الهيئــة الوطنيــة
للأمــن السيبــرانى
Nat onal 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 1st of April to 8th of April. 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 ١ أبريل إلى ٨ أبريل. 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-2023-27284	ibm - multiple products	IBM Aspera Cargo 4.2.5 and IBM Aspera Connect 4.2.5 are vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow a buffer and execute arbitrary code on the system. IBM X-Force ID: 248616.	2023-04-02	9.8	Critical
CVE-2023-27286	ibm - multiple products	IBM Aspera Cargo 4.2.5 and IBM Aspera Connect 4.2.5 are vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow a buffer and execute arbitrary code on the system. IBM X-Force ID: 248616.	2023-04-02	9.8	Critical
CVE-2023-28668	jenkins - role-based_authorization_strategy	Jenkins Role-based Authorization Strategy Plugin 587.v2872c41fa_e51 and earlier grants permissions even after they've been disabled.	2023-04-02	9.8	Critical
CVE-2023-28677	jenkins - convert_to_pipeline	Jenkins Convert To Pipeline Plugin 1.0 and earlier uses basic string concatenation to convert Freestyle projects' Build Environment, Build Steps, and Post-build Actions to the equivalent Pipeline step invocations, allowing attackers able to configure Freestyle projects to prepare a crafted configuration that injects Pipeline script code into the (unsandboxed) Pipeline resulting from a convertion by Jenkins Convert To Pipeline Plugin.	2023-04-02	9.8	Critical
CVE-2023-1671	sophos - web_appliance	A pre-auth command injection vulnerability in the warn-proceed handler of Sophos Web Appliance older than version 4.3.10.4 allows execution of arbitrary code.	2023-04-04	9.8	Critical
CVE-2023-28613	samsung - exynos_1280_firmware	An issue was discovered in Samsung Exynos Mobile Processor and Baseband Modem Processor for Exynos 1280, Exynos 2200, and Exynos Modem 5300. An integer overflow in IPv4 fragment handling can occur due to insufficient parameter validation when reassembling these fragments.	2023-04-04	9.8	Critical
CVE-2023-20073	cisco - rv340_firmware	A vulnerability in the web-based management interface of Cisco RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to upload arbitrary files to an affected device. This vulnerability is due to insufficient authorization enforcement mechanisms in the context of file uploads. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to upload arbitrary files to the affected device.	2023-04-05	9.8	Critical
CVE-2023-28500	adobe - livecycle_es4	** UNSUPPORTED WHEN ASSIGNED ** A Java insecure deserialization vulnerability in Adobe LiveCycle ES4 version 11.0 and earlier allows unauthenticated remote attackers to gain operating system code execution by submitting specially crafted Java serialized objects to a specific URL. Adobe LiveCycle ES4 version 11.0.1 and later may be vulnerable if the application is installed with Java environment 7u21 and earlier. Exploitation of the vulnerability depends on two factors: insecure deserialization methods used in the Adobe LiveCycle application, and the use of Java environments 7u21 and earlier. The code execution is performed in the context of the account that is running the Adobe LiveCycle application. If the account is privileged, exploitation provides privileged access to the operating system. NOTE: This	2023-04-06	9.8	Critical

		vulnerability only affects products that are no longer supported by the maintainer.			
CVE-2023-28706	apache - airflow_hive_provider	Improper Control of Generation of Code ('Code Injection') vulnerability in Apache Software Foundation Apache Airflow Hive Provider.This issue affects Apache Airflow Hive Provider: before 6.0.0.	2023-04-07	9.8	Critical
CVE-2023-28674	jenkins - octoperf_load_testing	A cross-site request forgery (CSRF) vulnerability in Jenkins OctoPerf Load Testing Plugin Plugin 4.5.2 and earlier allows attackers to connect to a previously configured Octoperf server using attacker-specified credentials.	2023-04-02	8.8	High
CVE-2023-28676	jenkins - convert_to_pipeline	A cross-site request forgery (CSRF) vulnerability in Jenkins Convert To Pipeline Plugin 1.0 and earlier allows attackers to create a Pipeline based on a Freestyle project, potentially leading to remote code execution (RCE).	2023-04-02	8.8	High
CVE-2023-1810	google - chrome	Heap buffer overflow in Visuals in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-04-04	8.8	High
CVE-2023-1811	google - chrome	Use after free in Frames in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-04-04	8.8	High
CVE-2023-1812	google - chrome	Out of bounds memory access in DOM Bindings in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	2023-04-04	8.8	High
CVE-2023-1815	google - chrome	Use after free in Networking APIs in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2023-04-04	8.8	High
CVE-2023-1818	google - chrome	Use after free in Vulkan in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2023-04-04	8.8	High
CVE-2023-1820	google - chrome	Heap buffer overflow in Browser History in Google Chrome prior to 112.0.5615.49 allowed a remote attacker who convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2023-04-04	8.8	High
CVE-2023-20102	cisco - secure_network_analytics	A vulnerability in the web-based management interface of Cisco Secure Network Analytics could allow an authenticated, remote attacker to execute arbitrary code on the underlying operating system. This vulnerability is due to insufficient sanitization of user-provided data that is parsed into system memory. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system as the administrator user.	2023-04-05	8.8	High
CVE-2023-28681	jenkins - visual_studio_code_metrics	Jenkins Visual Studio Code Metrics Plugin 1.7 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2023-04-02	8.2	High
CVE-2023-28682	jenkins - performance_publisher	Jenkins Performance Publisher Plugin 8.09 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2023-04-02	8.2	High
CVE-2023-28683	jenkins - phabricator_differential	Jenkins Phabricator Differential Plugin 2.1.5 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2023-04-02	8.2	High
CVE-2022-33959	ibm - sterling_order_management	IBM Sterling Order Management 10.0 could allow a user to bypass validation and perform unauthorized actions on behalf of other users. IBM X-Force ID: 229320.	2023-04-07	8.1	High
CVE-2023-26269	apache - james	Apache James server version 3.7.3 and earlier provides a JMX management service without authentication by default. This allows privilege escalation by a malicious local user. Administrators are advised to disable JMX, or set up a JMX password. Note that version 3.7.4 onward will set up a JMX password automatically for Guice users.	2023-04-03	7.8	High
CVE-2023-0975	trellix - agent	A vulnerability exists in Trellix Agent for Windows version 5.7.8 and earlier, that allows local users, during install/upgrade workflow, to replace one of the Agent’s executables before it can be executed. This allows the user to elevate their permissions.	2023-04-03	7.8	High
CVE-2023-1579	gnu - binutils	Heap based buffer overflow in binutils-gdb/bfd/libbfd.c in bfd_getl64.	2023-04-03	7.8	High
CVE-2023-25940	dell - emc_powerscale_onefs	Dell PowerScale OneFS version 9.5.0.0 contains improper link resolution before file access vulnerability in isi_gather_info. A low privilege local attacker could potentially exploit this vulnerability, leading to system takeover and it breaks the compliance mode guarantees.	2023-04-04	7.8	High
CVE-2023-25941	dell - multiple products	Dell PowerScale OneFS versions 8.2.x-9.5.0.x contain an elevation of privilege vulnerability. A low-privileged local attacker could	2023-04-04	7.8	High

		potentially exploit this vulnerability, leading to Denial of service, escalation of privileges, and information disclosure. This vulnerability breaks the compliance mode guarantee.			
CVE-2023-20122	cisco - identity_services_engine	Multiple vulnerabilities in the restricted shell of Cisco Evolved Programmable Network Manager (EPNM), Cisco Identity Services Engine (ISE), and Cisco Prime Infrastructure could allow an authenticated, local attacker to escape the restricted shell and gain root privileges on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory.	2023-04-05	7.8	High
CVE-2023-20655	google - multiple products	In mmsdk, there is a possible escalation of privilege due to a parcel format mismatch. This could lead to local code execution with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07203022; Issue ID: ALPS07203022.	2023-04-06	7.8	High
CVE-2023-28051	dell - power_manager	Dell Power Manager, versions 3.10 and prior, contains an Improper Access Control vulnerability. A low-privileged attacker could potentially exploit this vulnerability to elevate privileges on the system.	2023-04-07	7.8	High
CVE-2023-28680	jenkins - crap4j	Jenkins Crap4J Plugin 0.9 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2023-04-02	7.5	High
CVE-2023-28625	apache - http_server	mod_auth_openidc is an authentication and authorization module for the Apache 2.x HTTP server that implements the OpenID Connect Relying Party functionality. In versions 2.0.0 through 2.4.13.1, when `OIDCStripCookies` is set and a crafted cookie supplied, a NULL pointer dereference would occur, resulting in a segmentation fault. This could be used in a Denial-of-Service attack and thus presents an availability risk. Version 2.4.13.2 contains a patch for this issue. As a workaround, avoid using `OIDCStripCookies`.	2023-04-03	7.5	High
CVE-2023-20051	cisco - packet_data_network_gateway	A vulnerability in the Vector Packet Processor (VPP) of Cisco Packet Data Network Gateway (PGW) could allow an unauthenticated, remote attacker to stop ICMP traffic from being processed over an IPsec connection. This vulnerability is due to the VPP improperly handling a malformed packet. An attacker could exploit this vulnerability by sending a malformed Encapsulating Security Payload (ESP) packet over an IPsec connection. A successful exploit could allow the attacker to stop ICMP traffic over an IPsec connection and cause a denial of service (DoS).	2023-04-05	7.5	High
CVE-2023-28342	zohocorp - multiple products	Zoho ManageEngine ADSelfService Plus before 6218 allows anyone to conduct a Denial-of-Service attack via the Mobile App Authentication API.	2023-04-05	7.5	High
CVE-2022-34333	ibm - sterling_order_management	IBM Sterling Order Management 10.0 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 229698.	2023-04-07	7.5	High
CVE-2023-28707	apache - airflow_drill_provider	Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow Drill Provider.This issue affects Apache Airflow Drill Provider: before 2.3.2.	2023-04-07	7.5	High
CVE-2023-28710	apache - airflow_spark_provider	Improper Input Validation vulnerability in Apache Software Foundation Apache Airflow Spark Provider.This issue affects Apache Airflow Spark Provider: before 4.0.1.	2023-04-07	7.5	High
CVE-2022-4934	sophos - web_appliance	A post-auth command injection vulnerability in the exception wizard of Sophos Web Appliance older than version 4.3.10.4 allows administrators to execute arbitrary code.	2023-04-04	7.2	High
CVE-2023-20124	cisco - rv016_firmware	A vulnerability in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an authenticated, remote attacker to execute arbitrary commands on an affected device. This vulnerability is due to improper validation of user input within incoming HTTP packets. An attacker could exploit this vulnerability by sending a crafted HTTP request to the web-based management interface. A successful exploit could allow the attacker to gain root-level privileges and access unauthorized data. To exploit this vulnerability, an attacker would need to have valid administrative credentials on the affected device. Cisco has not released software updates that address this vulnerability.	2023-04-05	7.2	High
CVE-2023-20128	cisco - rv320_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands as the root user on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. Cisco has not released software updates to address these vulnerabilities.	2023-04-05	7.2	High

CVE-2023-20103	cisco - secure_network_analytics	A vulnerability in Cisco Secure Network Analytics could allow an authenticated, remote attacker to execute arbitrary code as a root user on an affected device. This vulnerability is due to insufficient validation of user input to the web interface. An attacker could exploit this vulnerability by uploading a crafted file to an affected device. A successful exploit could allow the attacker to execute code on the affected device. To exploit this vulnerability, an attacker would need to have valid Administrator credentials on the affected device.	2023-04-05	7.2	High
CVE-2023-20117	cisco - rv320_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV320 and RV325 Dual Gigabit WAN VPN Routers could allow an authenticated, remote attacker to inject and execute arbitrary commands on the underlying operating system of an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by sending malicious input to an affected device. A successful exploit could allow the attacker to execute arbitrary commands as the root user on the underlying Linux operating system of the affected device. To exploit these vulnerabilities, an attacker would need to have valid Administrator credentials on the affected device. Cisco has not released software updates to address these vulnerabilities.	2023-04-05	7.2	High
CVE-2023-1838	linux - linux_kernel	A use-after-free flaw was found in vhost_net_set_backend in drivers/vhost/net.c in virtio network subcomponent in the Linux kernel due to a double fget. This flaw could allow a local attacker to crash the system, and could even lead to a kernel information leak problem.	2023-04-05	7.1	High
CVE-2023-28046	dell - display_manager	Dell Display Manager, versions 2.1.0 and prior, contains an arbitrary file or folder deletion vulnerability during uninstallation A local low privilege attacker could potentially exploit this vulnerability, leading to the deletion of arbitrary files on the operating system with high privileges.	2023-04-06	7.1	High
CVE-2023-27876	ibm - tririga_application_platform	IBM TRIRIGA 4.0 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 249975.	2023-04-07	7.1	High
CVE-2023-20021	cisco - identity_services_engine	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local 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 Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	2023-04-05	6.7	Medium
CVE-2023-20022	cisco - identity_services_engine	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local 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 Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	2023-04-05	6.7	Medium
CVE-2023-20023	cisco - identity_services_engine	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local 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 Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	2023-04-05	6.7	Medium
CVE-2023-20152	cisco - identity_services_engine	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local 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 Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	2023-04-05	6.7	Medium
CVE-2023-20121	cisco - multiple products	Multiple vulnerabilities in the restricted shell of Cisco Evolved Programmable Network Manager (EPNM), Cisco Identity Services Engine (ISE), and Cisco Prime Infrastructure could allow an authenticated, local attacker to escape the restricted shell and	2023-04-05	6.7	Medium

		gain root privileges on the underlying operating system. For more information about these vulnerabilities, see the Details section of this advisory.			
CVE-2023-20153	cisco - identity_services_engine	Multiple vulnerabilities in specific Cisco Identity Services Engine (ISE) CLI commands could allow an authenticated, local 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 Administrator privileges on the affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by submitting a crafted CLI command. A successful exploit could allow the attacker to elevate privileges to root.	2023-04-05	6.7	Medium
CVE-2022-32599	google - multiple products	In rpmb, 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: ALPS07460390; Issue ID: ALPS07460390.	2023-04-06	6.7	Medium
CVE-2023-20652	google - multiple products	In keyinstall, 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: ALPS07628168; Issue ID: ALPS07589135.	2023-04-06	6.7	Medium
CVE-2023-20653	google - multiple products	In keyinstall, 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: ALPS07628168; Issue ID: ALPS07589144.	2023-04-06	6.7	Medium
CVE-2023-20654	google - multiple products	In keyinstall, 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: ALPS07628168; Issue ID: ALPS07589148.	2023-04-06	6.7	Medium
CVE-2023-20656	google - multiple products	In geniezone, 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: ALPS07571494; Issue ID: ALPS07571494.	2023-04-06	6.7	Medium
CVE-2023-20657	google - multiple products	In mtee, 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: ALPS07571485; Issue ID: ALPS07571485.	2023-04-06	6.7	Medium
CVE-2023-20658	google - multiple products	In isp, 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: ALPS07537393; Issue ID: ALPS07180396.	2023-04-06	6.7	Medium
CVE-2023-20659	google - multiple products	In wlan, 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: ALPS07588413; Issue ID: ALPS07588413.	2023-04-06	6.7	Medium
CVE-2023-20661	google - multiple products	In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560782; Issue ID: ALPS07560782.	2023-04-06	6.7	Medium
CVE-2023-20662	google - multiple products	In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560765; Issue ID: ALPS07560765.	2023-04-06	6.7	Medium
CVE-2023-20663	google - multiple products	In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07560741; Issue ID: ALPS07560741.	2023-04-06	6.7	Medium
CVE-2023-20664	google - multiple products	In gz, there is a possible double free due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07505952; Issue ID: ALPS07505952.	2023-04-06	6.7	Medium
CVE-2023-20666	google - multiple products	In display drm, 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: ALPS07310651; Issue ID: ALPS07292173.	2023-04-06	6.7	Medium
CVE-2023-20670	google - multiple products	In audio, 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	2023-04-06	6.7	Medium

		needed for exploitation. Patch ID: ALPS07648710; Issue ID: ALPS07648710.			
CVE-2023-20680	google - multiple products	In adsp, 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: ALPS07664785; Issue ID: ALPS07664785.	2023-04-06	6.7	Medium
CVE-2023-20681	google - multiple products	In adsp, 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: ALPS07696134; Issue ID: ALPS07696134.	2023-04-06	6.7	Medium
CVE-2023-20682	google - multiple products	In wlan, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07441605; Issue ID: ALPS07441605.	2023-04-06	6.7	Medium
CVE-2023-28672	jenkins - octoperf_load_testing	Jenkins OctoPerf Load Testing Plugin Plugin 4.5.1 and earlier does not perform a permission check in a connection test HTTP endpoint, allowing attackers with Overall/Read permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	2023-04-02	6.5	Medium
CVE-2023-28684	jenkins - remote-jobs-view	Jenkins remote-jobs-view-plugin Plugin 0.0.3 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2023-04-02	6.5	Medium
CVE-2023-0977	trellix - agent	A heap-based overflow vulnerability in Trellix Agent (Windows and Linux) version 5.7.8 and earlier, allows a remote user to alter the page heap in the macmnsvc process memory block resulting in the service becoming unavailable.	2023-04-03	6.5	Medium
CVE-2023-0614	samba - multiple products	The fix in 4.6.16, 4.7.9, 4.8.4 and 4.9.7 for CVE-2018-10919 Confidential attribute disclosure vi LDAP filters was insufficient and an attacker may be able to obtain confidential BitLocker recovery keys from a Samba AD DC.	2023-04-03	6.5	Medium
CVE-2023-25942	dell - multiple products	Dell PowerScale OneFS versions 8.2.x-9.4.x contain an uncontrolled resource consumption vulnerability. A malicious network user with low privileges could potentially exploit this vulnerability in SMB, leading to a potential denial of service.	2023-04-04	6.5	Medium
CVE-2023-1813	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 112.0.5615.49 allowed an attacker who convinced a user to install a malicious extension to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Medium)	2023-04-04	6.5	Medium
CVE-2023-1814	google - chrome	Insufficient validation of untrusted input in Safe Browsing in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass download checking via a crafted HTML page. (Chromium security severity: Medium)	2023-04-04	6.5	Medium
CVE-2023-1816	google - chrome	Incorrect security UI in Picture In Picture in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially perform navigation spoofing via a crafted HTML page. (Chromium security severity: Medium)	2023-04-04	6.5	Medium
CVE-2023-1817	google - chrome	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 112.0.5615.49 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2023-04-04	6.5	Medium
CVE-2023-1819	google - chrome	Out of bounds read in Accessibility in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	2023-04-04	6.5	Medium
CVE-2023-1821	google - chrome	Inappropriate implementation in WebShare in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to potentially hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Low)	2023-04-04	6.5	Medium
CVE-2023-1822	google - chrome	Incorrect security UI in Navigation in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	2023-04-04	6.5	Medium
CVE-2023-1823	google - chrome	Inappropriate implementation in FedCM in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2023-04-04	6.5	Medium
CVE-2023-20127	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow a remote attacker to obtain privileged information and conduct cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory.	2023-04-05	6.5	Medium
CVE-2023-20129	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow a remote attacker to obtain	2023-04-05	6.5	Medium

		privileged information and conduct cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory.			
CVE-2023-20130	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow a remote attacker to obtain privileged information and conduct cross-site scripting (XSS) and cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory.	2023-04-05	6.5	Medium
CVE-2023-20134	cisco - webex_meetings	Multiple vulnerabilities in the web interface of Cisco Webex Meetings could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack or upload arbitrary files as recordings. For more information about these vulnerabilities, see the Details section of this advisory.	2023-04-05	6.5	Medium
CVE-2022-43928	ibm - multiple products	The IBM Toolbox for Java (Db2 Mirror for i 7.4 and 7.5) could allow a user to obtain sensitive information, caused by utilizing a Java string for processing. Since Java strings are immutable, their contents exist in memory until garbage collected. This means sensitive data could be visible in memory over an indefinite amount of time. IBM has addressed this issue by reducing the amount of time the sensitive data is visible in memory. IBM X-Force ID: 241675.	2023-04-07	6.5	Medium
CVE-2023-20684	google - multiple products	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07671069; Issue ID: ALPS07671069.	2023-04-06	6.4	Medium
CVE-2023-20685	google - multiple products	In vdec, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07608575; Issue ID: ALPS07608575.	2023-04-06	6.4	Medium
CVE-2023-20686	google - multiple products	In display drm, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570826; Issue ID: ALPS07570826.	2023-04-06	6.4	Medium
CVE-2023-20687	google - multiple products	In display drm, there is a possible double free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07570772; Issue ID: ALPS07570772.	2023-04-06	6.4	Medium
CVE-2023-1611	linux - linux_kernel	A use-after-free flaw was found in btrfs_search_slot in fs/btrfs/ctree.c in btrfs in the Linux Kernel.This flaw allows an attacker to crash the system and possibly cause a kernel information lea	2023-04-03	6.3	Medium
CVE-2023-1855	linux - multiple products	A use-after-free flaw was found in xgene_hwmon_remove in drivers/hwmon/xgene-hwmon.c in the Hardware Monitoring Linux Kernel Driver (xgene-hwmon). This flaw could allow a local attacker to crash the system due to a race problem. This vulnerability could even lead to a kernel information leak problem.	2023-04-05	6.3	Medium
CVE-2023-26789	veritas - netbackup_opscenter	Veritas NetBackUp OpsCenter Version 9.1.0.1 is vulnerable to Reflected Cross-site scripting (XSS). The Web App fails to adequately sanitize special characters. By leveraging this issue, an attacker is able to cause arbitrary HTML and JavaScript code to be executed in a user's browser.	2023-04-05	6.1	Medium
CVE-2023-20068	cisco - prime_infrastructure	A vulnerability in the web-based management interface of Cisco Prime Infrastructure Software could allow an unauthenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by persuading a user of the web-based management interface on an affected device to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or to access sensitive, browser-based information.	2023-04-05	6.1	Medium
CVE-2023-20137	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVE-2023-20138	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and	2023-04-05	6.1	Medium

		RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.			
CVE-2023-20139	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVE-2023-20140	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVE-2023-20141	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVE-2023-20142	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVE-2023-20143	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVE-2023-20144	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the	2023-04-05	6.1	Medium

		interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.			
CVE-2023-20145	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVE-2023-20146	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVE-2023-20147	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVE-2023-20148	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVE-2023-20149	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVE-2023-20150	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker	2023-04-05	6.1	Medium

		could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.			
CVE-2023-20151	cisco - rv016_firmware	Multiple vulnerabilities in the web-based management interface of Cisco Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers could allow an unauthenticated, remote attacker to conduct cross-site scripting (XSS) attacks against a user of the interface. These vulnerabilities are due to insufficient input validation by the web-based management interface. An attacker could exploit these vulnerabilities by sending crafted HTTP requests to an affected device and then persuading a user to visit specific web pages that include malicious payloads. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. Cisco has not released software updates that address these vulnerabilities.	2023-04-05	6.1	Medium
CVE-2023-20030	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to access sensitive information, conduct a server-side request forgery (SSRF) attack through an affected device, or negatively impact the responsiveness of the web-based management interface itself. This vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by uploading a crafted XML file that contains references to external entities. A successful exploit could allow the attacker to retrieve files from the local system, resulting in the disclosure of confidential information. A successful exploit could also cause the web application to perform arbitrary HTTP requests on behalf of the attacker or consume memory resources to reduce the availability of the web-based management interface. To successfully exploit this vulnerability, an attacker would need valid Super Admin or Policy Admin credentials.	2023-04-05	6	Medium
CVE-2023-0922	samba - multiple products	The Samba AD DC administration tool, when operating against a remote LDAP server, will by default send new or reset passwords over a signed-only connection.	2023-04-03	5.9	Medium
CVE-2023-26283	ibm - websphere_application_server	IBM WebSphere Application Server 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 248416.	2023-04-02	5.4	Medium
CVE-2023-28669	jenkins - jacoco	Jenkins JaCoCo Plugin 3.3.2 and earlier does not escape class and method names shown on the UI, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control input files for the 'Record JaCoCo coverage report' post-build action.	2023-04-02	5.4	Medium
CVE-2023-28670	jenkins - pipeline_aggregator_view	Jenkins Pipeline Aggregator View Plugin 1.13 and earlier does not escape a variable representing the current view's URL in inline JavaScript, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by authenticated attackers with Overall/Read permission.	2023-04-02	5.4	Medium
CVE-2023-28678	jenkins - cppcheck	Jenkins Cppcheck Plugin 1.26 and earlier does not escape file names from Cppcheck report files before showing them on the Jenkins UI, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control report file contents.	2023-04-02	5.4	Medium
CVE-2023-28679	jenkins - mashup_portlets	Jenkins Mashup Portlets Plugin 1.1.2 and earlier provides the "Generic JS Portlet" feature that lets a user populate a portlet using a custom JavaScript expression, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by authenticated attackers with Overall/Read permission.	2023-04-02	5.4	Medium
CVE-2020-36692	sophos - web_appliance	A reflected XSS via POST vulnerability in report scheduler of Sophos Web Appliance versions older than 4.3.10.4 allows execution of JavaScript code in the victim browser via a malicious form that must be manually submitted by the victim while logged in to SWA.	2023-04-04	5.4	Medium
CVE-2023-28069	dell - streaming_data_platform	Dell Streaming Data Platform prior to 1.4 contains Open Redirect vulnerability. An attacker with privileges same as a legitimate user can phish the legitimate the user to redirect to malicious website leading to information disclosure and launch of phishing attacks.	2023-04-05	5.4	Medium
CVE-2023-20131	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow a remote attacker to obtain privileged information and conduct cross-site scripting (XSS) and	2023-04-05	5.4	Medium

		cross-site request forgery (CSRF) attacks. For more information about these vulnerabilities, see the Details section of this advisory.			
CVE-2023-20132	cisco - webex_meetings	Multiple vulnerabilities in the web interface of Cisco Webex Meetings could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack or upload arbitrary files as recordings. For more information about these vulnerabilities, see the Details section of this advisory.	2023-04-05	5.4	Medium
CVE-2023-20096	cisco - unified_contact_center_express	A vulnerability in the web-based management interface of Cisco Unified Contact Center Express (Unified CCX) could allow an authenticated, remote attacker to perform a stored cross-site scripting (XSS) attack. This vulnerability is due to insufficient input validation of user-supplied data. An attacker could exploit this vulnerability by entering crafted text into various input fields within the web-based management interface. A successful exploit could allow the attacker to perform a stored XSS attack, which could allow the execution of scripts within the context of other users of the interface.	2023-04-05	5.4	Medium
CVE-2022-43914	ibm - tririga_application_platform	IBM TRIRIGA Application Platform 4.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 241036.	2023-04-07	5.4	Medium
CVE-2023-1582	linux - multiple products	A race problem was found in fs/proc/task_mmu.c in the memory management sub-component in the Linux kernel. This issue may allow a local attacker with user privilege to cause a denial of service.	2023-04-05	4.7	Medium
CVE-2023-20123	cisco - multiple products	A vulnerability in the offline access mode of Cisco Duo Two-Factor Authentication for macOS and Duo Authentication for Windows Logon and RDP could allow an unauthenticated, physical attacker to replay valid user session credentials and gain unauthorized access to an affected macOS or Windows device. This vulnerability exists because session credentials do not properly expire. An attacker could exploit this vulnerability by replaying previously used multifactor authentication (MFA) codes to bypass MFA protection. A successful exploit could allow the attacker to gain unauthorized access to the affected device.	2023-04-05	4.6	Medium
CVE-2023-20660	google - multiple products	In wlan, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07588383; Issue ID: ALPS07588383.	2023-04-06	4.4	Medium
CVE-2023-20665	google - multiple products	In ril, 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: ALPS07628604; Issue ID: ALPS07628604.	2023-04-06	4.4	Medium
CVE-2023-20674	google - multiple products	In wlan, 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: ALPS07588569; Issue ID: ALPS07588552.	2023-04-06	4.4	Medium
CVE-2023-20675	google - multiple products	In wlan, 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: ALPS07588569; Issue ID: ALPS07588569.	2023-04-06	4.4	Medium
CVE-2023-20676	google - multiple products	In wlan, 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: ALPS07588569; Issue ID: ALPS07628518.	2023-04-06	4.4	Medium
CVE-2023-20677	google - multiple products	In wlan, 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: ALPS07588413; Issue ID: ALPS07588436.	2023-04-06	4.4	Medium
CVE-2023-20679	google - multiple products	In wlan, 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: ALPS07588413; Issue ID: ALPS07588453.	2023-04-06	4.4	Medium
CVE-2023-20688	google - multiple products	In power, 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: ALPS07441821; Issue ID: ALPS07441821.	2023-04-06	4.4	Medium
CVE-2023-28671	jenkins - octoperf_load_testing	A cross-site request forgery (CSRF) vulnerability in Jenkins OctoPerf Load Testing Plugin Plugin 4.5.0 and earlier allows attackers to connect to an attacker-specified URL using attacker-	2023-04-02	4.3	Medium

		specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.			
CVE-2023-28673	jenkins - octoperf_load_testing	A missing permission check in Jenkins OctoPerf Load Testing Plugin Plugin 4.5.2 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	2023-04-02	4.3	Medium
CVE-2023-28675	jenkins - octoperf_load_testing	A missing permission check in Jenkins OctoPerf Load Testing Plugin Plugin 4.5.2 and earlier allows attackers to connect to a previously configured Octoperf server using attacker-specified credentials.	2023-04-02	4.3	Medium
CVE-2023-0225	samba - multiple products	A flaw was found in Samba. An incomplete access check on dnsHostName allows authenticated but otherwise unprivileged users to delete this attribute from any object in the directory.	2023-04-03	4.3	Medium

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.