الهيئة الوطنية
للأمن السيبراني
National Cybersecurity Authority

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

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

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 14th of May to 20th of May. 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**

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 ١٤ مايو إلى ٢٠ مايو. 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**

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2022-47937	apache - sling_commons_json	Improper input validation in the Apache Sling Commons JSON bundle allows an attacker to trigger unexpected errors by supplying specially-crafted input. NOTE: This vulnerability only affects products that are no longer supported by the maintainer The org.apache.sling.commons.json bundle has been deprecated as of March 2017 and should not be used anymore. Consumers are encouraged to consider the Apache Sling Commons Johnzon OSGi bundle provided by the Apache Sling project, but may of course use other JSON libraries.	2023-05-15	9.8	Critical
CVE-2021-0877	google - android	Product: AndroidVersions: Android SoCAndroid ID: A-273754094	2023-05-15	9.8	Critical
CVE-2023-32956	synology - multiple products	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in CGI component in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows remote attackers to execute arbitrary code via unspecified vectors.	2023-05-16	9.8	Critical
CVE-2023-32981	jenkins - pipeline_utility_steps	An arbitrary file write vulnerability in Jenkins Pipeline Utility Steps Plugin 2.15.2 and earlier allows attackers able to provide crafted archives as parameters to create or replace arbitrary files on the agent file system with attacker-specified content.	2023-05-16	9.8	Critical
CVE-2023-20156	cisco - business_250-16p-2g_firmware	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	9.8	Critical
CVE-2023-20157	cisco - business_250-16p-2g_firmware	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	9.8	Critical
CVE-2023-20158	cisco - business_250-16p-2g_firmware	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	9.8	Critical

CVE-2023-20159	cisco - business_250-16p-2g_firmware	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	9.8	Critical
CVE-2023-20160	cisco - business_250-16p-2g_firmware	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	9.8	Critical
CVE-2023-20161	cisco - business_250-16p-2g_firmware	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	9.8	Critical
CVE-2023-20162	cisco - business_250-16p-2g_firmware	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	9.8	Critical
CVE-2023-20189	cisco - business_250-16p-2g_firmware	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	9.8	Critical
CVE-2022-47984	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 243163.	2023-05-19	9.8	Critical
CVE-2023-31131	vmware - greenplum_database	Greenplum Database (GPDB) is an open source data warehouse based on PostgreSQL. In versions prior to 6.22.3 Greenplum Database used an unsafe methods to extract tar files within GPPKGs. greenplum-db is vulnerable to path traversal leading to arbitrary file writes. An attacker can use this vulnerability to overwrite data or system files potentially leading to crash or malfunction of the system. Any files which are accessible to the running process are at risk. All users are requested to upgrade to Greenplum Database version 6.23.2 or higher. There are no known workarounds for this vulnerability.	2023-05-15	9.1	Critical
CVE-2023-32986	jenkins - file_parameters	Jenkins File Parameter Plugin 285.v757c5b_67a_c25 and earlier does not restrict the name (and resulting uploaded file name) of Stashed File Parameters, allowing attackers with Item/Configure permission to create or replace arbitrary files on the Jenkins controller file system with attacker-specified content.	2023-05-16	8.8	High
CVE-2023-32987	jenkins - reverse_proxy_auth	A cross-site request forgery (CSRF) vulnerability in Jenkins Reverse Proxy Auth Plugin 1.7.4 and earlier allows attackers to connect to an attacker-specified LDAP server using attacker-specified credentials.	2023-05-16	8.8	High
CVE-2023-32989	jenkins - azure_vm_agents	A cross-site request forgery (CSRF) vulnerability in Jenkins Azure VM Agents Plugin 852.v8d35f0960a_43 and earlier allows attackers to connect to an attacker-specified Azure Cloud server using attacker-specified credentials IDs obtained through another method.	2023-05-16	8.8	High
CVE-2023-32991	jenkins - saml_single_sign_on	A cross-site request forgery (CSRF) vulnerability in Jenkins SAML Single Sign On(SSO) Plugin 2.0.2 and earlier allows attackers to send an HTTP request to an attacker-specified URL and parse the response as XML, or parse a local file on the Jenkins controller as XML.	2023-05-16	8.8	High
CVE-2023-32992	jenkins - saml_single_sign_on	Missing permission checks in Jenkins SAML Single Sign On(SSO) Plugin 2.0.2 and earlier allow attackers with Overall/Read permission to send an HTTP request to an attacker-specified URL and parse the response as XML, or parse a local file on the Jenkins controller as XML.	2023-05-16	8.8	High

CVE-2023-32995	jenkins - saml_single_sign_on	A cross-site request forgery (CSRF) vulnerability in Jenkins SAML Single Sign On(SSO) Plugin 2.0.0 and earlier allows attackers to send an HTTP POST request with JSON body containing attacker-specified content, to miniOrange's API for sending emails.	2023-05-16	8.8	High
CVE-2023-2721	google - chrome	Use after free in Navigation in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2023-05-16	8.8	High
CVE-2023-2722	google - chrome	Use after free in Autofill UI in Google Chrome on Android prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-05-16	8.8	High
CVE-2023-2723	google - chrome	Use after free in DevTools in Google Chrome prior to 113.0.5672.126 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-05-16	8.8	High
CVE-2023-2724	google - chrome	Type confusion in V8 in Google Chrome prior to 113.0.5672.126 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-05-16	8.8	High
CVE-2023-2725	google - chrome	Use after free in Guest View in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-05-16	8.8	High
CVE-2023-2726	google - chrome	Inappropriate implementation in WebApp Installs in Google Chrome prior to 113.0.5672.126 allowed an attacker who convinced a user to install a malicious web app to bypass install dialog via a crafted HTML page. (Chromium security severity: Medium)	2023-05-16	8.8	High
CVE-2023-30501	arubanetworks - multiple products	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	2023-05-16	8.8	High
CVE-2023-30502	arubanetworks - multiple products	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	2023-05-16	8.8	High
CVE-2023-30503	arubanetworks - multiple products	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	2023-05-16	8.8	High
CVE-2023-30504	arubanetworks - multiple products	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	2023-05-16	8.8	High
CVE-2023-30505	arubanetworks - multiple products	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	2023-05-16	8.8	High
CVE-2023-30506	arubanetworks - multiple products	Vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface that allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as root on the underlying operating system leading to complete system compromise.	2023-05-16	8.8	High
CVE-2023-30438	ibm - powervm_hypervisor	An internally discovered vulnerability in PowerVM on IBM Power9 and Power10 systems could allow an attacker with privileged user access to a logical partition to perform an undetected violation of the isolation between logical partitions which could lead to data leakage or the execution of arbitrary code in other logical partitions on the same physical server. IBM X-Force ID: 252706.	2023-05-17	8.8	High
CVE-2023-31700	tp-link - multiple products	TP-Link TL-WPA4530 KIT V2 (EU)_170406 and V2 (EU)_161115 is vulnerable to Command Injection via _httpRpmPlcDeviceAdd.	2023-05-17	8.8	High

CVE-2023-31701	tp-link - multiple products	TP-Link TL-WPA4530 KIT V2 (EU)_170406 and V2 (EU)_161115 is vulnerable to Command Injection via _httpRpmPlcDeviceRemove.	2023-05-17	8.8	High
CVE-2023-20003	cisco - business_140ac_access_point_firmware	A vulnerability in the social login configuration option for the guest users of Cisco Business Wireless Access Points (APs) could allow an unauthenticated, adjacent attacker to bypass social login authentication. This vulnerability is due to a logic error with the social login implementation. An attacker could exploit this vulnerability by attempting to authenticate to an affected device. A successful exploit could allow the attacker to access the Guest Portal without authentication.	2023-05-18	8.8	High
CVE-2023-20182	cisco - multiple products	Multiple vulnerabilities in the API of Cisco DNA Center Software could allow an authenticated, remote attacker to read information from a restricted container, enumerate user information, or execute arbitrary commands in a restricted container as the root user. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	8.8	High
CVE-2023-32955	synology - multiple products	Improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability in DHCP Client Functionality in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows man-in-the-middle attackers to execute arbitrary commands via unspecified vectors.	2023-05-16	8.1	High
CVE-2023-21102	google - android	In __efi_rt_asm_wrapper of efi-rt-wrapper.S, there is a possible bypass of shadow stack protection 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 kernelAndroid ID: A-260821414References: Upstream kernel	2023-05-15	7.8	High
CVE-2023-21106	google - android	In adreno_set_param of adreno_gpu.c, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-265016072References: Upstream kernel	2023-05-15	7.8	High
CVE-2023-21107	google - multiple products	In retrieveAppEntry of NotificationAccessDetails.java, there is a missing permission check. This could lead to local escalation of privilege across user boundaries 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-259385017	2023-05-15	7.8	High
CVE-2023-21109	google - multiple products	In multiple places of AccessibilityService, there is a possible way to hide the app from the user 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-261589597	2023-05-15	7.8	High
CVE-2023-21110	google - multiple products	In several functions of SnoozeHelper.java, there is a possible way to grant notifications access due to resource exhaustion. 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-258422365	2023-05-15	7.8	High
CVE-2023-21117	google - android	In registerReceiverWithFeature of ActivityManagerService.java, there is a possible way for isolated processes to register a broadcast receiver due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-263358101	2023-05-15	7.8	High
CVE-2023-2124	linux - linux_kernel	An out-of-bounds memory access flaw was found in the Linux kernel's XFS file system in how a user restores an XFS image after failure (with a dirty log journal). This flaw allows a local user to crash or potentially escalate their privileges on the system.	2023-05-15	7.8	High
CVE-2023-2491	gnu - multiple products	A flaw was found in the Emacs text editor. Processing a specially crafted org-mode code with the "org-babel-execute:latex" function in ob-latex.el can result in arbitrary command execution. This CVE exists because of a CVE-2023-28617 security regression for the emacs package in Red Hat Enterprise Linux 8.8 and Red Hat Enterprise Linux 9.2.	2023-05-17	7.8	High
CVE-2023-28076	dell - cloudlink	CloudLink 7.1.2 and all prior versions contain a broken or risky cryptographic algorithm vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability leading to some information disclosure.	2023-05-16	7.5	High
CVE-2023-33001	jenkins - hashicorp_vault	Jenkins HashiCorp Vault Plugin 360.v0a_1c04cf807d and earlier does not properly mask (i.e., replace with asterisks) credentials in the build log when push mode for durable task logging is enabled.	2023-05-16	7.5	High
CVE-2023-20024	cisco - business_250-16p-2g_firmware	Multiple vulnerabilities in the web-based user interface of certain Cisco Small Business Series Switches could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or execute arbitrary code with root privileges on an affected device. These vulnerabilities are due to improper	2023-05-18	7.5	High

		validation of requests that are sent to the web interface. For more information about these vulnerabilities, see the Details section of this advisory.			
CVE-2023-2789	gnu - cflow	A vulnerability was found in GNU cflow 1.7. It has been rated as problematic. This issue affects the function func_body/parse_variable_declaration of the file parser.c. The manipulation leads to denial of service. The exploit has been disclosed to the public and may be used. The identifier VDB-229373 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	2023-05-18	7.5	High
CVE-2023-1692	huawei - multiple products	The window management module lacks permission verification.Successful exploitation of this vulnerability may affect confidentiality.	2023-05-20	7.5	High
CVE-2023-1693	huawei - multiple products	The Settings module has the file privilege escalation vulnerability.Successful exploitation of this vulnerability may affect confidentiality.	2023-05-20	7.5	High
CVE-2023-1694	huawei - multiple products	The Settings module has the file privilege escalation vulnerability.Successful exploitation of this vulnerability may affect confidentiality.	2023-05-20	7.5	High
CVE-2023-1696	huawei - multiple products	The multimedia video module has a vulnerability in data processing.Successful exploitation of this vulnerability may affect availability.	2023-05-20	7.5	High
CVE-2023-20163	cisco - multiple products	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	7.2	High
CVE-2023-20164	cisco - multiple products	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform command injection attacks on the underlying operating system and elevate privileges to root. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	7.2	High
CVE-2023-28045	dell - cloudiq_collector	Dell CloudIQ Collector version 1.10.2 contains a missing encryption of sensitive data vulnerability. An attacker with low privileges could potentially exploit this vulnerability, leading to gain access to unauthorized data.	2023-05-19	7.1	High
CVE-2023-20694	google - multiple products	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07733998 / ALPS07874388 (For MT6880 and MT6890 only); Issue ID: ALPS07733998 / ALPS07874388 (For MT6880 and MT6890 only).	2023-05-15	6.7	Medium
CVE-2023-20695	google - multiple products	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07734012 / ALPS07874363 (For MT6880, MT6890, MT6980 and MT6990 only); Issue ID: ALPS07734012 / ALPS07874363 (For MT6880, MT6890, MT6980 and MT6990 only).	2023-05-15	6.7	Medium
CVE-2023-20696	google - multiple products	In preloader, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07856356 / ALPS07874388 (For MT6880 and MT6890 only); Issue ID: ALPS07856356 / ALPS07874388 (For MT6880 and MT6890 only).	2023-05-15	6.7	Medium
CVE-2023-20699	google - multiple products	In adsp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07696073; Issue ID: ALPS07696073.	2023-05-15	6.7	Medium
CVE-2023-20700	google - multiple products	In widevine, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07643304; Issue ID: ALPS07643304.	2023-05-15	6.7	Medium
CVE-2023-20701	google - multiple products	In widevine, there is a possible out of bounds write due to a logic error. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07643270; Issue ID: ALPS07643270.	2023-05-15	6.7	Medium
CVE-2023-20707	google - multiple products	In ril, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07628556; Issue ID: ALPS07628556.	2023-05-15	6.7	Medium
CVE-2023-20708	google - multiple products	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of	2023-05-15	6.7	Medium

		privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07581655; Issue ID: ALPS07581655.			
CVE-2023-20718	google - multiple products	In vcu, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645181; Issue ID: ALPS07645181.	2023-05-15	6.7	Medium
CVE-2023-20720	google - multiple products	In pqframework, there is a possible out of bounds read due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629586; Issue ID: ALPS07629586.	2023-05-15	6.7	Medium
CVE-2023-20721	google - multiple products	In isp, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07162155; Issue ID: ALPS07162155.	2023-05-15	6.7	Medium
CVE-2023-20722	google - multiple products	In m4u, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07771518; Issue ID: ALPS07680084.	2023-05-15	6.7	Medium
CVE-2023-21116	google - multiple products	In verifyReplacingVersionCode of InstallPackageHelper.java, there is a possible way to downgrade system apps below system image version due to a logic error in the code. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-256202273	2023-05-15	6.7	Medium
CVE-2023-20166	cisco - multiple products	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform path traversal attacks on the underlying operating system to either elevate privileges to root or read arbitrary files. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	6.7	Medium
CVE-2023-31756	tp-link - archer_vr1600v_firmware	A command injection vulnerability exists in the administrative web portal in TP-Link Archer VR1600V devices running firmware Versions <= 0.1.0. 0.9.1 v5006.0 Build 220518 Rel.32480n which allows remote attackers, authenticated to the administrative web portal as an administrator user to open an operating system level shell via the 'X_TP_IfName' parameter.	2023-05-19	6.7	Medium
CVE-2023-32990	jenkins - azure_vm_agents	A missing permission check in Jenkins Azure VM Agents Plugin 852.v8d35f0960a_43 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified Azure Cloud server using attacker-specified credentials IDs obtained through another method.	2023-05-16	6.5	Medium
CVE-2023-30507	arubanetworks - multiple products	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including sensitive system files.	2023-05-16	6.5	Medium
CVE-2023-30508	arubanetworks - multiple products	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including sensitive system files.	2023-05-16	6.5	Medium
CVE-2023-30509	arubanetworks - multiple products	Multiple authenticated path traversal vulnerabilities exist in the Aruba EdgeConnect Enterprise command line interface. Successful exploitation of these vulnerabilities result in the ability to read arbitrary files on the underlying operating system, including sensitive system files.	2023-05-16	6.5	Medium
CVE-2023-1972	gnu - binutils	A potential heap based buffer overflow was found in _bfd_elf_slurp_version_tables() in bfd/elf.c. This may lead to loss of availability.	2023-05-17	6.5	Medium
CVE-2023-20077	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to download arbitrary files from the filesystem of an affected device. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to download arbitrary files from the underlying filesystem of the affected device.	2023-05-18	6.5	Medium
CVE-2023-20087	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to download arbitrary files from the filesystem of an affected device. These vulnerabilities are due to insufficient input validation. An attacker could exploit these vulnerabilities by	2023-05-18	6.5	Medium

		sending crafted HTTP requests to an affected device. A successful exploit could allow the attacker to download arbitrary files from the underlying filesystem of the affected device.			
CVE-2023-20110	cisco - smart_software_manager_on-prem	A vulnerability in the web-based management interface of Cisco Smart Software Manager On-Prem (SSM On-Prem) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. This vulnerability exists because the web-based management interface inadequately validates user input. An attacker could exploit this vulnerability by authenticating to the application as a low-privileged user and sending crafted SQL queries to an affected system. A successful exploit could allow the attacker to read sensitive data on the underlying database.	2023-05-18	6.5	Medium
CVE-2023-20171	cisco - multiple products	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to delete or read arbitrary files on the underlying operating system. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	6.5	Medium
CVE-2023-33203	linux - linux_kernel	The Linux kernel before 6.2.9 has a race condition and resultant use-after-free in drivers/net/ethernet/qualcomm/emac/emac.c if a physically proximate attacker unplugs an emac based device.	2023-05-18	6.4	Medium
CVE-2023-2745	wordpress - multiple products	WordPress Core is vulnerable to Directory Traversal in versions up to, and including, 6.2, via the 'wp_lang' parameter. This allows unauthenticated attackers to access and load arbitrary translation files. In cases where an attacker is able to upload a crafted translation file onto the site, such as via an upload form, this could be also used to perform a Cross-Site Scripting attack.	2023-05-17	6.1	Medium
CVE-2023-20703	google - multiple products	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767853; Issue ID: ALPS07767853.	2023-05-15	5.5	Medium
CVE-2023-20704	google - multiple products	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767826; Issue ID: ALPS07767826.	2023-05-15	5.5	Medium
CVE-2023-20705	google - multiple products	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767870; Issue ID: ALPS07767870.	2023-05-15	5.5	Medium
CVE-2023-20706	google - multiple products	In apu, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07767860; Issue ID: ALPS07767860.	2023-05-15	5.5	Medium
CVE-2023-20914	google - android	In onSetRuntimePermissionGrantStateByDeviceAdmin of AdminRestrictedPermissionsUtils.java, there is a possible way for the work profile to read SMS messages due to a permissions bypass. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-189942529	2023-05-15	5.5	Medium
CVE-2023-20930	google - multiple products	In pushDynamicShortcut of ShortcutPackage.java, there is a possible way to get the device into a boot loop due to resource exhaustion. 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-250576066	2023-05-15	5.5	Medium
CVE-2023-21103	google - multiple products	In registerPhoneAccount of PhoneAccountRegistrar.java, uncaught exceptions in parsing persisted user data 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-259064622	2023-05-15	5.5	Medium
CVE-2023-21104	google - multiple products	In applySyncTransaction of WindowOrganizer.java, a missing permission check could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12L Android-13Android ID: A-259938771	2023-05-15	5.5	Medium
CVE-2023-21111	google - multiple products	In several functions of PhoneAccountRegistrar.java, there is a possible way to prevent an access to emergency services 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-256819769	2023-05-15	5.5	Medium
CVE-2023-21112	google - multiple products	In AnalyzeMfcResp of NxpMfcReader.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to	2023-05-15	5.5	Medium

		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-252763983			
CVE-2023-21118	google - multiple products	In unflattenString8 of Sensor.cpp, there is a possible out of bounds read due to a heap buffer overflow. 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-269014004	2023-05-15	5.5	Medium
CVE-2023-2700	redhat - libvirt	A vulnerability was found in libvirt. This security flaw ouccers due to repeatedly querying an SR-IOV PCI device's capabilities that exposes a memory leak caused by a failure to free the virPCIVirtualFunction array within the parent struct's g_autoptr cleanup.	2023-05-15	5.5	Medium
CVE-2023-2161	schneider-electric - multiple products	A CWE-611: Improper Restriction of XML External Entity Reference vulnerability exists that could cause unauthorized read access to the file system when a malicious configuration file is loaded on to the software by a local user.	2023-05-16	5.5	Medium
CVE-2023-1195	linux - multiple products	A use-after-free flaw was found in reconn_set_ipaddr_from_hostname in fs/cifs/connect.c in the Linux kernel. The issue occurs when it forgets to set the free pointer server->hostname to NULL, leading to an invalid pointer request.	2023-05-18	5.5	Medium
CVE-2023-28514	ibm - multiple products	IBM MQ 8.0, 9.0, and 9.1 could allow a local user to obtain sensitive credential information when a detailed technical error message is returned in a stack trace. IBM X-Force ID: 250398.	2023-05-19	5.5	Medium
CVE-2023-22878	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 244373.	2023-05-19	5.5	Medium
CVE-2023-28950	ibm - multiple products	IBM MQ 8.0, 9.0, 9.1, 9.2, and 9.3 could disclose sensitive user information from a trace file if that functionality has been enabled. IBM X-Force ID: 251358.	2023-05-19	5.5	Medium
CVE-2023-32977	jenkins - pipeline\	Jenkins Pipeline: Job Plugin does not escape the display name of the build that caused an earlier build to be aborted, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to set build display names immediately.	2023-05-16	5.4	Medium
CVE-2023-32984	jenkins - testng_results	Jenkins TestNG Results Plugin 730.v4c5283037693 and earlier does not escape several values that are parsed from TestNG report files and displayed on the plugin's test information pages, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to provide a crafted TestNG report file.	2023-05-16	5.4	Medium
CVE-2023-33002	jenkins - testcomplete_support	Jenkins TestComplete support Plugin 2.8.1 and earlier does not escape the TestComplete project name, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	2023-05-16	5.4	Medium
CVE-2023-33005	jenkins - wso2_oauth	Jenkins WSO2 Oauth Plugin 1.0 and earlier does not invalidate the previous session on login.	2023-05-16	5.4	Medium
CVE-2023-33007	jenkins - loadcomplete_support	Jenkins LoadComplete support Plugin 1.0 and earlier does not escape the LoadComplete test name, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Item/Configure permission.	2023-05-16	5.4	Medium
CVE-2023-28529	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 251213.	2023-05-19	5.4	Medium
CVE-2023-32983	jenkins - ansible	Jenkins Ansible Plugin 204.v8191fd551eb_f and earlier does not mask extra variables displayed on the configuration form, increasing the potential for attackers to observe and capture them.	2023-05-16	5.3	Medium
CVE-2023-20167	cisco - multiple products	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to perform path traversal attacks on the underlying operating system to either elevate privileges to root or read arbitrary files. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	4.9	Medium
CVE-2023-20172	cisco - multiple products	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to delete or read arbitrary files on the underlying operating system. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	4.9	Medium
CVE-2023-20173	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to read arbitrary files or conduct a server-side	2023-05-18	4.9	Medium

		request forgery (SSRF) attack through an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory.			
CVE-2023-20174	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to read arbitrary files or conduct a server-side request forgery (SSRF) attack through an affected device. To exploit these vulnerabilities, an attacker must have valid Administrator credentials on the affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	4.9	Medium
CVE-2023-32993	jenkins - saml_single_sign_on	Jenkins SAML Single Sign On(SSO) Plugin 2.0.2 and earlier does not perform hostname validation when connecting to miniOrange or the configured IdP to retrieve SAML metadata, which could be abused using a man-in-the-middle attack to intercept these connections.	2023-05-16	4.8	Medium
CVE-2023-1859	linux - multiple products	A use-after-free flaw was found in xen_9pfs_front_removet in net/9p/trans_xen.c in Xen transport for 9pfs in the Linux Kernel. This flaw could allow a local attacker to crash the system due to a race problem, possibly leading to a kernel information leak.	2023-05-17	4.7	Medium
CVE-2023-20697	google - multiple products	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07589148; Issue ID: ALPS07589148.	2023-05-15	4.4	Medium
CVE-2023-20698	google - multiple products	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07589144; Issue ID: ALPS07589144.	2023-05-15	4.4	Medium
CVE-2023-20709	google - multiple products	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07576951; Issue ID: ALPS07576951.	2023-05-15	4.4	Medium
CVE-2023-20710	google - multiple products	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07576935; Issue ID: ALPS07576935.	2023-05-15	4.4	Medium
CVE-2023-20711	google - multiple products	In keyinstall, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07581668; Issue ID: ALPS07581668.	2023-05-15	4.4	Medium
CVE-2023-20719	google - multiple products	In pqframework, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07629583; Issue ID: ALPS07629583.	2023-05-15	4.4	Medium
CVE-2023-32978	jenkins - lightweight_directory_access_protocol	A cross-site request forgery (CSRF) vulnerability in Jenkins LDAP Plugin allows attackers to connect to an attacker-specified LDAP server using attacker-specified credentials.	2023-05-16	4.3	Medium
CVE-2023-32979	jenkins - email_extension	Jenkins Email Extension Plugin does not perform a permission check in a method implementing form validation, allowing attackers with Overall/Read permission to check for the existence of files in the email-templates/ directory in the Jenkins home directory on the controller file system.	2023-05-16	4.3	Medium
CVE-2023-32980	jenkins - email_extension	A cross-site request forgery (CSRF) vulnerability in Jenkins Email Extension Plugin allows attackers to make another user stop watching an attacker-specified job.	2023-05-16	4.3	Medium
CVE-2023-32982	jenkins - ansible	Jenkins Ansible Plugin 204.v8191fd551eb_f and earlier stores extra variables unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	2023-05-16	4.3	Medium
CVE-2023-32985	jenkins - sidebar_link	Jenkins Sidebar Link Plugin 2.2.1 and earlier does not restrict the path of files in a method implementing form validation, allowing attackers with Overall/Read permission to check for the existence of an attacker-specified file path on the Jenkins controller file system.	2023-05-16	4.3	Medium
CVE-2023-32988	jenkins - azure_vm_agents	A missing permission check in Jenkins Azure VM Agents Plugin 852.v8d35f0960a_43 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	2023-05-16	4.3	Medium
CVE-2023-33003	jenkins - tag_profiler	A cross-site request forgery (CSRF) vulnerability in Jenkins Tag Profiler Plugin 0.2 and earlier allows attackers to reset profiler statistics.	2023-05-16	4.3	Medium

CVE-2023-33004	jenkins - tag_profiler	A missing permission check in Jenkins Tag Profiler Plugin 0.2 and earlier allows attackers with Overall/Read permission to reset profiler statistics.	2023-05-16	4.3	Medium
CVE-2023-2196	jenkins - code_dx	A missing permission check in Jenkins Code Dx Plugin 3.1.0 and earlier allows attackers with Item/Read permission to check for the existence of an attacker-specified file path on an agent file system.	2023-05-16	4.3	Medium
CVE-2023-2632	jenkins - code_dx	Jenkins Code Dx Plugin 3.1.0 and earlier stores Code Dx server API keys unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission or access to the Jenkins controller file system.	2023-05-16	4.3	Medium
CVE-2023-2633	jenkins - code_dx	Jenkins Code Dx Plugin 3.1.0 and earlier does not mask Code Dx server API keys displayed on the configuration form, increasing the potential for attackers to observe and capture them.	2023-05-16	4.3	Medium
CVE-2023-2631	jenkins - code_dx	A missing permission check in Jenkins Code Dx Plugin 3.1.0 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified URL.	2023-05-16	4.3	Medium
CVE-2023-30510	arubanetworks - multiple products	A vulnerability exists in the Aruba EdgeConnect Enterprise web management interface that allows remote authenticated users to issue arbitrary URL requests from the Aruba EdgeConnect Enterprise instance. The impact of this vulnerability is limited to a subset of URLs which can result in the possible disclosure of data due to the network position of the Aruba EdgeConnect Enterprise instance.	2023-05-16	4.3	Medium
CVE-2023-20183	cisco - multiple products	Multiple vulnerabilities in the API of Cisco DNA Center Software could allow an authenticated, remote attacker to read information from a restricted container, enumerate user information, or execute arbitrary commands in a restricted container as the root user. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	4.3	Medium
CVE-2023-20184	cisco - dna_center	Multiple vulnerabilities in the API of Cisco DNA Center Software could allow an authenticated, remote attacker to read information from a restricted container, enumerate user information, or execute arbitrary commands in a restricted container as the root user. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	4.3	Medium
CVE-2023-20717	google - multiple products	In vcu, there is a possible leak of dma buffer due to a race condition. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07645185; Issue ID: ALPS07645185.	2023-05-15	4.1	Medium
CVE-2023-20106	cisco - multiple products	Multiple vulnerabilities in Cisco Identity Services Engine (ISE) could allow an authenticated attacker to delete or read arbitrary files on the underlying operating system. To exploit these vulnerabilities, an attacker must have valid credentials on an affected device. For more information about these vulnerabilities, see the Details section of this advisory.	2023-05-18	3.8	Low
CVE-2023-2195	jenkins - code_dx	A cross-site request forgery (CSRF) vulnerability in Jenkins Code Dx Plugin 3.1.0 and earlier allows attackers to connect to an attacker-specified URL.	2023-05-16	3.5	Low
CVE-2022-35798	microsoft - azure_arc_jumpstart	Azure Arc Jumpstart Information Disclosure Vulnerability	2023-05-18	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.