible remote code execution due to a buffer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-273502002	2023-06-15	9.8	Critical
CVE-2023-34832	tp-link - archer_ax10_firmware	TP-Link Archer AX10(EU)_V1.2_230220 was discovered to contain a buffer overflow via the function FUN_131e8 - 0x132B4.	2023-06-16	9.8	Critical

CVE-2023-24470	microfocus - arcsight_logger	Potential XML External Entity Injection in ArcSight Logger versions prior to 7.3.0.	2023-06-13	9.1	Critical
CVE-2023-34468	apache - nifi	The DBCPConnectionPool and HikariCPConnectionPool Controller Services in Apache NiFi 0.0.2 through 1.21.0 allow an authenticated and authorized user to configure a Database URL with the H2 driver that enables custom code execution. The resolution validates the Database URL and rejects H2 JDBC locations. You are recommended to upgrade to version 1.22.0 or later which fixes this issue.	2023-06-12	8.8	High
CVE-2023-28478	tp-link - ec70_firmware	TP-Link EC-70 devices through 2.3.4 Build 20220902 rel.69498 have a Buffer Overflow.	2023-06-12	8.8	High
CVE-2023-26296	hp - multiple products	Previous versions of HP Device Manager (prior to HPDM 5.0.10) could potentially allow command injection and/or elevation of privileges.	2023-06-12	8.8	High
CVE-2023-26297	hp - multiple products	Previous versions of HP Device Manager (prior to HPDM 5.0.10) could potentially allow command injection and/or elevation of privileges.	2023-06-12	8.8	High
CVE-2023-26298	hp - multiple products	Previous versions of HP Device Manager (prior to HPDM 5.0.10) could potentially allow command injection and/or elevation of privileges.	2023-06-12	8.8	High
CVE-2022-42478	fortinet - multiple products	An Improper Restriction of Excessive Authentication Attempts [CWE-307] in FortiSIEM below 7.0.0 may allow a non-privileged user with access to several endpoints to brute force attack these endpoints.	2023-06-13	8.8	High
CVE-2023-34113	zoom - zoom	Insufficient verification of data authenticity in Zoom for Windows clients before 5.14.0 may allow an authenticated user to potentially enable an escalation of privilege via network access.	2023-06-13	8.8	High
CVE-2023-34121	zoom - multiple products	Improper input validation in the Zoom for Windows, Zoom Rooms, Zoom VDI Windows Meeting clients before 5.14.0 may allow an authenticated user to potentially enable an escalation of privilege via network access.	2023-06-13	8.8	High
CVE-2023-3214	google - chrome	Use after free in Autofill payments in Google Chrome prior to 114.0.5735.133 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2023-06-13	8.8	High
CVE-2023-3215	google - chrome	Use after free in WebRTC in Google Chrome prior to 114.0.5735.133 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-06-13	8.8	High
CVE-2023-3216	google - chrome	Type confusion in V8 in Google Chrome prior to 114.0.5735.133 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-06-13	8.8	High
CVE-2023-3217	google - chrome	Use after free in WebXR in Google Chrome prior to 114.0.5735.133 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-06-13	8.8	High
CVE-2023-29362	microsoft - multiple products	Remote Desktop Client Remote Code Execution Vulnerability	2023-06-14	8.8	High
CVE-2023-29372	microsoft - multiple products	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	2023-06-14	8.8	High
CVE-2023-29373	microsoft - multiple products	Microsoft ODBC Driver Remote Code Execution Vulnerability	2023-06-14	8.8	High
CVE-2023-32009	microsoft - multiple products	Windows Collaborative Translation Framework Elevation of Privilege Vulnerability	2023-06-14	8.8	High
CVE-2023-33131	microsoft - multiple products	Microsoft Outlook Remote Code Execution Vulnerability	2023-06-14	8.8	High
CVE-2023-32031	microsoft - multiple products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-06-14	8.8	High
CVE-2022-32752	ibm - security_directory_suite_va	IBM Security Directory Suite VA 8.0.1 through 8.0.1.19 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 228439.	2023-06-15	8.8	High
CVE-2023-35030	liferay - multiple products	Cross-site request forgery (CSRF) vulnerability in the Layout module's SEO configuration in Liferay Portal 7.4.3.70 through 7.4.3.76, and Liferay DXP 7.4 update 70 through 76 allows remote attackers to execute arbitrary code in the scripting console via the `_com_liferay_layout_admin_web_portlet_GroupPagesPortlet_backURL` parameter.	2023-06-15	8.8	High
CVE-2023-21108	google - multiple products	In sdpu_build_uuid_seq of sdp_discovery.cc, there is a possible out of bounds write due to a use after free. This could lead to remote code execution over Bluetooth, if HFP support is enabled, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-239414876	2023-06-15	8.8	High
CVE-2023-21115	google - multiple products	In btm_sec_encrypt_change of btm_sec.cc, there is a possible way to downgrade the link key type due to improperly used crypto.	2023-06-15	8.8	High

		This could lead to paired device escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-258834033			
CVE-2023-21127	google - multiple products	In readSampleData of NuMediaExtractor.cpp, there is a possible out of bounds write due to uninitialized data. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-275418191	2023-06-15	8.8	High
CVE-2023-32022	microsoft - multiple products	 Windows Server Service Security Feature Bypass Vulnerability 	2023-06-14	8.6	High
CVE-2023-33991	sap - multiple products	SAP UI5 Variant Management - versions SAP_UI 750, SAP_UI 754, SAP_UI 755, SAP_UI 756, SAP_UI 757, UI_700 200, does not sufficiently encode user-controlled inputs on reading data from the server, resulting in Stored Cross-Site Scripting (Stored XSS) vulnerability. After successful exploitation, an attacker with user level access can cause high impact on confidentiality, modify some information and can cause unavailability of the application at user level.	2023-06-13	8.2	High
CVE-2023-0142	synology - multiple products	Uncontrolled search path element vulnerability in Backup Management Functionality in Synology DiskStation Manager (DSM) before 7.1-42661 allows remote authenticated users to read or write arbitrary files via unspecified vectors.	2023-06-13	8.1	High
CVE-2023-29351	microsoft - multiple products	Windows Group Policy Elevation of Privilege Vulnerability	2023-06-14	8.1	High
CVE-2023-35142	jenkins - checkmarx	Jenkins Checkmarx Plugin 2022.4.3 and earlier disables SSL/TLS validation for connections to the Checkmarx server by default.	2023-06-14	8.1	High
CVE-2022-33163	ibm - security_directory_suite_va	IBM Security Directory Suite VA 8.0.1 specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors. IBM X-Force ID: 228571.	2023-06-15	8.1	High
CVE-2023-35141	jenkins - multiple products	In Jenkins 2.399 and earlier, LTS 2.387.3 and earlier, POST requests are sent in order to load the list of context actions. If part of the URL includes insufficiently escaped user-provided values, a victim may be tricked into sending a POST request to an unexpected endpoint by opening a context menu.	2023-06-14	8	High
CVE-2023-28310	microsoft - multiple products	Microsoft Exchange Server Remote Code Execution Vulnerability	2023-06-14	8	High
CVE-2023-26294	hp - multiple products	Previous versions of HP Device Manager (prior to HPDM 5.0.10) could potentially allow command injection and/or elevation of privileges.	2023-06-12	7.8	High
CVE-2022-43953	fortinet - multiple products	A use of externally-controlled format string in Fortinet FortiOS version 7.2.0 through 7.2.4, FortiOS all versions 7.0, FortiOS all versions 6.4, FortiOS all versions 6.2, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7 allows attacker to execute unauthorized code or commands via specially crafted commands.	2023-06-13	7.8	High
CVE-2023-22639	fortinet - multiple products	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.12, FortiOS all versions 6.2, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.2, FortiProxy version 7.0.0 through 7.0.8, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows attacker to escalation of privilege via specifically crafted commands.	2023-06-13	7.8	High
CVE-2023-26210	fortinet - multiple products	Multiple improper neutralization of special elements used in an os command ('OS Command Injection') vulnerabilties [CWE-78] in Fortinet FortiADCManager version 7.1.0 and before 7.0.0, FortiADC version 7.2.0 and before 7.1.2 allows a local authenticated attacker to execute arbitrary shell code as `root` user via crafted CLI requests.	2023-06-13	7.8	High
CVE-2023-28000	fortinet - multiple products	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in FortiADC CLI 7.1.0, 7.0.0 through 7.0.3, 6.2.0 through 6.2.4, 6.1 all versions, 6.0 all versions may allow a local and authenticated attacker to execute unauthorized commands via specifically crafted arguments in diagnose system df CLI command.	2023-06-13	7.8	High
CVE-2023-34120	zoom - virtual_desktop_infrastructure	Improper privilege management in Zoom for Windows, Zoom Rooms for Windows, and Zoom VDI for Windows clients before 5.14.0 may allow an authenticated user to potentially enable an escalation of privilege via local access. Users may potentially utilize higher level system privileges maintained by the Zoom client to spawn processes with escalated privileges.	2023-06-13	7.8	High
CVE-2023-34122	zoom - zoom	Improper input validation in the installer for Zoom for Windows clients before 5.14.0 may allow an authenticated user to potentially enable an escalation of privilege via local access.	2023-06-13	7.8	High

CVE-2023-29346	microsoft - multiple products	NTFS Elevation of Privilege Vulnerability	2023-06-14	7.8	High
CVE-2023-29358	microsoft - multiple products	Windows GDI Elevation of Privilege Vulnerability	2023-06-14	7.8	High
CVE-2023-29359	microsoft - multiple products	GDI Elevation of Privilege Vulnerability	2023-06-14	7.8	High
CVE-2023-29360	microsoft - multiple products	Windows TPM Device Driver Elevation of Privilege Vulnerability	2023-06-14	7.8	High
CVE-2023-29365	microsoft - multiple products	Windows Media Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-29366	microsoft - multiple products	Windows Geolocation Service Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-29367	microsoft - multiple products	iSCSI Target WMI Provider Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-29370	microsoft - multiple products	Windows Media Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-29371	microsoft - multiple products	Windows GDI Elevation of Privilege Vulnerability	2023-06-14	7.8	High
CVE-2023-32008	microsoft - multiple products	Windows Resilient File System (ReFS) Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-32012	microsoft - multiple products	Windows Container Manager Service Elevation of Privilege Vulnerability	2023-06-14	7.8	High
CVE-2023-32017	microsoft - multiple products	Microsoft PostScript Printer Driver Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-32018	microsoft - multiple products	Windows Hello Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-32029	microsoft - multiple products	Microsoft Excel Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-33133	microsoft - multiple products	Microsoft Excel Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-33137	microsoft - multiple products	Microsoft Excel Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-33146	microsoft - multiple products	Microsoft Office Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-1049	schneider-electric - multiple products	A CWE-94: Improper Control of Generation of Code ('Code Injection') vulnerability exists that could cause execution of malicious code when an unsuspicious user loads a project file from the local filesystem into the HMI.	2023-06-14	7.8	High
CVE-2023-2569	schneider-electric - ecostruxure_foxboro_dcs_control_core_services	A CWE-787: Out-of-Bounds Write vulnerability exists that could cause local denial-of-service, elevation of privilege, and potentially kernel execution when a malicious actor with local user access crafts a script/program using an IOCTL call in the Foxboro.sys driver.	2023-06-14	7.8	High
CVE-2023-2570	schneider-electric - ecostruxure_foxboro_dcs_control_core_services	A CWE-129: Improper Validation of Array Index vulnerability exists that could cause local denial-of-service, and potentially kernel execution when a malicious actor with local user access crafts a script/program using an unpredictable index to an IOCTL call in the Foxboro.sys driver.	2023-06-14	7.8	High
CVE-2023-3001	schneider-electric - igss_dashboard	A CWE-502: Deserialization of Untrusted Data vulnerability exists in the Dashboard module that could cause an interpretation of malicious payload data, potentially leading to remote code execution when an attacker gets the user to open a malicious file.	2023-06-14	7.8	High
CVE-2023-24895	microsoft - .net_framework	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-24897	microsoft - .net_framework	.NET, .NET Framework, and Visual Studio Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2023-29326	microsoft - .net_framework	.NET Framework Remote Code Execution Vulnerability	2023-06-14	7.8	High
CVE-2022-22307	ibm - multiple products	IBM Security Guardium 11.3, 11.4, and 11.5 could allow a local user to obtain elevated privileges due to incorrect authorization checks. IBM X-Force ID: 216753.	2023-06-15	7.8	High
CVE-2023-21120	google - android	In multiple functions of cdm_engine.cpp, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-258188673	2023-06-15	7.8	High

CVE-2023-21121	google - multiple products	In onResume of AppManagementFragment.java, there is a possible way to prevent users from forgetting a previously connected VPN 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.Product: AndroidVersions: Android-11 Android-12Android ID: A-205460459	2023-06-15	7.8	High
CVE-2023-21122	google - multiple products	In various functions of various files, there is a possible way to bypass the DISALLOW_DEBUGGING_FEATURES restriction for tracing due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-270050191	2023-06-15	7.8	High
CVE-2023-21123	google - multiple products	In multiple functions of multiple files, there is a possible way to bypass the DISALLOW_DEBUGGING_FEATURES restriction for tracing due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-270050064	2023-06-15	7.8	High
CVE-2023-21124	google - multiple products	In run of multiple files, there is a possible escalation of privilege due to unsafe deserialization. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-265798353	2023-06-15	7.8	High
CVE-2023-21126	google - android	In bindOutputSwitcherAndBroadcastButton of MediaControlPanel.java, there is a possible launch arbitrary activity under SysUI due to Unsafe Intent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-271846393	2023-06-15	7.8	High
CVE-2023-21128	google - multiple products	In various functions of AppStandbyController.java, there is a possible way to break manageability scenarios 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.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-272042183	2023-06-15	7.8	High
CVE-2023-21129	google - multiple products	In getFullScreenIntentDecision of NotificationInterruptStateProviderImpl.java, there is a possible activity launch while the app is in the background due to a BAL bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-274759612	2023-06-15	7.8	High
CVE-2023-21131	google - multiple products	In checkKeyIntentParceledCorrectly() of ActivityManagerService.java, there is a possible bypass of Parcel Mismatch mitigations due to a logic error in the code. This could lead to local escalation of privilege and the ability to launch arbitrary activities in settings with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-265015796	2023-06-15	7.8	High
CVE-2023-21135	google - multiple products	In onCreate of NotificationAccessSettings.java, there is a possible failure to persist notifications settings 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.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-260570119	2023-06-15	7.8	High
CVE-2023-21138	google - multiple products	In onNullBinding of CallRedirectionProcessor.java, there is a possible long lived connection due to improper input validation. This could lead to local escalation of privilege and background activity launches with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-273260090	2023-06-15	7.8	High
CVE-2023-21139	google - android	In bindPlayer of MediaControlPanel.java, there is a possible launch arbitrary activity in SysUI due to Unsafe Intent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-271845008	2023-06-15	7.8	High
CVE-2023-32027	microsoft - multiple products	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	2023-06-16	7.8	High
CVE-2023-32028	microsoft - multiple products	Microsoft OLE DB Remote Code Execution Vulnerability	2023-06-16	7.8	High
CVE-2023-35788	linux - linux_kernel	An issue was discovered in fl_set_geneve_opt in net/sched/cls_flower.c in the Linux kernel before 6.3.7. It allows an out-of-bounds write in the flower classifier code via	2023-06-16	7.8	High

		TCA_FLOWER_KEY_ENC_OPTS_GENEVE packets. This may result in denial of service or privilege escalation.			
CVE-2023-28602	zoom - zoom	Zoom for Windows clients prior to 5.13.5 contain an improper verification of cryptographic signature vulnerability. A malicious user may potentially downgrade Zoom Client components to previous versions.	2023-06-13	7.7	High
CVE-2023-2729	synology - multiple products	Use of insufficiently random values vulnerability in User Management Functionality in Synology DiskStation Manager (DSM) before 7.2-64561 allows remote attackers to obtain user credential via unspecified vectors.	2023-06-13	7.5	High
CVE-2022-43949	fortinet - multiple products	A use of a broken or risky cryptographic algorithm [CWE-327] in Fortinet FortiSIEM before 6.7.1 allows a remote unauthenticated attacker to perform brute force attacks on GUI endpoints via taking advantage of outdated hashing methods.	2023-06-13	7.5	High
CVE-2023-22633	fortinet - multiple products	An improper permissions, privileges, and access controls vulnerability [CWE-264] in FortiNAC-F 7.2.0, FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.0 all versions 8.7.0 all versions may allow an unauthenticated attacker to perform a DoS attack on the device via client-secure renegotiation.	2023-06-13	7.5	High
CVE-2023-32011	microsoft - multiple products	Windows iSCSI Discovery Service Denial of Service Vulnerability	2023-06-14	7.5	High
CVE-2022-47184	apache - multiple products	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Software Foundation Apache Traffic Server.This issue affects Apache Traffic Server: 8.0.0 to 9.2.0.	2023-06-14	7.5	High
CVE-2023-30631	apache - multiple products	Improper Input Validation vulnerability in Apache Software Foundation Apache Traffic Server. The configuration option proxy.config.http.push_method_enabled didn't function. However, by default the PUSH method is blocked in the ip_allow configuration file.This issue affects Apache Traffic Server: from 8.0.0 through 9.2.0. 8.x users should upgrade to 8.1.7 or later versions 9.x users should upgrade to 9.2.1 or later versions	2023-06-14	7.5	High
CVE-2023-33933	apache - multiple products	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Software Foundation Apache Traffic Server.This issue affects Apache Traffic Server: from 8.0.0 through 9.2.0. 8.x users should upgrade to 8.1.7 or later versions 9.x users should upgrade to 9.2.1 or later versions	2023-06-14	7.5	High
CVE-2023-34396	apache - multiple products	Allocation of Resources Without Limits or Throttling vulnerability in Apache Software Foundation Apache Struts.This issue affects Apache Struts: through 2.5.30, through 6.1.2. Upgrade to Struts 2.5.31 or 6.1.2.1 or greater	2023-06-14	7.5	High
CVE-2023-24936	microsoft - .net_framework	.NET, .NET Framework, and Visual Studio Elevation of Privilege Vulnerability	2023-06-14	7.5	High
CVE-2023-29331	microsoft - .net_framework	.NET, .NET Framework, and Visual Studio Denial of Service Vulnerability	2023-06-14	7.5	High
CVE-2023-32030	microsoft - .net_framework	.NET and Visual Studio Denial of Service Vulnerability	2023-06-14	7.5	High
CVE-2023-25683	ibm - multiple products	IBM PowerVM Hypervisor FW950.00 through FW950.71, FW1010.00 through FW1010.40, FW1020.00 through FW1020.20, and FW1030.00 through FW1030.11 could allow an attacker to obtain sensitive information if they gain service access to the HMC. IBM X-Force ID: 247592.	2023-06-15	7.5	High
CVE-2022-33168	ibm - security_directory_suite_va	IBM Security Directory Suite VA 8.0.1 could allow an attacker to cause a denial of service due to uncontrolled resource consumption. IBM X-Force ID: 228588.	2023-06-15	7.5	High
CVE-2022-32757	ibm - security_directory_suite_va	IBM Security Directory Suite VA 8.0.1 through 8.0.1.19 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 228510.	2023-06-15	7.5	High
CVE-2023-21144	google - multiple products	In doInBackground of NotificationContentInflater.java, there is a possible temporary denial or service due to long running operations. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-252766417	2023-06-15	7.5	High
CVE-2023-22248	adobe - multiple products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. An attacker could leverage this vulnerability to leak another user's data. Exploitation of this issue does not require user interaction.	2023-06-15	7.5	High
CVE-2023-33126	microsoft - multiple products	.NET and Visual Studio Remote Code Execution Vulnerability	2023-06-14	7.3	High
CVE-2023-33128	microsoft - multiple products	.NET and Visual Studio Remote Code Execution Vulnerability	2023-06-14	7.3	High

CVE-2023-33130	microsoft - multiple products	Microsoft SharePoint Server Spoofing Vulnerability	2023-06-14	7.3	High
CVE-2023-33135	microsoft - multiple products	.NET and Visual Studio Elevation of Privilege Vulnerability	2023-06-14	7.3	High
CVE-2022-39946	fortinet - multiple products	An access control vulnerability [CWE-284] in FortiNAC version 9.4.2 and below, version 9.2.7 and below, 9.1 all versions, 8.8 all versions, 8.7 all versions, 8.6 all versions, 8.5 all versions may allow a remote attacker authenticated on the administrative interface to perform unauthorized jsp calls via crafted HTTP requests.	2023-06-13	7.2	High
CVE-2022-33166	ibm - security_directory_suite_va	IBM Security Directory Suite VA 8.0.1 through 8.0.1.19 could allow a privileged user to upload malicious files of dangerous types that can be automatically processed within the product's environment. IBM X-Force ID: 228586.	2023-06-15	7.2	High
CVE-2023-29297	adobe - multiple products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by a Improper Neutralization of Special Elements Used in a Template Engine vulnerability that could lead to arbitrary code execution by an admin-privilege authenticated attacker. Exploitation of this issue does not require user interaction.	2023-06-15	7.2	High
CVE-2023-28603	zoom - virtual_desktop_infrastructure	Zoom VDI client installer prior to 5.14.0 contains an improper access control vulnerability. A malicious user may potentially delete local files without proper permissions.	2023-06-13	7.1	High
CVE-2023-21565	microsoft - multiple products	Azure DevOps Server Spoofing Vulnerability	2023-06-14	7.1	High
CVE-2023-32021	microsoft - multiple products	Windows SMB Witness Service Security Feature Bypass Vulnerability	2023-06-14	7.1	High
CVE-2023-29337	microsoft - multiple products	NuGet Client Remote Code Execution Vulnerability	2023-06-14	7.1	High
CVE-2023-29361	microsoft - multiple products	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	2023-06-14	7	High
CVE-2023-29364	microsoft - multiple products	Windows Authentication Elevation of Privilege Vulnerability	2023-06-14	7	High
CVE-2023-29368	microsoft - multiple products	Windows Filtering Platform Elevation of Privilege Vulnerability	2023-06-14	7	High
CVE-2023-32010	microsoft - multiple products	Windows Bus Filter Driver Elevation of Privilege Vulnerability	2023-06-14	7	High
CVE-2023-21101	google - android	In multiple functions of WVDrmPlugin.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.Product: AndroidVersions: Android SoCAndroid ID: A-258189255	2023-06-15	7	High
CVE-2023-3159	linux - multiple products	A use after free issue was discovered in driver/firewire in outbound_phy_packet_callback in the Linux Kernel. In this flaw a local attacker with special privilege may cause a use after free problem when queue_event() fails.	2023-06-12	6.7	Medium
CVE-2023-33144	microsoft - visual_studio_code	Visual Studio Code Spoofing Vulnerability	2023-06-14	6.6	Medium
CVE-2023-34212	apache - nifi	The JndiJmsConnectionFactoryProvider Controller Service, along with the ConsumeJMS and PublishJMS Processors, in Apache NiFi 1.8.0 through 1.21.0 allow an authenticated and authorized user to configure URL and library properties that enable deserialization of untrusted data from a remote location. The resolution validates the JNDI URL and restricts locations to a set of allowed schemes. You are recommended to upgrade to version 1.22.0 or later which fixes this issue.	2023-06-12	6.5	Medium
CVE-2023-25609	fortinet - multiple products	A server-side request forgery (SSRF) vulnerability [CWE-918] in FortiManager and FortiAnalyzer GUI 7.2.0 through 7.2.1, 7.0.0 through 7.0.6, 6.4.8 through 6.4.11 may allow a remote and authenticated attacker to access unauthorized files and services on the system via specially crafted web requests.	2023-06-13	6.5	Medium
CVE-2023-26207	fortinet - multiple products	An insertion of sensitive information into log file vulnerability in Fortinet FortiOS 7.2.0 through 7.2.4 and FortiProxy 7.0.0 through 7.0.10. 7.2.0 through 7.2.1 allows an attacker to read certain passwords in plain text.	2023-06-13	6.5	Medium
CVE-2023-33305	fortinet - multiple products	A loop with unreachable exit condition ('infinite loop') in Fortinet FortiOS version 7.2.0 through 7.2.4, FortiOS version 7.0.0 through 7.0.10, FortiOS 6.4 all versions, FortiOS 6.2 all versions, FortiOS 6.0 all versions, FortiProxy version 7.2.0 through 7.2.3, FortiProxy version 7.0.0 through 7.0.9, FortiProxy 2.0 all versions, FortiProxy 1.2 all versions, FortiProxy 1.1 all versions, FortiProxy 1.0 all versions, FortiWeb version 7.2.0 through 7.2.1, FortiWeb version 7.0.0 through 7.0.6, FortiWeb 6.4 all versions, FortiWeb 6.3 all versions allows attacker to perform a denial of service via specially crafted HTTP requests.	2023-06-13	6.5	Medium

CVE-2023-28598	zoom - zoom	Zoom for Linux clients prior to 5.13.10 contain an HTML injection vulnerability. If a victim starts a chat with a malicious user it could result in a Zoom application crash.	2023-06-13	6.5	Medium
CVE-2023-28601	zoom - zoom	Zoom for Windows clients prior to 5.14.0 contain an improper restriction of operations within the bounds of a memory buffer vulnerability. A malicious user may alter protected Zoom Client memory buffer potentially causing integrity issues within the Zoom Client.	2023-06-13	6.5	Medium
CVE-2023-34114	zoom - multiple products	Exposure of resource to wrong sphere in Zoom for Windows and Zoom for MacOS clients before 5.14.10 may allow an authenticated user to potentially enable information disclosure via network access.	2023-06-13	6.5	Medium
CVE-2023-24938	microsoft - multiple products	Windows CryptoAPI Denial of Service Vulnerability	2023-06-14	6.5	Medium
CVE-2023-29352	microsoft - multiple products	Windows Remote Desktop Security Feature Bypass Vulnerability	2023-06-14	6.5	Medium
CVE-2023-29369	microsoft - multiple products	Remote Procedure Call Runtime Denial of Service Vulnerability	2023-06-14	6.5	Medium
CVE-2023-32032	microsoft - multiple products	.NET and Visual Studio Elevation of Privilege Vulnerability	2023-06-14	6.5	Medium
CVE-2023-33129	microsoft - multiple products	Microsoft SharePoint Denial of Service Vulnerability	2023-06-14	6.5	Medium
CVE-2023-33140	microsoft - onenote	Microsoft OneNote Spoofing Vulnerability	2023-06-14	6.5	Medium
CVE-2023-33142	microsoft - multiple products	Microsoft SharePoint Server Elevation of Privilege Vulnerability	2023-06-14	6.5	Medium
CVE-2023-33145	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2023-06-14	6.5	Medium
CVE-2023-24937	microsoft - multiple products	Windows CryptoAPI Denial of Service Vulnerability	2023-06-14	6.5	Medium
CVE-2023-34149	apache - multiple products	Allocation of Resources Without Limits or Throttling vulnerability in Apache Software Foundation Apache Struts.This issue affects Apache Struts: through 2.5.30, through 6.1.2. Upgrade to Struts 2.5.31 or 6.1.2.1 or greater.	2023-06-14	6.5	Medium
CVE-2023-35147	jenkins - aws_codecommit_trigger	Jenkins AWS CodeCommit Trigger Plugin 3.0.12 and earlier does not restrict the AWS SQS queue name path parameter in an HTTP endpoint, allowing attackers with Item/Read permission to obtain the contents of arbitrary files on the Jenkins controller file system.	2023-06-14	6.5	Medium
CVE-2023-35149	jenkins - digital.ai_app_management_publisher	A missing permission check in Jenkins Digital.ai App Management Publisher Plugin 2.6 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL, capturing credentials stored in Jenkins.	2023-06-14	6.5	Medium
CVE-2022-33159	ibm - security_directory_suite_va	IBM Security Directory Suite VA 8.0.1 through 8.0.1.19 stores user credentials in plain clear text which can be read by an authenticated user. IBM X-Force ID: 228567.	2023-06-15	6.5	Medium
CVE-2023-29289	adobe - multiple products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an XML Injection vulnerability. An attacker with low privileges can trigger a specially crafted script to a security feature bypass. Exploitation of this issue does not require user interaction.	2023-06-15	6.5	Medium
CVE-2023-33306	fortinet - multiple products	A null pointer dereference in Fortinet FortiOS before 7.2.5, before 7.0.11 and before 6.4.13, FortiProxy before 7.2.4 and before 7.0.10 allows attacker to denial of sslvpn service via specifically crafted request in bookmark parameter.	2023-06-16	6.5	Medium
CVE-2023-33307	fortinet - multiple products	A null pointer dereference in Fortinet FortiOS before 7.2.5 and before 7.0.11, FortiProxy before 7.2.3 and before 7.0.9 allows attacker to denial of sslvpn service via specifically crafted request in network parameter.	2023-06-16	6.5	Medium
CVE-2023-33132	microsoft - multiple products	Microsoft SharePoint Server Spoofing Vulnerability	2023-06-14	6.3	Medium
CVE-2023-33985	sap - netweaver	SAP NetWeaver Enterprise Portal - version 7.50, does not sufficiently encode user-controlled inputs over the network, resulting in reflected Cross-Site Scripting (XSS) vulnerability, therefore changing the scope of the attack. On successful exploitation, an attacker can view or modify information causing a limited impact on confidentiality and integrity of the application.	2023-06-13	6.1	Medium
CVE-2023-33986	sap - customer_relationship_management_abap	SAP CRM ABAP (Grantor Management) - versions 700, 701, 702, 712, 713, 714, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. After successful exploitation, an attacker can cause limited impact on confidentiality and integrity of the application.	2023-06-13	6.1	Medium
CVE-2023-24469	microfocus - arcsight_logger	Potential Cross-Site Scripting in ArcSight Logger versions prior to 7.3.0	2023-06-13	6.1	Medium
CVE-2023-35029	liferay - multiple products	Open redirect vulnerability in the Layout module's SEO configuration in Liferay Portal 7.4.3.70 through 7.4.3.76, and Liferay DXP 7.4 update 70 through 76 allows remote attackers to redirect users to arbitrary external URLs via the	2023-06-15	6.1	Medium

		`_com_liferay_layout_admin_web_portlet_GroupPagesPortlet_backURL` parameter.			
CVE-2023-3193	liferay - multiple products	Cross-site scripting (XSS) vulnerability in the Layout module's SEO configuration in Liferay Portal 7.4.3.70 through 7.4.3.73, and Liferay DXP 7.4 update 70 through 73 allows remote attackers to inject arbitrary web script or HTML via the `_com_liferay_layout_admin_web_portlet_GroupPagesPortlet_backURL` parameter.	2023-06-15	6.1	Medium
CVE-2023-32020	microsoft - multiple products	Windows DNS Spoofing Vulnerability	2023-06-14	5.6	Medium
CVE-2023-3161	linux - multiple products	A flaw was found in the Framebuffer Console (fbcon) in the Linux Kernel. When providing font->width and font->height greater than 32 to fbcon_set_font, since there are no checks in place, a shift-out-of-bounds occurs leading to undefined behavior and possible denial of service.	2023-06-12	5.5	Medium
CVE-2022-33877	fortinet - multiple products	An incorrect default permission [CWE-276] vulnerability in FortiClient (Windows) versions 7.0.0 through 7.0.6 and 6.4.0 through 6.4.8 and FortiConverter (Windows) versions 6.2.0 through 6.2.1, 7.0.0 and all versions of 6.0.0 may allow a local authenticated attacker to tamper with files in the installation folder, if FortiClient or FortiConverter is installed in an insecure folder.	2023-06-13	5.5	Medium
CVE-2023-21569	microsoft - multiple products	Azure DevOps Server Spoofing Vulnerability	2023-06-14	5.5	Medium
CVE-2023-29353	microsoft - multiple products	Sysinternals Process Monitor for Windows Denial of Service Vulnerability	2023-06-14	5.5	Medium
CVE-2023-32016	microsoft - multiple products	Windows Installer Information Disclosure Vulnerability	2023-06-14	5.5	Medium
CVE-2023-33139	microsoft - multiple products	Visual Studio Information Disclosure Vulnerability	2023-06-14	5.5	Medium
CVE-2023-0837	teamviewer - remote	An improper authorization check of local device settings in TeamViewer Remote between version 15.41 and 15.42.7 for Windows and macOS allows an unprivileged user to change basic local device settings even though the options were locked. This can result in unwanted changes to the configuration.	2023-06-14	5.5	Medium
CVE-2023-21105	google - multiple products	In multiple functions of ChooserActivity.java, there is a possible cross-user media read 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.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-261036568	2023-06-15	5.5	Medium
CVE-2023-21136	google - multiple products	In multiple functions of JobStore.java, there is a possible way to cause a crash on startup due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-246542285	2023-06-15	5.5	Medium
CVE-2023-21137	google - multiple products	In several methods of JobStore.java, uncaught exceptions in job map parsing could lead to local persistent denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-246541702	2023-06-15	5.5	Medium
CVE-2023-21141	google - multiple products	In several functions of several files, there is a possible way to access developer mode traces due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-262244249	2023-06-15	5.5	Medium
CVE-2023-21142	google - multiple products	In multiple files, there is a possible way to access traces in the dev mode due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-262243665	2023-06-15	5.5	Medium
CVE-2023-21143	google - multiple products	In multiple functions of multiple files, there is a possible way to make the device unusable due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-268193777	2023-06-15	5.5	Medium
CVE-2023-33984	sap - netweaver	SAP NetWeaver (Design Time Repository) - version 7.50, returns an unfavorable content type for some versioned files, which could allow an authorized attacker to create a file with a malicious content and send a link to a victim in an email or instant message. Under certain circumstances, this could lead to Cross-Site Scripting vulnerability.	2023-06-13	5.4	Medium
CVE-2023-28600	zoom - zoom	Zoom for MacOSclients prior to 5.14.0 contain an improper access control vulnerability. A malicious user may be able to	2023-06-13	5.4	Medium

		delete/replace Zoom Client files potentially causing a loss of integrity and availability to the Zoom Client.			
CVE-2023-35143	jenkins - maven_repository_server	Jenkins Maven Repository Server Plugin 1.10 and earlier does not escape the versions of build artifacts on the Build Artifacts As Maven Repository page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control maven project versions in `pom.xml`.	2023-06-14	5.4	Medium
CVE-2023-35144	jenkins - maven_repository_server	Jenkins Maven Repository Server Plugin 1.10 and earlier does not escape project and build display names on the Build Artifacts As Maven Repository page, resulting in a stored cross-site scripting (XSS) vulnerability.	2023-06-14	5.4	Medium
CVE-2023-35145	jenkins - sonargraph_integration	Jenkins Sonargraph Integration Plugin 5.0.1 and earlier does not escape the file path and the project name for the Log file field form validation, resulting in a stored cross-site scripting vulnerability exploitable by attackers with Item/Configure permission.	2023-06-14	5.4	Medium
CVE-2023-35146	jenkins - template_workflows	Jenkins Template Workflows Plugin 41.v32d86a_313b_4a and earlier does not escape names of jobs used as buildings blocks for Template Workflow Job, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to create jobs.	2023-06-14	5.4	Medium
CVE-2023-0010	paloaltonetworks - multiple products	A reflected cross-site scripting (XSS) vulnerability in the Captive Portal feature of Palo Alto Networks PAN-OS software can allow a JavaScript payload to be executed in the context of an authenticated Captive Portal user’s browser when they click on a specifically crafted link.	2023-06-14	5.4	Medium
CVE-2023-29302	adobe - multiple products	Adobe Experience Manager versions 6.5.16.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-06-15	5.4	Medium
CVE-2023-29304	adobe - multiple products	Adobe Experience Manager versions 6.5.16.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-06-15	5.4	Medium
CVE-2023-29307	adobe - multiple products	Adobe Experience Manager versions 6.5.16.0 (and earlier) is affected by a URL Redirection to Untrusted Site ('Open Redirect') vulnerability. A low-privilege authenticated attacker could leverage this vulnerability to redirect users to malicious websites. Exploitation of this issue requires user interaction.	2023-06-15	5.4	Medium
CVE-2023-29322	adobe - multiple products	Adobe Experience Manager versions 6.5.16.0 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	2023-06-15	5.4	Medium
CVE-2023-29355	microsoft - multiple products	DHCP Server Service Information Disclosure Vulnerability	2023-06-14	5.3	Medium
CVE-2023-32013	microsoft - multiple products	Windows Hyper-V Denial of Service Vulnerability	2023-06-14	5.3	Medium
CVE-2023-29287	adobe - multiple products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Information Exposure vulnerability that could lead to a security feature bypass. An attacker could leverage this vulnerability to leak minor user data. Exploitation of this issue does not require user interaction..	2023-06-15	5.3	Medium
CVE-2023-29290	adobe - multiple products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. An attacker could leverage this vulnerability to bypass a minor functionality. Exploitation of this issue does not require user interaction.	2023-06-15	5.3	Medium
CVE-2023-29291	adobe - multiple products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. An admin-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require user interaction.	2023-06-15	4.9	Medium
CVE-2023-29292	adobe - multiple products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by a Server-Side Request Forgery (SSRF) vulnerability that could lead to arbitrary file system read. An admin-privilege authenticated attacker can force the application to make arbitrary requests via injection of arbitrary URLs. Exploitation of this issue does not require user interaction.	2023-06-15	4.9	Medium
CVE-2023-29175	fortinet - multiple products	An improper certificate validation vulnerability [CWE-295] in FortiOS 6.2 all versions, 6.4 all versions, 7.0.0 through 7.0.10, 7.2.0 and FortiProxy 1.2 all versions, 2.0 all versions, 7.0.0 through 7.0.9, 7.2.0 through 7.2.3 may allow a remote and unauthenticated attacker to perform a Man-in-the-Middle attack on the	2023-06-13	4.8	Medium

		communication channel between the vulnerable device and the remote FortiGuard's map server.			
CVE-2023-32019	microsoft - multiple products	Windows Kernel Information Disclosure Vulnerability	2023-06-14	4.7	Medium
CVE-2023-21095	google - multiple products	In canStartSystemGesture of RecentsAnimationDeviceState.java, there is a possible partial lockscreen bypass 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.Product: AndroidVersions: Android-12L Android-13Android ID: A-242704576	2023-06-15	4.7	Medium
CVE-2022-41327	fortinet - multiple products	A cleartext transmission of sensitive information vulnerability [CWE-319] in Fortinet FortiOS version 7.2.0 through 7.2.4, 7.0.0 through 7.0.8, FortiProxy version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.8 allows an authenticated attacker with readonly superadmin privileges to intercept traffic in order to obtain other adminstrators cookies via diagnose CLI commands.	2023-06-13	4.4	Medium
CVE-2023-29178	fortinet - multiple products	A access of uninitialized pointer vulnerability [CWE-824] in Fortinet FortiProxy version 7.2.0 through 7.2.3 and before 7.0.9 and FortiOS version 7.2.0 through 7.2.4 and before 7.0.11 allows an authenticated attacker to repetitively crash the httpsd process via crafted HTTP or HTTPS requests.	2023-06-13	4.3	Medium
CVE-2023-28599	zoom - multiple products	Zoom clients prior to 5.13.10 contain an HTML injection vulnerability. A malicious user could inject HTML into their display name potentially leading a victim to a malicious website during meeting creation.	2023-06-13	4.3	Medium
CVE-2023-29288	adobe - multiple products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A privileged attacker could leverage this vulnerability to modify a minor functionality of another user's data. Exploitation of this issue does not require user interaction.	2023-06-15	4.3	Medium
CVE-2023-29294	adobe - multiple products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by a Business Logic Errors vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass a minor functionality. Exploitation of this issue does not require user interaction.	2023-06-15	4.3	Medium
CVE-2023-29295	adobe - multiple products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass a minor functionality. Exploitation of this issue does not require user interaction.	2023-06-15	4.3	Medium
CVE-2023-29296	adobe - multiple products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Incorrect Authorization vulnerability that could result in a security feature bypass. A low-privileged attacker could leverage this vulnerability to modify a minor functionality of another user's data. Exploitation of this issue does not require user interaction.	2023-06-15	4.3	Medium
CVE-2023-20867	vmware - tools	A fully compromised ESXi host can force VMware Tools to fail to authenticate host-to-guest operations, impacting the confidentiality and integrity of the guest virtual machine.	2023-06-13	3.9	Low
CVE-2023-34115	zoom - meeting_sdk	Buffer copy without checking size of input in Zoom Meeting SDK before 5.13.0 may allow an authenticated user to potentially enable a denial of service via local access. This issue may result in the Zoom Meeting SDK to crash and need to be restarted.	2023-06-13	3.8	Low
CVE-2023-28303	microsoft - multiple products	Windows Snipping Tool Information Disclosure Vulnerability	2023-06-13	3.3	Low
CVE-2023-32024	microsoft - power_apps	Microsoft Power Apps Spoofing Vulnerability	2023-06-14	3	Low
CVE-2023-32114	sap - multiple products	SAP NetWeaver (Change and Transport System) - versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, allows an authenticated user with admin privileges to maliciously run a benchmark program repeatedly in intent to slowdown or make the server unavailable which may lead to a limited impact on Availability with No impact on Confidentiality and Integrity of the application.	2023-06-13	2.7	Low
CVE-2022-42474	fortinet - multiple products	A relative path traversal vulnerability [CWE-23] in Fortinet FortiOS version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.9 and before 6.4.12, FortiProxy version 7.2.0 through 7.2.1 and 7.0.0 through 7.0.7, FortiSwitchManager version 7.2.0 through 7.2.1 and before 7.0.1 allows an privileged attacker to delete arbitrary directories from the filesystem through crafted HTTP requests.	2023-06-13	2.7	Low
CVE-2023-29293	adobe - multiple products	Adobe Commerce versions 2.4.6 (and earlier), 2.4.5-p2 (and earlier) and 2.4.4-p3 (and earlier) are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An admin privileged attacker could leverage this vulnerability to impact the availability of a user's minor feature. Exploitation of this issue does not require user interaction.	2023-06-15	2.7	Low

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.

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.