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 13th of August to 19th of August. 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 ١٣ أغسطس إلى ١٩ أغسطس. 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-2023-39405	huawei - multiple products	Vulnerability of out-of-bounds parameter read/write in the Wi-Fi module. Successful exploitation of this vulnerability may cause other apps to be executed with escalated privileges.	2023-08-13	9.8	Critical
CVE-2023-32748	mitel - mivoice_connect	The Linux DVS server component of Mitel MiVoice Connect through 19.3 SP2 (22.24.1500.0) could allow an unauthenticated attacker with internal network access to execute arbitrary scripts due to improper access control.	2023-08-14	9.8	Critical
CVE-2023-39292	mitel - multiple products	A SQL Injection vulnerability has been identified in the MiVoice Office 400 SMB Controller through 1.2.5.23 which could allow a malicious actor to access sensitive information and execute arbitrary database and management operations.	2023-08-14	9.8	Critical
CVE-2023-39293	mitel - multiple products	A Command Injection vulnerability has been identified in the MiVoice Office 400 SMB Controller through 1.2.5.23 which could allow a malicious actor to execute arbitrary commands within the context of the system.	2023-08-14	9.8	Critical
CVE-2023-20965	google - android	In processMessageImpl of ClientModeImpl.java, there is a possible credential disclosure in the TOFU flow due to a logic error in the code. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	9.8	Critical
CVE-2023-21242	google - android	In isServerCertChainValid of InsecureEapNetworkHandler.java, there is a possible way to trust an imposter server due to a logic error in the code. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	9.8	Critical
CVE-2023-21287	google - multiple products	In multiple locations, there is a possible code execution due to type confusion. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	9.8	Critical
CVE-2023-35082	ivanti - endpoint_manager_mobile	An authentication bypass vulnerability in Ivanti EPMM 11.10 and older, allows unauthorized users to access restricted functionality or resources of the application without proper authentication. This vulnerability is unique to CVE-2023-35078 announced earlier.	2023-08-15	9.8	Critical
CVE-2023-32493	dell - powerscale_onefs	Dell PowerScale OneFS, 9.5.0.x, contains a protection mechanism bypass vulnerability. An unprivileged, remote attacker could potentially exploit this vulnerability, leading to denial of service, information disclosure and remote execution.	2023-08-16	9.8	Critical
CVE-2021-46895	huawei - multiple products	Vulnerability of defects introduced in the design process in the Multi-Device Task Center. Successful exploitation of this vulnerability will cause the hopped app to bypass the app lock and reset the device that initiates the hop.	2023-08-13	9.1	Critical
CVE-2023-39385	huawei - multiple products	Vulnerability of configuration defects in the media module of certain products.. Successful exploitation of this vulnerability may cause unauthorized access.	2023-08-13	9.1	Critical
CVE-2023-39398	huawei - multiple products	Parameter verification vulnerability in the installd module. Successful exploitation of this vulnerability may cause sandbox files to be read and written without authorization.	2023-08-13	9.1	Critical

CVE-2023-39399	huawei - multiple products	Parameter verification vulnerability in the installd module. Successful exploitation of this vulnerability may cause sandbox files to be read and written without authorization.	2023-08-13	9.1	Critical
CVE-2023-39400	huawei - multiple products	Parameter verification vulnerability in the installd module. Successful exploitation of this vulnerability may cause sandbox files to be read and written without authorization.	2023-08-13	9.1	Critical
CVE-2023-39401	huawei - multiple products	Parameter verification vulnerability in the installd module. Successful exploitation of this vulnerability may cause sandbox files to be read and written without authorization.	2023-08-13	9.1	Critical
CVE-2023-39402	huawei - multiple products	Parameter verification vulnerability in the installd module. Successful exploitation of this vulnerability may cause sandbox files to be read and written without authorization.	2023-08-13	9.1	Critical
CVE-2023-39403	huawei - multiple products	Parameter verification vulnerability in the installd module. Successful exploitation of this vulnerability may cause sandbox files to be read and written without authorization.	2023-08-13	9.1	Critical
CVE-2023-20013	cisco - intersight_private_virtual_appliance	Multiple vulnerabilities in Cisco Intersight Private Virtual Appliance could allow an authenticated, remote attacker to execute arbitrary commands using root-level privileges. The attacker would need to have Administrator privileges on the affected device to exploit these vulnerabilities. These vulnerabilities are due to insufficient input validation when extracting uploaded software packages. An attacker could exploit these vulnerabilities by authenticating to an affected device and uploading a crafted software package. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges.	2023-08-16	9.1	Critical
CVE-2023-20017	cisco - intersight_private_virtual_appliance	Multiple vulnerabilities in Cisco Intersight Private Virtual Appliance could allow an authenticated, remote attacker to execute arbitrary commands using root-level privileges. The attacker would need to have Administrator privileges on the affected device to exploit these vulnerabilities. These vulnerabilities are due to insufficient input validation when extracting uploaded software packages. An attacker could exploit these vulnerabilities by authenticating to an affected device and uploading a crafted software package. A successful exploit could allow the attacker to execute commands on the underlying operating system with root-level privileges.	2023-08-16	9.1	Critical
CVE-2023-33013	zyxel - nbg6604_firmware	A post-authentication command injection vulnerability in the NTP feature of Zyxel NBG6604 firmware version V1.01(ABIR.1)C0 could allow an authenticated attacker to execute some OS commands remotely by sending a crafted HTTP request.	2023-08-14	8.8	High
CVE-2023-21273	google - multiple products	In SDP_AddAttribute of sdp_db.cc, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	8.8	High
CVE-2023-21282	google - multiple products	In TRANSPOSER_SETTINGS of lpp_tran.h, there is a possible out of bounds write due to an incorrect bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.	2023-08-14	8.8	High
CVE-2022-42828	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13. An app may be able to execute arbitrary code with kernel privileges.	2023-08-14	8.8	High
CVE-2022-48503	apple - multiple products	The issue was addressed with improved bounds checks. This issue is fixed in tvOS 15.6, watchOS 8.7, iOS 15.6 and iPadOS 15.6, macOS Monterey 12.5, Safari 15.6. Processing web content may lead to arbitrary code execution.	2023-08-14	8.8	High
CVE-2023-28198	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in iOS 16.4 and iPadOS 16.4, macOS Ventura 13.3. Processing web content may lead to arbitrary code execution.	2023-08-14	8.8	High
CVE-2023-32358	apple - multiple products	A type confusion issue was addressed with improved checks. This issue is fixed in iOS 16.4 and iPadOS 16.4, macOS Ventura 13.3. Processing web content may lead to arbitrary code execution.	2023-08-14	8.8	High
CVE-2023-2312	google - chrome	Use after free in Offline in Google Chrome on Android prior to 116.0.5845.96 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-15	8.8	High
CVE-2023-4349	google - chrome	Use after free in Device Trust Connectors in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-15	8.8	High
CVE-2023-4351	google - chrome	Use after free in Network in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who has elicited a browser shutdown to	2023-08-15	8.8	High

		potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)			
CVE-2023-4352	google - chrome	Type confusion in V8 in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-15	8.8	High
CVE-2023-4353	google - chrome	Heap buffer overflow in ANGLE in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-15	8.8	High
CVE-2023-4354	google - chrome	Heap buffer overflow in Skia in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-15	8.8	High
CVE-2023-4355	google - chrome	Out of bounds memory access in V8 in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-08-15	8.8	High
CVE-2023-4356	google - chrome	Use after free in Audio in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who has convinced a user to engage in specific UI interaction to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2023-08-15	8.8	High
CVE-2023-4357	google - chrome	Insufficient validation of untrusted input in XML in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to bypass file access restrictions via a crafted HTML page. (Chromium security severity: Medium)	2023-08-15	8.8	High
CVE-2023-4358	google - chrome	Use after free in DNS in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2023-08-15	8.8	High
CVE-2023-4362	google - chrome	Heap buffer overflow in Mojom IDL in Google Chrome prior to 116.0.5845.96 allowed a remote attacker who had compromised the renderer process and gained control of a WebUI process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2023-08-15	8.8	High
CVE-2023-4366	google - chrome	Use after free in Extensions in Google Chrome prior to 116.0.5845.96 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: Medium)	2023-08-15	8.8	High
CVE-2023-4368	google - chrome	Insufficient policy enforcement in Extensions API in Google Chrome prior to 116.0.5845.96 allowed an attacker who convinced a user to install a malicious extension to bypass an enterprise policy via a crafted HTML page. (Chromium security severity: Medium)	2023-08-15	8.8	High
CVE-2023-4369	google - chrome	Insufficient data validation in Systems Extensions in Google Chrome on ChromeOS prior to 116.0.5845.96 allowed an attacker who convinced a user to install a malicious extension to bypass file restrictions via a crafted HTML page. (Chromium security severity: Medium)	2023-08-15	8.8	High
CVE-2023-40336	jenkins - folders	A cross-site request forgery (CSRF) vulnerability in Jenkins Folders Plugin 6.846.v23698686f0f6 and earlier allows attackers to copy folders.	2023-08-16	8.8	High
CVE-2023-40341	jenkins - blue_ocean	A cross-site request forgery (CSRF) vulnerability in Jenkins Blue Ocean Plugin 1.27.5 and earlier allows attackers to connect to an attacker-specified URL, capturing GitHub credentials associated with an attacker-specified job.	2023-08-16	8.8	High
CVE-2023-35893	ibm - multiple products	IBM Security Guardium 10.6, 11.3, 11.4, and 11.5 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 258824.	2023-08-16	8.8	High
CVE-2023-39438	sap - contributor_license_agreement_assistant	A missing authorization check allows an arbitrary authenticated user to perform certain operations through the API of CLA-assistant by executing specific additional steps. This allows an arbitrary authenticated user to read CLA information including information of the persons who signed them as well as custom fields the CLA requester had configured. In addition, an arbitrary authenticated user can update or delete the CLA-configuration for repositories or organizations using CLA-assistant. The stored access tokens for GitHub are not affected, as these are redacted from the API-responses.	2023-08-15	8.1	High
CVE-2023-40283	linux - linux_kernel	An issue was discovered in l2cap_sock_release in net/bluetooth/l2cap_sock.c in the Linux kernel before 6.4.10. There is a use-after-free because the children of an sk are mishandled.	2023-08-14	7.8	High
CVE-2023-40303	gnu - inetutils	GNU inetutils through 2.4 may allow privilege escalation because of unchecked return values of set*id() family functions in ftpd, rcp, rlogin, rsh, rshd, and uucpd. This is, for example, relevant if the setuid system call fails when a process is trying to drop privileges before letting an ordinary user control the activities of the process.	2023-08-14	7.8	High
CVE-2023-40305	gnu - indent	GNU indent 2.2.13 has a heap-based buffer overflow in search_brace in indent.c via a crafted file.	2023-08-14	7.8	High

CVE-2023-38721	ibm - multiple products	The IBM i 7.2, 7.3, 7.4, and 7.5 product Facsimile Support for i contains a local privilege escalation vulnerability. A malicious actor could gain access to a command line with elevated privileges allowing root access to the host operating system. IBM X-Force ID: 262173.	2023-08-14	7.8	High
CVE-2023-21269	google - android	In startActivityInner of ActivityStarter.java, there is a possible way to launch an activity into PiP mode from the background due to BAL bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	7.8	High
CVE-2023-21229	google - multiple products	In registerServiceLocked of ManagedServices.java, there is a possible bypass of background activity launch restrictions due to an unsafe PendingIntent. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	7.8	High
CVE-2023-21231	google - android	In getIntentForButton of ButtonManager.java, there is a possible way for an unprivileged application to start a non-exported or permission-protected activity due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	7.8	High
CVE-2023-21235	google - multiple products	In onCreate of LockSettingsActivity.java, there is a possible way set a new lockscreen PIN without entering the existing PIN 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.	2023-08-14	7.8	High
CVE-2023-21272	google - multiple products	In readFrom of Uri.java, there is a possible bad URI permission grant due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	7.8	High
CVE-2023-21275	google - multiple products	In decideCancelProvisioningDialog of AdminIntegratedFlowPrepareActivity.java, there is a possible way to bypass factory reset protections 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.	2023-08-14	7.8	High
CVE-2023-21281	google - multiple products	In multiple functions of KeyguardViewMediator.java, there is a possible failure to lock after screen timeout due to a logic error in the code. This could lead to local escalation of privilege across users with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	7.8	High
CVE-2023-21286	google - multiple products	In visitUris of RemoteViews.java, there is a possible way to reveal images across users due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	7.8	High
CVE-2023-35689	google - multiple products	In checkDebuggingDisallowed of DeviceVersionFragment.java, there is a possible way to access adb before SUW completion due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	7.8	High
CVE-2020-36615	apple - macos	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Big Sur 11.0.1. Processing a maliciously crafted font may lead to arbitrary code execution.	2023-08-14	7.8	High
CVE-2022-46706	apple - multiple products	A type confusion issue was addressed with improved state handling. This issue is fixed in Security Update 2022-003 Catalina, macOS Monterey 12.3, macOS Big Sur 11.6.5. An application may be able to execute arbitrary code with kernel privileges.	2023-08-14	7.8	High
CVE-2023-38401	hp - aruba_virtual_intranet_access	A vulnerability in the HPE Aruba Networking Virtual Intranet Access (VIA) client could allow local users to elevate privileges. Successful exploitation could allow execution of arbitrary code with NT AUTHORITY\SYSTEM privileges on the operating system.	2023-08-15	7.8	High
CVE-2023-32486	dell - powerscale_onefs	Dell PowerScale OneFS 9.5.x version contain a privilege escalation vulnerability. A low privilege local attacker could potentially exploit this vulnerability, leading to escalation of privileges.	2023-08-16	7.8	High
CVE-2023-32487	dell - multiple products	Dell PowerScale OneFS, 8.2.x - 9.5.0.x, contains an elevation of privilege vulnerability. A low privileged local attacker could potentially exploit this vulnerability, leading to denial of service, code execution and information disclosure.	2023-08-16	7.8	High
CVE-2023-32495	dell - multiple products	Dell PowerScale OneFS, 8.2.x-9.5.x, contains a exposure of sensitive information to an unauthorized Actor vulnerability. An authorized local attacker could potentially exploit this vulnerability, leading to escalation of privileges.	2023-08-16	7.8	High
CVE-2023-20224	cisco - thousandeyes_enterprise_agent	A vulnerability in the CLI of Cisco ThousandEyes Enterprise Agent, Virtual Appliance installation type, could allow an authenticated, local attacker to elevate privileges to root on an affected device.	2023-08-16	7.8	High

		This vulnerability is due to insufficient input validation of user-supplied CLI arguments. An attacker could exploit this vulnerability by authenticating to an affected device and using crafted commands at the prompt. A successful exploit could allow the attacker to execute arbitrary commands as root. The attacker must have valid credentials on the affected device.			
CVE-2023-3078	lenovo - universal_device_client	An uncontrolled search path vulnerability was reported in the Lenovo Universal Device Client (UDC) that could allow an attacker with local access to execute code with elevated privileges.	2023-08-17	7.8	High
CVE-2023-4030	lenovo - thinkpad_t15_gen_2_firmware	A vulnerability was reported in BIOS for ThinkPad P14s Gen 2, P15s Gen 2, T14 Gen 2, and T15 Gen 2 that could cause the system to recover to insecure settings if the BIOS becomes corrupt.	2023-08-17	7.8	High
CVE-2023-39380	huawei - multiple products	Permission control vulnerability in the audio module. Successful exploitation of this vulnerability may cause audio devices to perform abnormally.	2023-08-13	7.5	High
CVE-2023-39381	huawei - multiple products	Input verification vulnerability in the storage module. Successful exploitation of this vulnerability may cause the device to restart.	2023-08-13	7.5	High
CVE-2023-39382	huawei - multiple products	Input verification vulnerability in the audio module. Successful exploitation of this vulnerability may cause virtual machines (VMs) to restart.	2023-08-13	7.5	High
CVE-2023-39383	huawei - multiple products	Vulnerability of input parameters being not strictly verified in the AMS module. Successful exploitation of this vulnerability may compromise apps' data security.	2023-08-13	7.5	High
CVE-2023-39384	huawei - multiple products	Vulnerability of incomplete permission verification in the input method module. Successful exploitation of this vulnerability may cause features to perform abnormally.	2023-08-13	7.5	High
CVE-2023-39388	huawei - multiple products	Vulnerability of input parameters being not strictly verified in the PMS module. Successful exploitation of this vulnerability may cause home screen unavailability.	2023-08-13	7.5	High
CVE-2023-39389	huawei - multiple products	Vulnerability of input parameters being not strictly verified in the PMS module. Successful exploitation of this vulnerability may cause home screen unavailability.	2023-08-13	7.5	High
CVE-2023-39392	huawei - multiple products	Vulnerability of insecure signatures in the OsuLogin module. Successful exploitation of this vulnerability may cause OsuLogin to be maliciously modified and overwritten.	2023-08-13	7.5	High
CVE-2023-39393	huawei - multiple products	Vulnerability of insecure signatures in the ServiceWifiResources module. Successful exploitation of this vulnerability may cause ServiceWifiResources to be maliciously modified and overwritten.	2023-08-13	7.5	High
CVE-2023-39396	huawei - multiple products	Deserialization vulnerability in the input module. Successful exploitation of this vulnerability may affect availability.	2023-08-13	7.5	High
CVE-2023-39386	huawei - multiple products	Vulnerability of input parameters being not strictly verified in the PMS module. Successful exploitation of this vulnerability may cause newly installed apps to fail to restart.	2023-08-13	7.5	High
CVE-2023-39390	huawei - multiple products	Vulnerability of input parameter verification in certain APIs in the window management module. Successful exploitation of this vulnerability may cause the device to restart.	2023-08-13	7.5	High
CVE-2023-39391	huawei - multiple products	Vulnerability of system file information leakage in the USB Service module. Successful exploitation of this vulnerability may affect confidentiality.	2023-08-13	7.5	High
CVE-2023-39394	huawei - multiple products	Vulnerability of API privilege escalation in the wifienhance module. Successful exploitation of this vulnerability may cause the arp list to be modified.	2023-08-13	7.5	High
CVE-2023-39395	huawei - multiple products	Mismatch vulnerability in the serialization process in the communication system. Successful exploitation of this vulnerability may affect availability.	2023-08-13	7.5	High
CVE-2023-39397	huawei - multiple products	Input parameter verification vulnerability in the communication system. Successful exploitation of this vulnerability may affect availability.	2023-08-13	7.5	High
CVE-2023-39404	huawei - emui	Vulnerability of input parameter verification in certain APIs in the window management module. Successful exploitation of this vulnerability may cause the device to restart.	2023-08-13	7.5	High
CVE-2023-39406	huawei - emui	Permission control vulnerability in the XLayout component. Successful exploitation of this vulnerability may cause apps to forcibly restart.	2023-08-13	7.5	High
CVE-2023-38741	ibm - multiple products	IBM TXSeries for Multiplatforms 8.1, 8.2, and 9.1 is vulnerable to a denial of service, caused by improper enforcement of the timeout on individual read operations. By conducting a slowloris-type attacks, a remote attacker could exploit this vulnerability to cause a denial of service. IBM X-Force ID: 262905.	2023-08-14	7.5	High
CVE-2023-21265	google - multiple products	In multiple locations, there are root CA certificates which need to be disabled. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	7.5	High
CVE-2023-21233	google - android	In multiple locations of avrc, there is a possible leak of heap data due to uninitialized data. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	7.5	High

CVE-2023-40338	jenkins - folders	Jenkins Folders Plugin 6.846.v23698686f0f6 and earlier displays an error message that includes an absolute path of a log file when attempting to access the Scan Organization Folder Log if no logs are available, exposing information about the Jenkins controller file system.	2023-08-16	7.5	High
CVE-2023-40339	jenkins - config_file_provider	Jenkins Config File Provider Plugin 952.va_544a_6234b_46 and earlier does not mask (i.e., replace with asterisks) credentials specified in configuration files when they're written to the build log.	2023-08-16	7.5	High
CVE-2023-40340	jenkins - nodejs	Jenkins NodeJS Plugin 1.6.0 and earlier does not properly mask (i.e., replace with asterisks) credentials specified in the Npm config file in Pipeline build logs.	2023-08-16	7.5	High
CVE-2023-38737	ibm - websphere_application_server	IBM WebSphere Application Server Liberty 22.0.0.13 through 23.0.0.7 is vulnerable to a denial of service, caused by sending a specially-crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. IBM X-Force ID: 262567.	2023-08-16	7.5	High
CVE-2023-20197	cisco - multiple products	A vulnerability in the filesystem image parser for Hierarchical File System Plus (HFS+) of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to an incorrect check for completion when a file is decompressed, which may result in a loop condition that could cause the affected software to stop responding. An attacker could exploit this vulnerability by submitting a crafted HFS+ filesystem image to be scanned by ClamAV on an affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to stop responding, resulting in a DoS condition on the affected software and consuming available system resources. For a description of this vulnerability, see the ClamAV blog .	2023-08-16	7.5	High
CVE-2023-40272	apache - apache-airflow-providers-apache-spark	Apache Airflow Spark Provider, versions before 4.1.3, is affected by a vulnerability that allows an attacker to pass in malicious parameters when establishing a connection giving an opportunity to read files on the Airflow server. It is recommended to upgrade to a version that is not affected.	2023-08-17	7.5	High
CVE-2023-20212	cisco - multiple products	A vulnerability in the AutoIt module of ClamAV could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to a logic error in the memory management of an affected device. An attacker could exploit this vulnerability by submitting a crafted AutoIt file to be scanned by ClamAV on the affected device. A successful exploit could allow the attacker to cause the ClamAV scanning process to restart unexpectedly, resulting in a DoS condition.	2023-08-18	7.5	High
CVE-2022-4894	hp - 2zn49a_firmware	Certain HP and Samsung Printer software packages may potentially be vulnerable to elevation of privilege due to Uncontrolled Search Path Element.	2023-08-16	7.3	High
CVE-2023-20209	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) could allow an authenticated, remote attacker with read-write privileges on the application to perform a command injection attack that could result in remote code execution on an affected device. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to establish a remote shell with root privileges.	2023-08-16	7.2	High
CVE-2023-28179	apple - macos	The issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. Processing a maliciously crafted AppleScript binary may result in unexpected app termination or disclosure of process memory.	2023-08-14	7.1	High
CVE-2023-38402	hp - aruba_virtual_intranet_access	A vulnerability in the HPE Aruba Networking Virtual Intranet Access (VIA) client could allow malicious users to overwrite arbitrary files as NT AUTHORITY\SYSTEM. A successful exploit could allow these malicious users to create a Denial-of-Service (DoS) condition affecting the Microsoft Windows operating System boot process.	2023-08-15	7.1	High
CVE-2023-32492	dell - multiple products	Dell PowerScale OneFS 9.5.0.x contains an incorrect default	2023-08-16	7.1	High

		permissions vulnerability. A low-privileged local attacker could potentially exploit this vulnerability, leading to information disclosure or allowing to modify files.			
CVE-2023-4387	linux - linux_kernel	A use-after-free flaw was found in vmxnet3_rq_alloc_rx_buf in drivers/net/vmxnet3/vmxnet3_drv.c in VMware's vmxnet3 ethernet NIC driver in the Linux Kernel. This issue could allow a local attacker to crash the system due to a double-free while cleaning up vmxnet3_rq_cleanup_all, which could also lead to a kernel information leak problem.	2023-08-16	7.1	High
CVE-2023-4389	linux - multiple products	A flaw was found in btrfs_get_root_ref in fs/btrfs/disk-io.c in the btrfs filesystem in the Linux Kernel due to a double decrement of the reference count. This issue may allow a local attacker with user privilege to crash the system or may lead to leaked internal kernel information.	2023-08-16	7.1	High
CVE-2023-20229	cisco - duo_device_health_application	A vulnerability in the CryptoService function of Cisco Duo Device Health Application for Windows could allow an authenticated, local attacker with low privileges to conduct directory traversal attacks and overwrite arbitrary files on an affected system. This vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by executing a directory traversal attack on an affected host. A successful exploit could allow an attacker to use a cryptographic key to overwrite arbitrary files with SYSTEM-level privileges, resulting in a denial of service (DoS) condition or data loss on the affected system.	2023-08-16	7.1	High
CVE-2023-40291	samsung - harman_infotainment	Harman Infotainment 20190525031613 allows root access via SSH over a USB-to-Ethernet dongle with a password that is an internal project name.	2023-08-14	6.8	Medium
CVE-2023-40293	samsung - harman_infotainment	Harman Infotainment 20190525031613 and later allows command injection via unauthenticated RPC with a D-Bus connection object.	2023-08-14	6.8	Medium
CVE-2023-21132	google - multiple products	In onCreate of ManagePermissionsActivity.java, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	6.8	Medium
CVE-2023-21133	google - multiple products	In onCreate of ManagePermissionsActivity.java, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	6.8	Medium
CVE-2023-21134	google - multiple products	In onCreate of ManagePermissionsActivity.java, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	6.8	Medium
CVE-2023-21140	google - multiple products	In onCreate of ManagePermissionsActivity.java, there is a possible way to bypass factory reset protections due to a missing permission check. This could lead to local escalation of privilege with physical access to a device that's been factory reset with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	6.8	Medium
CVE-2023-21264	google - android	In multiple functions of mem_protect.c, there is a possible way to access hypervisor memory due to a memory access check in the wrong place. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	6.7	Medium
CVE-2023-32494	dell - multiple products	Dell PowerScale OneFS, 8.0.x-9.5.x, contains an improper handling of insufficient privileges vulnerability. A local privileged attacker could potentially exploit this vulnerability, leading to elevation of privilege and affect in compliance mode also.	2023-08-16	6.7	Medium
CVE-2023-32489	dell - multiple products	Dell PowerScale OneFS 8.2x -9.5x contains a privilege escalation vulnerability. A local attacker with high privileges could potentially exploit this vulnerability, to bypass mode protections and gain elevated privileges.	2023-08-16	6.7	Medium
CVE-2023-32490	dell - multiple products	Dell PowerScale OneFS 8.2x -9.5x contains an improper privilege management vulnerability. A high privilege local attacker could potentially exploit this vulnerability, leading to system takeover.	2023-08-16	6.7	Medium
CVE-2023-29182	fortinet - fortios	A stack-based buffer overflow vulnerability [CWE-121] in Fortinet FortiOS before 7.0.3 allows a privileged attacker to execute arbitrary code via specially crafted CLI commands, provided the attacker were able to evade FortiOS stack protections.	2023-08-17	6.7	Medium

CVE-2023-34419	lenovo - legion_5_pro_16iah7h_firmware	A buffer overflow has been identified in the SetupUtility driver in some Lenovo Notebook products which may allow an attacker with local access and elevated privileges to execute arbitrary code.	2023-08-17	6.7	Medium
CVE-2023-4028	lenovo - 13w_yoga_firmware	A buffer overflow has been identified in the SystemUserMasterHddPwdDxe driver in some Lenovo Notebook products which may allow an attacker with local access and elevated privileges to execute arbitrary code.	2023-08-17	6.7	Medium
CVE-2023-4029	lenovo - k14_type_21cu_firmware	A buffer overflow has been identified in the BoardUpdateAcpiDxe driver in some Lenovo ThinkPad products which may allow an attacker with local access and elevated privileges to execute arbitrary code.	2023-08-17	6.7	Medium
CVE-2023-28768	zyxel - xgs2220-30_firmware	Improper frame handling in the Zyxel XGS2220-30 firmware version V4.80(ABXN.1), XMG1930-30 firmware version V4.80(ACAR.1), and XS1930-10 firmware version V4.80(ABQE.1) could allow an unauthenticated LAN-based attacker to cause denial-of-service (DoS) conditions by sending crafted frames to an affected switch.	2023-08-14	6.5	Medium
CVE-2023-4350	google - chrome	Inappropriate implementation in Fullscreen in Google Chrome on Android prior to 116.0.5845.96 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: High)	2023-08-15	6.5	Medium
CVE-2023-4367	google - chrome	Insufficient policy enforcement in Extensions API in Google Chrome prior to 116.0.5845.96 allowed an attacker who convinced a user to install a malicious extension to bypass an enterprise policy via a crafted HTML page. (Chromium security severity: Medium)	2023-08-15	6.5	Medium
CVE-2023-32491	dell - powerscale_onefs	Dell PowerScale OneFS 9.5.0.x, contains an insertion of sensitive information into log file vulnerability in SNMPv3. A low privileges user could potentially exploit this vulnerability, leading to information disclosure.	2023-08-16	6.5	Medium
CVE-2023-40345	jenkins - delphix	Jenkins Delphix Plugin 3.0.2 and earlier does not set the appropriate context for credentials lookup, allowing attackers with Overall/Read permission to access and capture credentials they are not entitled to.	2023-08-16	6.5	Medium
CVE-2023-40347	jenkins - maven_artifact_choicelistprovider_\(nexus\)	Jenkins Maven Artifact ChoiceListProvider (Nexus) Plugin 1.14 and earlier does not set the appropriate context for credentials lookup, allowing attackers with Item/Configure permission to access and capture credentials they are not entitled to.	2023-08-16	6.5	Medium
CVE-2023-20111	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. This vulnerability is due to the improper storage of sensitive information within the web-based management interface. An attacker could exploit this vulnerability by logging in to the web-based management interface and viewing hidden fields within the application. A successful exploit could allow the attacker to access sensitive information, including device entry credentials, that could aid the attacker in further attacks.	2023-08-16	6.5	Medium
CVE-2023-20221	cisco - video_phone_8875_firmware	A vulnerability in the web-based management interface of Cisco IP Phone 6800, 7800, and 8800 Series with Multiplatform Firmware could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack against a user of the web-based management interface of an affected system. This vulnerability is due to insufficient CSRF protections for the web-based management interface of an affected device. An attacker could exploit this vulnerability by persuading an authenticated user of the interface to follow a crafted link. A successful exploit could allow the attacker to perform a factory reset of the affected device, resulting in a Denial of Service (DoS) condition.	2023-08-16	6.5	Medium
CVE-2023-31492	zohocorp - multiple products	Zoho ManageEngine ADManager Plus version 7182 and prior disclosed the default passwords for the account restoration of unauthorized domains to the authenticated users.	2023-08-17	6.5	Medium
CVE-2023-40037	apache - nifi	Apache NiFi 1.21.0 through 1.23.0 support JDBC and JNDI JMS access in several Processors and Controller Services with connection URL validation that does not provide sufficient protection against crafted inputs. An authenticated and authorized user can bypass connection URL validation using custom input formatting. The resolution enhances connection URL validation and introduces validation for additional related properties. Upgrading to Apache NiFi 1.23.1 is the recommended mitigation.	2023-08-18	6.5	Medium
CVE-2023-28075	dell - alienware_m15_r7_firmware	Dell BIOS contain a Time-of-check Time-of-use vulnerability in BIOS. A local authenticated malicious user with physical access to	2023-08-16	6.3	Medium

		the system could potentially exploit this vulnerability by using a specifically timed DMA transaction during an SMI in order to gain arbitrary code execution on the system.			
CVE-2023-20242	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Unified Communications Manager (Unified CM), Cisco Unified CM Session Management Edition (Unified CM SME), and Cisco Unified Communications Manager IM &amp; Presence Service (Unified CM IM&amp;P) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface 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 access sensitive, browser-based information.	2023-08-16	6.1	Medium
CVE-2023-20222	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface on an affected device. The vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. 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.	2023-08-16	6.1	Medium
CVE-2023-4394	linux - multiple products	A use-after-free flaw was found in btrfs_get_dev_args_from_path in fs/btrfs/volumes.c in btrfs file-system in the Linux Kernel. This flaw allows a local attacker with special privileges to cause a system crash or leak internal kernel information	2023-08-17	6	Medium
CVE-2023-40343	jenkins - tuleap_authentication	Jenkins Tuleap Authentication Plugin 1.1.20 and earlier uses a non-constant time comparison function when validating an authentication token allowing attackers to use statistical methods to obtain a valid authentication token.	2023-08-16	5.9	Medium
CVE-2023-21267	google - multiple products	In doKeyguardLocked of KeyguardViewMediator.java, there is a possible way to bypass lockdown mode with screen pinning due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium
CVE-2023-21268	google - multiple products	In update of MmsProvider.java, there is a possible way to change directory permissions due to a path traversal error. This could lead to local denial of service of SIM recognition with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium
CVE-2023-21230	google - multiple products	In onAccessPointChanged of AccessPointPreference.java, there is a possible way for unprivileged apps to receive a broadcast about WiFi access point change and its BSSID or SSID due to a precondition check failure. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium
CVE-2023-21234	google - multiple products	In launchConfirmationActivity of ChooseLockSettingsHelper.java, there is a possible way to enable developer options without the lockscreen PIN due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium
CVE-2023-21271	google - multiple products	In parseInputs of ShimPreparedModel.cpp, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium
CVE-2023-21274	google - multiple products	In convertSubgraphFromHAL of ShimConverter.cpp, 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.	2023-08-14	5.5	Medium
CVE-2023-21276	google - multiple products	In writeToParcel of CursorWindow.cpp, there is a possible information disclosure due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium
CVE-2023-21277	google - multiple products	In visitUris of RemoteViews.java, there is a possible way to reveal images across users due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium

CVE-2023-21279	google - multiple products	In visitUris of RemoteViews.java, there is a possible cross-user media read due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium
CVE-2023-21280	google - multiple products	In setMediaButtonBroadcastReceiver of MediaSessionRecord.java, there is a possible permanent DoS 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.	2023-08-14	5.5	Medium
CVE-2023-21283	google - multiple products	In multiple functions of StatusHints.java, there is a possible way to reveal images across users due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.	2023-08-14	5.5	Medium
CVE-2023-21284	google - multiple products	In multiple functions of DevicePolicyManager.java, there is a possible way to prevent enabling the Find my Device feature due to improper input validation. This could lead to local denial of service with User execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium
CVE-2023-21285	google - multiple products	In setMetadata of MediaSessionRecord.java, there is a possible way to view another user's images due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium
CVE-2023-21288	google - multiple products	In visitUris of Notification.java, there is a possible way to reveal images across users due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium
CVE-2023-21289	google - multiple products	In multiple locations, there is a possible bypass of a multi user security boundary due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium
CVE-2023-21290	google - multiple products	In update of MmsProvider.java, there is a possible way to bypass file permission checks due to a race condition. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium
CVE-2023-21292	google - multiple products	In openContentUri of ActivityManagerService.java, there is a possible way for a third party app to obtain restricted files due to a confused deputy. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	5.5	Medium
CVE-2022-22646	apple - macos	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Monterey 12.2. A malicious application may be able to modify protected parts of the file system.	2023-08-14	5.5	Medium
CVE-2022-22655	apple - multiple products	An access issue was addressed with improvements to the sandbox. This issue is fixed in macOS Monterey 12.3, iOS 15.4 and iPadOS 15.4. An app may be able to leak sensitive user information.	2023-08-14	5.5	Medium
CVE-2022-26699	apple - multiple products	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13. An app may be able to cause a denial-of-service to Endpoint Security clients.	2023-08-14	5.5	Medium
CVE-2022-46722	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13. An app may be able to modify protected parts of the file system.	2023-08-14	5.5	Medium
CVE-2023-27939	apple - macos	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3. Processing an image may result in disclosure of process memory.	2023-08-14	5.5	Medium
CVE-2023-27947	apple - macos	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3. Processing an image may result in disclosure of process memory.	2023-08-14	5.5	Medium
CVE-2023-27948	apple - macos	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3. Processing an image may result in disclosure of process memory.	2023-08-14	5.5	Medium
CVE-2023-28199	apple - macos	An out-of-bounds read issue existed that led to the disclosure of kernel memory. This was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3. An app may be able to disclose kernel memory.	2023-08-14	5.5	Medium
CVE-2023-24478	intel - quartus_prime	Use of insufficiently random values for some Intel Agilex(R) software included as part of Intel(R) Quartus(R) Prime Pro Edition for linux before version 22.4 may allow an authenticated user to potentially enable information disclosure via local access.	2023-08-15	5.5	Medium
CVE-2023-39250	dell - storage_integration_tools_for_vmware	Dell Storage Integration Tools for VMware (DSITV) 06.01.00.016 contain an information disclosure vulnerability. A local low-privileged malicious user could potentially exploit this vulnerability to retrieve an encryption key that could aid in further attacks.	2023-08-16	5.5	Medium
CVE-2023-4385	linux - linux_kernel	A NULL pointer dereference flaw was found in dbFree in fs/jfs/jfs_dmap.c in the journaling file system (JFS) in the Linux Kernel. This issue may allow a local attacker to crash the system due to a missing sanity check.	2023-08-16	5.5	Medium

CVE-2023-20217	cisco - multiple products	A vulnerability in the CLI of Cisco ThousandEyes Enterprise Agent, Virtual Appliance installation type, could allow an authenticated, local attacker to elevate privileges on an affected device. This vulnerability is due to insufficient input validation by the operating system CLI. An attacker could exploit this vulnerability by issuing certain commands using sudo. A successful exploit could allow the attacker to view arbitrary files as root on the underlying operating system. The attacker must have valid credentials on the affected device.	2023-08-16	5.5	Medium
CVE-2023-40342	jenkins - flaky_test_handler	Jenkins Flaky Test Handler Plugin 1.2.2 and earlier does not escape JUnit test contents when showing them on the Jenkins UI, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control JUnit report file contents.	2023-08-16	5.4	Medium
CVE-2023-40346	jenkins - shortcut_job	Jenkins Shortcut Job Plugin 0.4 and earlier does not escape the shortcut redirection URL, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to configure shortcut jobs.	2023-08-16	5.4	Medium
CVE-2023-40350	jenkins - docker_swarm	Jenkins Docker Swarm Plugin 1.11 and earlier does not escape values returned from Docker before inserting them into the Docker Swarm Dashboard view, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control responses from Docker.	2023-08-16	5.4	Medium
CVE-2023-20201	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker must have valid credentials to access the web-based management interface of the affected device.	2023-08-16	5.4	Medium
CVE-2023-20203	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker must have valid credentials to access the web-based management interface of the affected device.	2023-08-16	5.4	Medium
CVE-2023-20205	cisco - multiple products	Multiple vulnerabilities in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network Manager (EPNM) could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface on an affected device. These vulnerabilities are due to insufficient validation of user-supplied input. An attacker could exploit these vulnerabilities by persuading a user of an affected interface to view a page containing malicious HTML or script content. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit these vulnerabilities, the attacker must have valid credentials to access the web-based management interface of the affected device.	2023-08-16	5.4	Medium
CVE-2023-35011	ibm - multiple products	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 is vulnerable to server-side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. IBM X-Force ID: 257705.	2023-08-16	5.4	Medium
CVE-2023-39387	huawei - multiple products	Vulnerability of permission control in the window management module. Successful exploitation of this vulnerability may cause malicious pop-up windows.	2023-08-13	5.3	Medium

CVE-2023-4359	google - chrome	Inappropriate implementation in App Launcher in Google Chrome on iOS prior to 116.0.5845.96 allowed a remote attacker to potentially spoof elements of the security UI via a crafted HTML page. (Chromium security severity: Medium)	2023-08-15	5.3	Medium
CVE-2023-4361	google - chrome	Inappropriate implementation in Autofill in Google Chrome on Android prior to 116.0.5845.96 allowed a remote attacker to bypass Autofill restrictions via a crafted HTML page. (Chromium security severity: Medium)	2023-08-15	5.3	Medium
CVE-2023-40348	jenkins - gogs	The webhook endpoint in Jenkins Gogs Plugin 1.0.15 and earlier provides unauthenticated attackers information about the existence of jobs in its output.	2023-08-16	5.3	Medium
CVE-2023-40349	jenkins - gogs	Jenkins Gogs Plugin 1.0.15 and earlier improperly initializes an option to secure its webhook endpoint, allowing unauthenticated attackers to trigger builds of jobs.	2023-08-16	5.3	Medium
CVE-2023-35009	ibm - multiple products	IBM Cognos Analytics 11.1.7, 11.2.0, and 11.2.1 could allow a remote attacker to obtain system information without authentication which could be used in reconnaissance to gather information that could be used for future attacks. IBM X-Force ID: 257703.	2023-08-16	5.3	Medium
CVE-2023-36844	juniper - multiple products	A PHP External Variable Modification vulnerability in J-Web of Juniper Networks Junos OS on EX Series allows an unauthenticated, network-based attacker to control certain, important environments variables. Utilizing a crafted request an attacker is able to modify certain PHP environments variables leading to partial loss of integrity, which may allow chaining to other vulnerabilities. This issue affects Juniper Networks Junos OS on EX Series: * All versions prior to 20.4R3-S9; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S5; * 22.1 versions prior to 22.1R3-S4; * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.3R3-S1; * 22.4 versions prior to 22.4R2-S2, 22.4R3.	2023-08-17	5.3	Medium
CVE-2023-36845	juniper - multiple products	A PHP External Variable Modification vulnerability in J-Web of Juniper Networks Junos OS on EX Series and SRX Series allows an unauthenticated, network-based attacker to control certain, important environments variables. Utilizing a crafted request an attacker is able to modify a certain PHP environment variable leading to partial loss of integrity, which may allow chaining to other vulnerabilities. This issue affects Juniper Networks Junos OS on SRX Series:	2023-08-17	5.3	Medium

		* All versions prior to 21.4R3-S5; * 22.1 versions prior to 22.1R3-S4; * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.3R2-S2, 22.3R3-S1; * 22.4 versions prior to 22.4R2-S1, 22.4R3; * 23.2 versions prior to 23.2R1-S1, 23.2R2.			
CVE-2023-36846	juniper - multiple products	A Missing Authentication for Critical Function vulnerability in Juniper Networks Junos OS on SRX Series allows an unauthenticated, network-based attacker to cause limited impact to the file system integrity. With a specific request that doesn't require authentication an attacker is able to upload arbitrary files via J-Web, leading to a loss of integrity for a certain part of the file system, which may allow chaining to other vulnerabilities. This issue affects Juniper Networks Junos OS on SRX Series: * All versions prior to 20.4R3-S8; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S5; * 22.1 versions prior to 22.1R3-S3; * 22.2 versions prior to 22.2R3-S2; * 22.3 versions prior to 22.3R2-S2, 22.3R3; * 22.4 versions prior to 22.4R2-S1, 22.4R3.	2023-08-17	5.3	Medium

CVE-2023-36847	juniper - multiple products	A Missing Authentication for Critical Function vulnerability in Juniper Networks Junos OS on EX Series allows an unauthenticated, network-based attacker to cause limited impact to the file system integrity. With a specific request that doesn't require authentication an attacker is able to upload arbitrary files via J-Web, leading to a loss of integrity for a certain part of the file system, which may allow chaining to other vulnerabilities. This issue affects Juniper Networks Junos OS on EX Series: * All versions prior to 20.4R3-S8; * 21.2 versions prior to 21.2R3-S6; * 21.3 versions prior to 21.3R3-S5; * 21.4 versions prior to 21.4R3-S4; * 22.1 versions prior to 22.1R3-S3; * 22.2 versions prior to 22.2R3-S1; * 22.3 versions prior to 22.3R2-S2, 22.3R3; * 22.4 versions prior to 22.4R2-S1, 22.4R3.	2023-08-17	5.3	Medium
CVE-2023-39950	siemens - efibootguard	efibootguard is a simple UEFI boot loader with support for safely switching between current and updated partition sets. Insufficient or missing validation and sanitization of input from untrustworthy bootloader environment files can cause crashes and probably also code injections into `bg_setenv`) or programs using `libebgenv`. This is triggered when the affected components try to modify a manipulated environment, in particular its user variables. Furthermore, `bg_printenv` may crash over invalid read accesses or report invalid results. Not affected by this issue is EFI Boot Guard's bootloader EFI binary. EFI Boot Guard release v0.15 contains required patches to sanitize and validate the bootloader environment prior to processing it in userspace. Its library and tools should be updated, so should programs statically linked against it. An update of the bootloader EFI executable is not required. The only way to prevent the issue with an unpatched EFI Boot Guard version is to avoid accesses to user variables, specifically modifications to them.	2023-08-14	5.2	Medium
CVE-2023-40292	samsung - harman_infotainment	Harman Infotainment 20190525031613 and later discloses the IP address via CarPlay CTRL packets.	2023-08-14	4.3	Medium

CVE-2022-46725	apple - multiple products	A spoofing issue existed in the handling of URLs. This issue was addressed with improved input validation. This issue is fixed in iOS 16.4 and iPadOS 16.4. Visiting a malicious website may lead to address bar spoofing.	2023-08-14	4.3	Medium
CVE-2023-4360	google - chrome	Inappropriate implementation in Color in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	2023-08-15	4.3	Medium
CVE-2023-4363	google - chrome	Inappropriate implementation in WebShare in Google Chrome on Android prior to 116.0.5845.96 allowed a remote attacker to spoof the contents of a dialog URL via a crafted HTML page. (Chromium security severity: Medium)	2023-08-15	4.3	Medium
CVE-2023-4364	google - chrome	Inappropriate implementation in Permission Prompts in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	2023-08-15	4.3	Medium
CVE-2023-4365	google - chrome	Inappropriate implementation in Fullscreen in Google Chrome prior to 116.0.5845.96 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	2023-08-15	4.3	Medium
CVE-2023-32488	dell - multiple products	Dell PowerScale OneFS, 8.2.x-9.5.0.x, contains an information disclosure vulnerability in NFS. A low privileged attacker could potentially exploit this vulnerability, leading to information disclosure.	2023-08-16	4.3	Medium
CVE-2023-40337	jenkins - folders	A cross-site request forgery (CSRF) vulnerability in Jenkins Folders Plugin 6.846.v23698686f0f6 and earlier allows attackers to copy a view inside a folder.	2023-08-16	4.3	Medium
CVE-2023-40344	jenkins - delphix	A missing permission check in Jenkins Delphix Plugin 3.0.2 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of credentials stored in Jenkins.	2023-08-16	4.3	Medium
CVE-2023-40351	jenkins - favorite_view	A cross-site request forgery (CSRF) vulnerability in Jenkins Favorite View Plugin 5.v77a_37f62782d and earlier allows attackers to add or remove views from another user's favorite views tab bar.	2023-08-16	4.3	Medium
CVE-2023-20237	cisco - intersight_virtual_appliance	A vulnerability in Cisco Intersight Virtual Appliance could allow an unauthenticated, adjacent attacker to access internal HTTP services that are otherwise inaccessible. This vulnerability is due to insufficient restrictions on internally accessible http proxies. An attacker could exploit this vulnerability by submitting a crafted CLI command. A successful exploit could allow the attacker access to internal subnets beyond the sphere of their intended access level.	2023-08-16	4.3	Medium
CVE-2023-32453	dell - alienware_m15_r7_firmware	Dell BIOS contains an improper authentication vulnerability. A malicious user with physical access to the system may potentially exploit this vulnerability in order to modify a security-critical UEFI variable without knowledge of the BIOS administrator.	2023-08-16	3.9	Low
CVE-2023-21232	google - multiple products	In multiple locations, there is a possible way to retrieve sensor data without permissions due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2023-08-14	3.3	Low
CVE-2023-21278	google - multiple products	In multiple locations, there is a possible way to obscure the microphone privacy indicator 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.	2023-08-14	3.3	Low
CVE-2022-32876	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13. A shortcut may be able to view the hidden photos album without authentication.	2023-08-14	3.3	Low
CVE-2022-46724	apple - multiple products	This issue was addressed by restricting options offered on a locked device. This issue is fixed in iOS 16.4 and iPadOS 16.4. A person with physical access to an iOS device may be able to view the last image used in Magnifier from the lock screen.	2023-08-14	2.4	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.