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

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٣ سبتمبر إلى ١٠ سبتمبر. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

- عالي جدًا: النتيجة الأساسية لـ CVSS 9.0-10.0
- عالي: النتيجة الأساسية لـ CVSS 7.0-8.9
- متوسط: النتيجة الأساسية لـ CVSS 4.0-6.9
- منخفض: النتيجة الأساسية لـ CVSS 0.0-3.9

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 3rd of September to 10th of September. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-4613	lg - lg_led_assistant	This vulnerability allows remote attackers to execute arbitrary code on affected installations of LG LED Assistant. Authentication is not required to exploit this vulnerability. The specific flaw exists within the /api/settings/upload endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of the current user.	2023-09-04	9.8	Critical
CVE-2023-4614	lg - lg_led_assistant	This vulnerability allows remote attackers to execute arbitrary code on affected installations of LG LED Assistant. Authentication is not required to exploit this vulnerability. The specific flaw exists within the /api/installation/setThumbnailRc endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of the current user.	2023-09-04	9.8	Critical
CVE-2023-28543	qualcomm - sd855_firmware	A malformed DLC can trigger Memory Corruption in SNPE library due to out of bounds read, such as by loading an untrusted model (e.g. from a remote source).	2023-09-05	9.8	Critical
CVE-2023-28562	qualcomm - aqt1000_firmware	Memory corruption while handling payloads from remote ESL.	2023-09-05	9.8	Critical
CVE-2023-28581	qualcomm - fastconnect_6800_firmware	Memory corruption in WLAN Firmware while parsing receieved GTK Keys in GTK KDE.	2023-09-05	9.8	Critical
CVE-2023-40743	apache - axis	** UNSUPPPORTED WHEN ASSIGNED ** ** UNSUPPORTED WHEN ASSIGNED ** When integrating Apache Axis 1.x in an application, it may not have been obvious that looking up a service through "ServiceFactory.getService" allows potentially dangerous lookup mechanisms such as LDAP. When passing untrusted input to this API method, this could expose the application to DoS, SSRF and even attacks leading to RCE. As Axis 1 has been EOL we recommend you migrate to a different SOAP engine, such as Apache Axis 2/Java. As a workaround, you may review your code to verify no untrusted or unsanitized input is passed to "ServiceFactory.getService", or by applying the patch from https://github.com/apache/axis-axis1-java/commit/7e66753427466590d6def0125e448d2791723210 . The Apache Axis project does not expect to create an Axis 1.x release fixing this problem, though contributors that would like to work towards this are welcome.	2023-09-05	9.8	Critical
CVE-2023-39361	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a SQL injection discovered in graph_view.php. Since guest users can access graph_view.php without authentication by default, if guest users are being utilized in an enabled state, there could be the potential for significant damage. Attackers may exploit this vulnerability, and there may be possibilities for actions such as the usurpation of administrative privileges or remote code execution. This issue has been addressed in version 1.2.25. Users are advised	2023-09-05	9.8	Critical

		to upgrade. There are no known workarounds for this vulnerability.			
CVE-2023-30723	samsung - health	Improper input validation vulnerability in Samsung Health prior to version 6.24.2.011 allows attackers to write arbitrary file with Samsung Health privilege.	2023-09-06	9.8	Critical
CVE-2023-37941	apache - superset	If an attacker gains write access to the Apache Superset metadata database, they could persist a specifically crafted Python object that may lead to remote code execution on Superset's web backend. This vulnerability impacts Apache Superset versions 1.5.0 up to and including 2.1.0.	2023-09-06	9.8	Critical
CVE-2023-20238	cisco - multiple products	A vulnerability in the single sign-on (SSO) implementation of Cisco BroadWorks Application Delivery Platform and Cisco BroadWorks Xtended Services Platform could allow an unauthenticated, remote attacker to forge the credentials required to access an affected system. This vulnerability is due to the method used to validate SSO tokens. An attacker could exploit this vulnerability by authenticating to the application with forged credentials. A successful exploit could allow the attacker to commit toll fraud or to execute commands at the privilege level of the forged account. If that account is an Administrator account, the attacker would have the ability to view confidential information, modify customer settings, or modify settings for other users. To exploit this vulnerability, the attacker would need a valid user ID that is associated with an affected Cisco BroadWorks system.	2023-09-06	9.8	Critical
CVE-2023-40397	apple - macos	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.5. A remote attacker may be able to cause arbitrary javascript code execution.	2023-09-06	9.8	Critical
CVE-2023-30908	hp - multiple products	A remote authentication bypass issue exists in a OneView API.	2023-09-07	9.8	Critical
CVE-2023-35892	ibm - financial_transaction_manager	IBM Financial Transaction Manager for SWIFT Services 3.2.4 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: 258786.	2023-09-05	9.1	Critical
CVE-2023-20269	cisco - multiple products	A vulnerability in the remote access VPN feature of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct a brute force attack in an attempt to identify valid username and password combinations or an authenticated, remote attacker to establish a clientless SSL VPN session with an unauthorized user. This vulnerability is due to improper separation of authentication, authorization, and accounting (AAA) between the remote access VPN feature and the HTTPS management and site-to-site VPN features. An attacker could exploit this vulnerability by specifying a default connection profile/tunnel group while conducting a brute force attack or while establishing a clientless SSL VPN session using valid credentials. A successful exploit could allow the attacker to achieve one or both of the following: Identify valid credentials that could then be used to establish an unauthorized remote access VPN session. Establish a clientless SSL VPN session (only when running Cisco ASA Software Release 9.16 or earlier). Notes: Establishing a client-based remote access VPN tunnel is not possible as these default connection profiles/tunnel groups do not and cannot have an IP address pool configured. This vulnerability does not allow an attacker to bypass authentication. To successfully establish a remote access VPN session, valid credentials are required, including a valid second factor if multi-factor authentication (MFA) is configured. Cisco will release software updates that address this vulnerability. There are workarounds that address this vulnerability.	2023-09-06	9.1	Critical
CVE-2022-33164	ibm - security_directory_server	IBM Security Directory Server 7.2.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../)	2023-09-08	9.1	Critical

		to view or write to arbitrary files on the system. IBM X-Force ID: 228579.			
CVE-2015-1391	hp - airwave	Aruba AirWave before 8.0.7 allows bypass of a CSRF protection mechanism.	2023-09-05	8.8	High
CVE-2023-39359	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. An authenticated SQL injection vulnerability was discovered which allows authenticated users to perform privilege escalation and remote code execution. The vulnerability resides in the `graphs.php` file. When dealing with the cases of ajax_hosts and ajax_hosts_noany, if the `site_id` parameter is greater than 0, it is directly reflected in the WHERE clause of the SQL statement. This creates an SQL injection vulnerability. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-09-05	8.8	High
CVE-2023-39357	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. A defect in the sql_save function was discovered. When the column type is numeric, the sql_save function directly utilizes user input. Many files and functions calling the sql_save function do not perform prior validation of user input, leading to the existence of multiple SQL injection vulnerabilities in Cacti. This allows authenticated users to exploit these SQL injection vulnerabilities to perform privilege escalation and remote code execution. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-09-05	8.8	High
CVE-2023-39358	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. An authenticated SQL injection vulnerability was discovered which allows authenticated users to perform privilege escalation and remote code execution. The vulnerability resides in the `reports_user.php` file. In `ajax_get_branches`, the `tree_id` parameter is passed to the `reports_get_branch_select` function without any validation. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-09-05	8.8	High
CVE-2023-4762	google - chrome	Type Confusion in V8 in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2023-09-05	8.8	High
CVE-2023-4763	google - chrome	Use after free in Networks in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-09-05	8.8	High
CVE-2023-29166	apple - pro_video_formats	A logic issue was addressed with improved state management. This issue is fixed in Pro Video Formats 2.2.5. A user may be able to elevate privileges.	2023-09-06	8.8	High
CVE-2023-32619	tp-link - archer_c55_firmware	Archer C50 firmware versions prior to 'Archer C50(JP)_V3_230505' and Archer C55 firmware versions prior to 'Archer C55(JP)_V1_230506' use hard-coded credentials to login to the affected device, which may allow a network-adjacent unauthenticated attacker to execute an arbitrary OS command.	2023-09-06	8.8	High
CVE-2023-36489	tp-link - tl-wr902ac_firmware	Multiple TP-LINK products allow a network-adjacent unauthenticated attacker to execute arbitrary OS commands. Affected products/versions are as follows: TL-WR802N firmware versions prior to 'TL-WR802N(JP)_V4_221008', TL-WR841N firmware versions prior to 'TL-WR841N(JP)_V14_230506', and TL-WR902AC firmware versions prior to 'TL-WR902AC(JP)_V3_230506'.	2023-09-06	8.8	High
CVE-2023-37284	tp-link - archer_c20_firmware	Improper authentication vulnerability in Archer C20 firmware versions prior to 'Archer C20(JP)_V1_230616' allows a network-adjacent unauthenticated attacker to execute an arbitrary OS command via a crafted request to bypass authentication.	2023-09-06	8.8	High
CVE-2023-38563	tp-link - archer_c1200_firmware	Archer C1200 firmware versions prior to 'Archer C1200(JP)_V2_230508' and Archer C9 firmware versions prior to 'Archer C9(JP)_V3_230508' allow a network-adjacent unauthenticated attacker to execute arbitrary OS commands.	2023-09-06	8.8	High
CVE-2023-38568	tp-link - archer_a10_firmware	Archer A10 firmware versions prior to 'Archer A10(JP)_V2_230504' allows a network-adjacent unauthenticated attacker to execute arbitrary OS commands.	2023-09-06	8.8	High
CVE-2023-41933	jenkins - job_configuration_history	Jenkins Job Configuration History Plugin 1227.v7a_79fc4dc01f and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks.	2023-09-06	8.8	High
CVE-2023-41939	jenkins - ssh2_easy	Jenkins SSH2 Easy Plugin 1.4 and earlier does not verify that permissions configured to be granted are enabled, potentially allowing users formerly granted (typically optional permissions, like Overall/Manage) to access functionality they're no longer entitled to.	2023-09-06	8.8	High
CVE-2023-41945	jenkins - assembla_auth	Jenkins Assembla Auth Plugin 1.14 and earlier does not verify that the permissions it grants are enabled, resulting in users with EDIT permissions to be granted Overall/Manage and	2023-09-06	8.8	High

		Overall/SystemRead permissions, even if those permissions are disabled and should not be granted.			
CVE-2023-4761	google - chrome	Out of bounds memory access in FedCM in Google Chrome prior to 116.0.5845.179 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	2023-09-05	8.1	High
CVE-2023-31188	tp-link - archer_c55_firmware	Multiple TP-LINK products allow a network-adjacent authenticated attacker to execute arbitrary OS commands. Affected products/versions are as follows: Archer C50 firmware versions prior to 'Archer C50(JP)_V3_230505', Archer C55 firmware versions prior to 'Archer C55(JP)_V1_230506', and Archer C20 firmware versions prior to 'Archer C20(JP)_V1_230616'.	2023-09-06	8	High
CVE-2023-38588	tp-link - archer_c3150_firmware	Archer C3150 firmware versions prior to 'Archer C3150(JP)_V2_230511' allows a network-adjacent authenticated attacker to execute arbitrary OS commands.	2023-09-06	8	High
CVE-2023-39224	tp-link - archer_c7_firmware	Archer C5 firmware all versions and Archer C7 firmware versions prior to 'Archer C7(JP)_V2_230602' allow a network-adjacent authenticated attacker to execute arbitrary OS commands. Note that Archer C5 is no longer supported, therefore the update for this product is not provided.	2023-09-06	8	High
CVE-2023-39935	tp-link - archer_c5400_firmware	Archer C5400 firmware versions prior to 'Archer C5400(JP)_V2_230506' allows a network-adjacent authenticated attacker to execute arbitrary OS commands.	2023-09-06	8	High
CVE-2023-40193	tp-link - deco_m4_firmware	Deco M4 firmware versions prior to 'Deco M4(JP)_V2_1.5.8 Build 20230619' allows a network-adjacent authenticated attacker to execute arbitrary OS commands.	2023-09-06	8	High
CVE-2023-40357	tp-link - archer_ax50_firmware	Multiple TP-LINK products allow a network-adjacent authenticated attacker to execute arbitrary OS commands. Affected products/versions are as follows: Archer AX50 firmware versions prior to 'Archer AX50(JP)_V1_230529', Archer A10 firmware versions prior to 'Archer A10(JP)_V2_230504', Archer AX10 firmware versions prior to 'Archer AX10(JP)_V1.2_230508', and Archer AX11000 firmware versions prior to 'Archer AX11000(JP)_V1_230523'.	2023-09-06	8	High
CVE-2023-40531	tp-link - archer_ax6000_firmware	Archer AX6000 firmware versions prior to 'Archer AX6000(JP)_V1_1.3.0 Build 20221208' allows a network-adjacent authenticated attacker to execute arbitrary OS commands.	2023-09-06	8	High
CVE-2023-38443	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	2023-09-04	7.8	High
CVE-2023-38444	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	2023-09-04	7.8	High
CVE-2023-38449	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	2023-09-04	7.8	High
CVE-2023-38450	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	2023-09-04	7.8	High
CVE-2023-38451	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	2023-09-04	7.8	High
CVE-2023-38452	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	2023-09-04	7.8	High
CVE-2023-38453	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	2023-09-04	7.8	High
CVE-2023-38455	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	2023-09-04	7.8	High
CVE-2023-38456	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	2023-09-04	7.8	High
CVE-2023-38458	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	2023-09-04	7.8	High
CVE-2023-38459	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	2023-09-04	7.8	High
CVE-2023-38460	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	2023-09-04	7.8	High
CVE-2023-38464	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local escalation of privilege with no additional execution privileges	2023-09-04	7.8	High
CVE-2023-28072	dell - alienware_command_center	Dell Alienware Command Center, versions prior to 5.5.51.0, contain a deserialization of untrusted data vulnerability. A local	2023-09-04	7.8	High

		malicious user could potentially send specially crafted requests to the .NET Remoting server to run arbitrary code on the system.			
CVE-2022-33275	qualcomm - 315_5g_iot_modem_firmware	Memory corruption due to improper validation of array index in WLAN HAL when received lm_itemNum is out of range.	2023-09-05	7.8	High
CVE-2022-40524	qualcomm - aqt1000_firmware	Memory corruption due to buffer over-read in Modem while processing SetNativeHandle RTP service.	2023-09-05	7.8	High
CVE-2022-40534	qualcomm - wcn685x-5_firmware	Memory corruption due to improper validation of array index in Audio.	2023-09-05	7.8	High
CVE-2023-21636	qualcomm - aqt1000_firmware	Memory Corruption due to improper validation of array index in Linux while updating adn record.	2023-09-05	7.8	High
CVE-2023-21644	qualcomm - aqt1000_firmware	Memory corruption in RIL due to Integer Overflow while triggering qcril_uim_request_apdu request.	2023-09-05	7.8	High
CVE-2023-21654	qualcomm - apq8096au_firmware	Memory corruption in Audio during playback session with audio effects enabled.	2023-09-05	7.8	High
CVE-2023-21655	qualcomm - qca6391_firmware	Memory corruption in Audio while validating and mapping metadata.	2023-09-05	7.8	High
CVE-2023-21662	qualcomm - aqt1000_firmware	Memory corruption in Core Platform while printing the response buffer in log.	2023-09-05	7.8	High
CVE-2023-21663	qualcomm - aqt1000_firmware	Memory Corruption while accessing metadata in Display.	2023-09-05	7.8	High
CVE-2023-21664	qualcomm - aqt1000_firmware	Memory Corruption in Core Platform while printing the response buffer in log.	2023-09-05	7.8	High
CVE-2023-28538	qualcomm - aqt1000_firmware	Memory corruption in WIN Product while invoking WinAcpi update driver in the UEFI region.	2023-09-05	7.8	High
CVE-2023-28544	qualcomm - aqt1000_firmware	Memory corruption in WLAN while sending transmit command from HLOS to UTF handlers.	2023-09-05	7.8	High
CVE-2023-28548	qualcomm - aqt1000_firmware	Memory corruption in WLAN HAL while processing Tx/Rx commands from QDART.	2023-09-05	7.8	High
CVE-2023-28549	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in WLAN HAL while parsing Rx buffer in processing TLV payload.	2023-09-05	7.8	High
CVE-2023-28557	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in WLAN HAL while processing command parameters from untrusted WMI payload.	2023-09-05	7.8	High
CVE-2023-28558	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in WLAN handler while processing PhyID in Tx status handler.	2023-09-05	7.8	High
CVE-2023-28559	qualcomm - aqt1000_firmware	Memory corruption in WLAN FW while processing command parameters from untrusted WMI payload.	2023-09-05	7.8	High
CVE-2023-28560	qualcomm - apq8076_firmware	Memory corruption in WLAN HAL while processing devIndex from untrusted WMI payload.	2023-09-05	7.8	High
CVE-2023-28564	qualcomm - aqt1000_firmware	Memory corruption in WLAN HAL while passing command parameters through WMI interfaces.	2023-09-05	7.8	High
CVE-2023-28565	qualcomm - 9205_lte_firmware	Memory corruption in WLAN HAL while handling command streams through WMI interfaces.	2023-09-05	7.8	High
CVE-2023-28567	qualcomm - 315_5g_iot_firmware	Memory corruption in WLAN HAL while handling command through WMI interfaces.	2023-09-05	7.8	High
CVE-2023-28573	qualcomm - 315_5g_iot_firmware	Memory corruption in WLAN HAL while parsing WMI command parameters.	2023-09-05	7.8	High
CVE-2023-33021	qualcomm - apq8064au_firmware	Memory corruption in Graphics while processing user packets for command submission.	2023-09-05	7.8	High
CVE-2023-31132	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a privilege escalation vulnerability. A low-privileged OS user with access to a Windows host where Cacti is installed can create arbitrary PHP files in a web document directory. The user can then execute the PHP files under the security context of SYSTEM. This allows an attacker to escalate privilege from a normal user account to SYSTEM. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-09-05	7.8	High
CVE-2023-28209	apple - macos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory.	2023-09-06	7.8	High
CVE-2023-28210	apple - macos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory.	2023-09-06	7.8	High
CVE-2023-28211	apple - macos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory.	2023-09-06	7.8	High

CVE-2023-28212	apple - macos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory.	2023-09-06	7.8	High
CVE-2023-28213	apple - macos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory.	2023-09-06	7.8	High
CVE-2023-28214	apple - macos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory.	2023-09-06	7.8	High
CVE-2023-28215	apple - macos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory.	2023-09-06	7.8	High
CVE-2023-32356	apple - macos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.3. An app may be able to cause unexpected system termination or write kernel memory.	2023-09-06	7.8	High
CVE-2023-32379	apple - macos	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Ventura 13.4. An app may be able to execute arbitrary code with kernel privileges.	2023-09-06	7.8	High
CVE-2023-32425	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.5 and iPadOS 16.5, watchOS 9.5. An app may be able to gain elevated privileges.	2023-09-06	7.8	High
CVE-2023-32426	apple - macos	A logic issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.3. An app may be able to gain root privileges.	2023-09-06	7.8	High
CVE-2023-32428	apple - multiple products	This issue was addressed with improved file handling. This issue is fixed in macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, watchOS 9.5. An app may be able to gain root privileges.	2023-09-06	7.8	High
CVE-2023-30710	samsung - multiple products	Improper input validation vulnerability in Knox AI prior to SMR Sep-2023 Release 1 allows local attackers to launch privileged activities.	2023-09-06	7.8	High
CVE-2023-30712	samsung - multiple products	Improper input validation in Settings Suggestions prior to SMR Sep-2023 Release 1 allows attackers to launch arbitrary activity.	2023-09-06	7.8	High
CVE-2023-30722	samsung - blockchain_keystore	Protection Mechanism Failure in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.13.5 allows local attacker to execute arbitrary code.	2023-09-06	7.8	High
CVE-2021-21088	adobe - multiple products	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by a Use After Free vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-06	7.8	High
CVE-2021-28644	adobe - multiple products	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by a Path traversal vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-06	7.8	High
CVE-2021-35980	adobe - multiple products	Acrobat Reader DC versions 2021.005.20054 (and earlier), 2020.004.30005 (and earlier) and 2017.011.30197 (and earlier) are affected by a Path traversal vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-06	7.8	High
CVE-2023-3777	linux - multiple products	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. When nf_tables_delrule() is flushing table rules, it is not checked whether the chain is bound and the chain's owner rule can also release the objects in certain circumstances. We recommend upgrading past commit 6eaf41e87a223ae6f8e7a28d6e78384ad7e407f8.	2023-09-06	7.8	High
CVE-2023-4015	linux - linux_kernel	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. On an error when building a nftables rule, deactivating immediate expressions in nft_immediate_deactivate() can lead unbinding the chain and objects be deactivated but later used.	2023-09-06	7.8	High

		We recommend upgrading past commit 0a771f7b266b02d262900c75f1e175c7fe76fec2.			
CVE-2023-4206	linux - linux_kernel	A use-after-free vulnerability in the Linux kernel's net/sched: cls_route component can be exploited to achieve local privilege escalation. When route4_change() is called on an existing filter, the whole tcf_result struct is always copied into the new instance of the filter. This causes a problem when updating a filter bound to a class, as tcf_unbind_filter() is always called on the old instance in the success path, decreasing filter_cnt of the still referenced class and allowing it to be deleted, leading to a use-after-free. We recommend upgrading past commit b80b829e9e2c1b3f7aae34855e04d8f6ecaf13c8.	2023-09-06	7.8	High
CVE-2023-4207	linux - linux_kernel	A use-after-free vulnerability in the Linux kernel's net/sched: cls_fw component can be exploited to achieve local privilege escalation. When fw_change() is called on an existing filter, the whole tcf_result struct is always copied into the new instance of the filter. This causes a problem when updating a filter bound to a class, as tcf_unbind_filter() is always called on the old instance in the success path, decreasing filter_cnt of the still referenced class and allowing it to be deleted, leading to a use-after-free. We recommend upgrading past commit 76e42ae831991c828cffa8c37736ebfb831ad5ec.	2023-09-06	7.8	High
CVE-2023-4208	linux - linux_kernel	A use-after-free vulnerability in the Linux kernel's net/sched: cls_u32 component can be exploited to achieve local privilege escalation. When u32_change() is called on an existing filter, the whole tcf_result struct is always copied into the new instance of the filter. This causes a problem when updating a filter bound to a class, as tcf_unbind_filter() is always called on the old instance in the success path, decreasing filter_cnt of the still referenced class and allowing it to be deleted, leading to a use-after-free. We recommend upgrading past commit 3044b16e7c6fe5d24b1cdbcf1bd0a9d92d1ebd81.	2023-09-06	7.8	High
CVE-2023-4623	linux - multiple products	A use-after-free vulnerability in the Linux kernel's net/sched: sch_hfsc (HFSC qdisc traffic control) component can be exploited to achieve local privilege escalation. If a class with a link-sharing curve (i.e. with the HFSC_FSC flag set) has a parent without a link-sharing curve, then init_vf() will call vttree_insert() on the parent, but vttree_remove() will be skipped in update_vf(). This leaves a dangling pointer that can cause a use-after-free. We recommend upgrading past commit b3d26c5702c7d6c45456326e56d2ccf3f103e60f.	2023-09-06	7.8	High
CVE-2021-40795	adobe - multiple products	Adobe Premiere Pro versions 22.0 (and earlier) and 15.4.2 (and earlier) are affected by an out-of-bounds read vulnerability which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	7.8	High
CVE-2021-43018	adobe - multiple products	Adobe Photoshop versions 23.0.2 and 22.5.4 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious JPG file.	2023-09-07	7.8	High
CVE-2021-43027	adobe - multiple products	Adobe After Effects versions 22.0 (and earlier) and 18.4.2 (and earlier) are affected by an out-of-bounds read vulnerability which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	7.8	High
CVE-2021-43753	adobe - lightroom	Adobe Lightroom versions 4.4 (and earlier) are affected by a use-after-free vulnerability in the processing of parsing TIF files that could result in privilege escalation. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	7.8	High
CVE-2021-44188	adobe - multiple products	Adobe After Effects versions 22.0 (and earlier) and 18.4.2 (and earlier) are affected by an out-of-bounds read vulnerability which could result in a read past the end of an allocated memory	2023-09-07	7.8	High

متاح

		structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
CVE-2022-30637	adobe - multiple products	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	7.8	High
CVE-2022-30638	adobe - multiple products	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	7.8	High
CVE-2022-30639	adobe - multiple products	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	7.8	High
CVE-2022-30640	adobe - multiple products	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	7.8	High
CVE-2022-30641	adobe - multiple products	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	7.8	High
CVE-2022-30642	adobe - multiple products	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	7.8	High
CVE-2022-30643	adobe - multiple products	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	7.8	High
CVE-2022-30644	adobe - multiple products	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by a Use-After-Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	7.8	High
CVE-2022-30645	adobe - multiple products	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	7.8	High
CVE-2022-30646	adobe - multiple products	Adobe Illustrator versions 26.0.2 (and earlier) and 25.4.5 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	7.8	High
CVE-2023-41061	apple - multiple products	A validation issue was addressed with improved logic. This issue is fixed in watchOS 9.6.2, iOS 16.6.1 and iPadOS 16.6.1. A maliciously crafted attachment may result in arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.	2023-09-07	7.8	High
CVE-2023-41064	apple - multiple products	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6.9, macOS Big Sur 11.7.10, macOS Ventura 13.5.2, iOS 16.6.1 and iPadOS 16.6.1, iOS 15.7.9 and iPadOS 15.7.9. Processing a maliciously crafted image may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.	2023-09-07	7.8	High
CVE-2023-4807	openssl - multiple products	Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications on the Windows 64 platform when running on newer X86_64 processors supporting the AVX512-IFMA instructions. Impact summary: If in an application that uses the OpenSSL library an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences.	2023-09-08	7.8	High

متاح

		The POLY1305 MAC (message authentication code) implementation in OpenSSL does not save the contents of non-volatile XMM registers on Windows 64 platform when calculating the MAC of data larger than 64 bytes. Before returning to the caller all the XMM registers are set to zero rather than restoring their previous content. The vulnerable code is used only on newer x86_64 processors supporting the AVX512-IFMA instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However given the contents of the registers are just zeroized so the attacker cannot put arbitrary values inside, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3 and a malicious client can influence whether this AEAD cipher is used by the server. This implies that server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. As a workaround the AVX512-IFMA instructions support can be disabled at runtime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=:~0x200000 The FIPS provider is not affected by this issue.			
CVE-2023-38736	ibm - qradar_wincollect	IBM QRadar WinCollect Agent 10.0 through 10.1.6, when installed to run as ADMIN or SYSTEM, is vulnerable to a local escalation of privilege attack that a normal user could utilize to gain SYSTEM permissions. IBM X-Force ID: 262542.	2023-09-08	7.8	High
CVE-2023-33914	google - multiple products	In NIA0 algorithm in Security Mode Command, there is a possible missing verification incorrect input. This could lead to remote information disclosure no additional execution privileges needed	2023-09-04	7.5	High
CVE-2023-33915	google - android	In LTE protocol stack, there is a possible missing permission check. This could lead to remote information disclosure no additional execution privileges needed	2023-09-04	7.5	High
CVE-2023-4615	lg - lg_led_assistant	This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG LED Assistant. Authentication is not required to exploit this vulnerability. The specific flaw exists within the /api/download/updateFile endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of the current user.	2023-09-04	7.5	High
CVE-2023-4616	lg - lg_led_assistant	This vulnerability allows remote attackers to disclose sensitive information on affected installations of LG LED Assistant. Authentication is not required to exploit this vulnerability. The specific flaw exists within the /api/thumbnail endpoint. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose information in the context of the current user.	2023-09-04	7.5	High
CVE-2023-35906	ibm - aspera_faspex	IBM Aspera Faspex 5.0.5 could allow a remote attacked to bypass IP restrictions due to improper access controls. IBM X-Force ID: 259649.	2023-09-05	7.5	High

متاح

CVE-2023-21646	qualcomm - ar8035_firmware	Transient DOS in Modem while processing invalid System Information Block 1.	2023-09-05	7.5	High
CVE-2023-21653	qualcomm - ar8035_firmware	Transient DOS in Modem while processing RRC reconfiguration message.	2023-09-05	7.5	High
CVE-2023-28584	qualcomm - aqt1000_firmware	Transient DOS in WLAN Host when a mobile station receives invalid channel in CSA IE while doing channel switch announcement (CSA).	2023-09-05	7.5	High
CVE-2023-33015	qualcomm - 315_5g_firmware	Transient DOS in WLAN Firmware while interpreting MBSSID IE of a received beacon frame.	2023-09-05	7.5	High
CVE-2023-33016	qualcomm - csr8811_firmware	Transient DOS in WLAN firmware while parsing MLO (multi-link operation).	2023-09-05	7.5	High
CVE-2023-33019	qualcomm - 9206_lte_firmware	Transient DOS in WLAN Host while doing channel switch announcement (CSA), when a mobile station receives invalid channel in CSA IE.	2023-09-05	7.5	High
CVE-2023-33020	qualcomm - 9206_lte_firmware	Transient DOS in WLAN Host when an invalid channel (like channel out of range) is received in STA during CSA IE.	2023-09-05	7.5	High
CVE-2023-30708	samsung - multiple products	Improper authentication in SecSettings prior to SMR Sep-2023 Release 1 allows attacker to access Captive Portal Wi-Fi in Reactivation Lock status.	2023-09-06	7.5	High
CVE-2023-30729	samsung - email	Improper Certificate Validation in Samsung Email prior to version 6.1.82.0 allows remote attacker to intercept the network traffic including sensitive information.	2023-09-06	7.5	High
CVE-2023-41935	jenkins - multiple products	Jenkins Azure AD Plugin 396.v86ce29279947 and earlier, except 378.380.v545b_1154b_3fb_, uses a non-constant time comparison function when checking whether the provided and expected CSRF protection nonce are equal, potentially allowing attackers to use statistical methods to obtain a valid nonce.	2023-09-06	7.5	High
CVE-2023-41936	jenkins - google_login	Jenkins Google Login Plugin 1.7 and earlier uses a non-constant time comparison function when checking whether the provided and expected token are equal, potentially allowing attackers to use statistical methods to obtain a valid token.	2023-09-06	7.5	High
CVE-2023-41937	jenkins - bitbucket_push_and_pull_request	Jenkins Bitbucket Push and Pull Request Plugin 2.4.0 through 2.8.3 (both inclusive) trusts values provided in the webhook payload, including certain URLs, and uses configured Bitbucket credentials to connect to those URLs, allowing attackers to capture Bitbucket credentials stored in Jenkins by sending a crafted webhook payload.	2023-09-06	7.5	High
CVE-2023-30800	mikrotik - routeros	The web server used by MikroTik RouterOS version 6 is affected by a heap memory corruption issue. A remote and unauthenticated attacker can corrupt the server's heap memory by sending a crafted HTTP request. As a result, the web interface crashes and is immediately restarted. The issue was fixed in RouterOS 6.49.10 stable. RouterOS version 7 is not affected.	2023-09-07	7.5	High
CVE-2023-37368	samsung - exynos_9810_firmware	An issue was discovered in Samsung Exynos Mobile Processor, Automotive Processor, and Modem (Exynos Mobile Processor, Automotive Processor, and Modem - Exynos 9810, Exynos 9610, Exynos 9820, Exynos 980, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos 9110, Exynos W920, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123). In the Shannon MM Task, Missing validation of a NULL pointer can cause abnormal termination via a malformed NR MM packet.	2023-09-08	7.5	High
CVE-2023-37377	samsung - exynos_980_firmware	An issue was discovered in Samsung Exynos Mobile Processor and Wearable Processor (Exynos 980, Exynos 850, Exynos 2100, and Exynos W920). Improper handling of length parameter inconsistency can cause incorrect packet filtering.	2023-09-08	7.5	High
CVE-2023-30995	ibm - aspera_faspex	IBM Aspera Faspex 5.0.5 could allow a malicious actor to bypass IP whitelist restrictions using a specially crafted HTTP request. IBM X-Force ID: 254268.	2023-09-08	7.5	High
CVE-2022-22401	ibm - aspera_faspex	IBM Aspera Faspex 5.0.5 could allow a remote attacker to gather or persuade a naive user to supply sensitive information. IBM X-Force ID: 222567.	2023-09-08	7.5	High
CVE-2021-40698	adobe - multiple products	ColdFusion version 2021 update 1 (and earlier) and versions 2018.10 (and earlier) are impacted by an Use of Inherently Dangerous Function vulnerability that can lead to a security feature bypass??. An authenticated attacker could leverage this vulnerability to access and manipulate arbitrary data on the environment.	2023-09-07	7.4	High
CVE-2021-40699	adobe - multiple products	ColdFusion version 2021 update 1 (and earlier) and versions 2018.10 (and earlier) are impacted by an improper access control vulnerability when checking permissions in the CFIDE path. An authenticated attacker could leverage this vulnerability to access and manipulate arbitrary data on the environment.	2023-09-07	7.4	High
CVE-2015-2201	arubanetworks - multiple products	Aruba AirWave before 7.7.14.2 and 8.x before 8.0.7 allows VisualRF remote OS command execution and file disclosure by administrative users.	2023-09-05	7.2	High
CVE-2015-2202	arubanetworks - multiple products	Aruba AirWave before 7.7.14.2 and 8.x before 8.0.7 allows administrative users to escalate privileges to root on the underlying OS.	2023-09-05	7.2	High

CVE-2023-39362	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. In Cacti 1.2.24, under certain conditions, an authenticated privileged user, can use a malicious string in the SNMP options of a Device, performing command injection and obtaining remote code execution on the underlying server. The `lib/snmp.php` file has a set of functions, with similar behavior, that accept in input some variables and place them into an `exec` call without a proper escape or validation. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-09-05	7.2	High
CVE-2023-20250	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an authenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to improper validation of requests that are sent to the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface. A successful exploit could allow the attacker to execute arbitrary code with root privileges on an affected device. To exploit this vulnerability, the attacker must have valid Administrator credentials on the affected device.	2023-09-06	7.2	High
CVE-2023-40060	solarwinds - multiple products	A vulnerability has been identified within Serv-U 15.4 and 15.4 Hotfix 1 that, if exploited, allows an actor to bypass multi-factor/two-factor authentication. The actor must have administrator-level access to Serv-U to perform this action. 15.4. SolarWinds found that the issue was not completely fixed in 15.4 Hotfix 1.	2023-09-07	7.2	High
CVE-2023-30707	samsung - multiple products	Improper input validation vulnerability in FileProviderStatusReceiver in Samsung Keyboard prior to SMR Sep-2023 Release 1 allows local attackers to delete arbitrary files with Samsung Keyboard privilege.	2023-09-06	7.1	High
CVE-2023-4244	linux - linux_kernel	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tables component can be exploited to achieve local privilege escalation. Due to a race condition between nf_tables netlink control plane transaction and nft_set element garbage collection, it is possible to underflow the reference counter causing a use-after-free vulnerability. We recommend upgrading past commit 3e91b0ebd994635df2346353322ac51ce84ce6d8.	2023-09-06	7	High
CVE-2023-4622	linux - linux_kernel	A use-after-free vulnerability in the Linux kernel's af_unix component can be exploited to achieve local privilege escalation. The unix_stream_sendpage() function tries to add data to the last skb in the peer's recv queue without locking the queue. Thus there is a race where unix_stream_sendpage() could access an skb locklessly that is being released by garbage collection, resulting in use-after-free. We recommend upgrading past commit 790c2f9d15b594350ae9bca7b236f2b1859de02c.	2023-09-06	7	High
CVE-2023-38616	apple - macos	A race condition was addressed with improved state handling. This issue is fixed in macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	2023-09-06	7	High
CVE-2023-35719	zohocorp - manageengine_adselfservice_plus	ManageEngine ADSelfService Plus GINA Client Insufficient Verification of Data Authenticity Authentication Bypass Vulnerability. This vulnerability allows physically present attackers to execute arbitrary code on affected installations of ManageEngine ADSelfService Plus. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Password Reset Portal used by the GINA client. The issue results from the lack of proper authentication of data received via HTTP. An attacker can leverage this vulnerability to bypass authentication and execute code in the context of SYSTEM. Was ZDI-CAN-17009.	2023-09-06	6.8	Medium
CVE-2023-38553	google - android	In gnss service, 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	2023-09-04	6.7	Medium
CVE-2023-20822	google - multiple products	In netdagent, 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: ALPS07944012; Issue ID: ALPS07944012.	2023-09-04	6.7	Medium

CVE-2023-20837	google - multiple products	In seninf, 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: ALPS07992786; Issue ID: ALPS07992786.	2023-09-04	6.7	Medium
CVE-2023-30709	samsung - multiple products	Improper access control in Dual Messenger prior to SMR Sep-2023 Release 1 allows local attackers launch activity with system privilege.	2023-09-06	6.7	Medium
CVE-2023-32805	google - multiple products	In power, there is a possible out of bounds write due to an insecure default value. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08102892; Issue ID: ALPS08102892.	2023-09-04	6.5	Medium
CVE-2022-43903	ibm - multiple products	IBM Security Guardium 10.6, 11.3, and 11.4 could allow an authenticated user to cause a denial of service due to due to improper input validation. IBM X-Force ID: 240894.	2023-09-05	6.5	Medium
CVE-2023-21667	qualcomm - qca6390_firmware	Transient DOS in Bluetooth HOST while passing descriptor to validate the blacklisted BT keyboard.	2023-09-05	6.5	Medium
CVE-2023-4764	google - chrome	Incorrect security UI in BFCache in Google Chrome prior to 116.0.5845.179 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: High)	2023-09-05	6.5	Medium
CVE-2023-28187	apple - macos	This issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.3. A user may be able to cause a denial-of-service.	2023-09-06	6.5	Medium
CVE-2023-28188	apple - macos	A denial-of-service issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.3. A remote user may be able to cause a denial-of-service.	2023-09-06	6.5	Medium
CVE-2023-32362	apple - macos	Error handling was changed to not reveal sensitive information. This issue is fixed in macOS Ventura 13.3. A website may be able to track sensitive user information.	2023-09-06	6.5	Medium
CVE-2023-41932	jenkins - job_configuration_history	Jenkins Job Configuration History Plugin 1227.v7a_79fc4dc01f and earlier does not restrict 'timestamp' query parameters in multiple endpoints, allowing attackers with to delete attacker-specified directories on the Jenkins controller file system as long as they contain a file called 'history.xml'.	2023-09-06	6.5	Medium
CVE-2023-41938	jenkins - ivy	A cross-site request forgery (CSRF) vulnerability in Jenkins Ivy Plugin 2.5 and earlier allows attackers to delete disabled modules.	2023-09-06	6.5	Medium
CVE-2023-41943	jenkins - aws_codecommit_trigger	Jenkins AWS CodeCommit Trigger Plugin 3.0.12 and earlier does not perform a permission check in an HTTP endpoint, allowing attackers with Overall/Read permission to clear the SQS queue.	2023-09-06	6.5	Medium
CVE-2023-39265	apache - superset	Apache Superset would allow for SQLite database connections to be incorrectly registered when an attacker uses alternative driver names like sqlite+pysqlite or by using database imports. This could allow for unexpected file creation on Superset webservers. Additionally, if Apache Superset is using a SQLite database for its metadata (not advised for production use) it could result in more severe vulnerabilities related to confidentiality and integrity. This vulnerability exists in Apache Superset versions up to and including 2.1.0.	2023-09-06	6.5	Medium
CVE-2023-20827	google - multiple products	In ims service, there is a possible memory corruption 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: ALPS07937105; Issue ID: ALPS07937105.	2023-09-04	6.4	Medium
CVE-2023-20834	google - multiple products	In pda, 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: ALPS07608514; Issue ID: ALPS07608514.	2023-09-04	6.4	Medium
CVE-2023-38484	arubanetworks - multiple products	Vulnerabilities exist in the BIOS implementation of Aruba 9200 and 9000 Series Controllers and Gateways that could allow an attacker to execute arbitrary code early in the boot sequence. An attacker could exploit this vulnerability to gain access to and change underlying sensitive information in the affected controller leading to complete system compromise.	2023-09-06	6.4	Medium
CVE-2023-38485	arubanetworks - multiple products	Vulnerabilities exist in the BIOS implementation of Aruba 9200 and 9000 Series Controllers and Gateways that could allow an attacker to execute arbitrary code early in the boot sequence. An attacker could exploit this vulnerability to gain access to and change underlying sensitive information in the affected controller leading to complete system compromise.	2023-09-06	6.4	Medium
CVE-2023-38486	arubanetworks - multiple products	A vulnerability in the secure boot implementation on affected Aruba 9200 and 9000 Series Controllers and Gateways allows an attacker to bypass security controls which would normally prohibit unsigned kernel images from executing. An attacker can use this vulnerability to execute arbitrary runtime operating systems, including unverified and unsigned OS images.	2023-09-06	6.4	Medium

CVE-2023-20851	google - multiple products	In stc, there is a possible out of bounds read due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is needed for exploitation. Patch ID: ALPS08048635; Issue ID: ALPS08048635.	2023-09-04	6.3	Medium
CVE-2023-39365	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. Issues with Cacti Regular Expression validation combined with the external links feature can lead to limited SQL Injections and subsequent data leakage. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-09-05	6.3	Medium
CVE-2015-1390	hp - airwave	Aruba AirWave before 8.0.7 allows XSS attacks agsinat an administrator.	2023-09-05	6.1	Medium
CVE-2023-39360	cacti - cacti	Cacti is an open source operational monitoring and fault management framework.Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability allows an authenticated user to poison data. The vulnerability is found in `graphs_new.php`. Several validations are performed, but the `returnto` parameter is directly passed to `form_save_button`. In order to bypass this validation, returnto must contain `host.php`. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to update should manually filter HTML output.	2023-09-05	6.1	Medium
CVE-2023-41944	jenkins - aws_codecommit_trigger	Jenkins AWS CodeCommit Trigger Plugin 3.0.12 and earlier does not escape the queue name parameter passed to a form validation URL, when rendering an error message, resulting in an HTML injection vulnerability.	2023-09-06	6.1	Medium
CVE-2023-40306	sap - multiple products	SAP S/4HANA Manage Catalog Items and Cross-Catalog searches Fiori apps allow an attacker to redirect users to a malicious site due to insufficient URL validation. As a result, it may have a slight impact on confidentiality and integrity.	2023-09-08	6.1	Medium
CVE-2023-41180	apache - nifi_minifi_c\+\+	Incorrect certificate validation in InvokeHTTP on Apache NiFi MiNiFi C++ versions 0.13 to 0.14 allows an intermediary to present a forged certificate during TLS handshake negotation. The Disable Peer Verification property of InvokeHTTP was effectively flipped, disabling verification by default, when using HTTPS. Mitigation: Set the Disable Peer Verification property of InvokeHTTP to true when using MiNiFi C++ versions 0.13.0 or 0.14.0. Upgrading to MiNiFi C++ 0.15.0 corrects the default behavior.	2023-09-03	5.9	Medium
CVE-2023-22870	ibm - aspera_faspex	IBM Aspera Faspex 5.0.5 transmits sensitive information in cleartext which could be obtained by an attacker using man in the middle techniques. IBM X-Force ID: 244121.	2023-09-05	5.9	Medium
CVE-2022-22405	ibm - aspera_faspex	IBM Aspera Faspex 5.0.5 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 222576.	2023-09-08	5.9	Medium
CVE-2023-33916	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-33917	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-33918	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38436	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38437	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38438	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38439	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38440	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38441	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38442	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-09-04	5.5	Medium

CVE-2023-38445	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38446	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38447	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38448	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38454	google - android	In vowifi service, there is a possible missing permission check.This could lead to local information disclosure with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38457	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38461	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38462	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38463	google - android	In vowifiservice, there is a possible missing permission check.This could lead to local denial of service with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38465	google - multiple products	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38466	google - multiple products	In ims service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-38554	google - multiple products	In wcn bsp driver, there is a possible out of bounds write due to a missing bounds check.This could lead to local denial of service with no additional execution privileges	2023-09-04	5.5	Medium
CVE-2023-20824	google - multiple products	In duraspeed, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privilege needed. User interaction is not needed for exploitation. Patch ID: ALPS07951402; Issue ID: ALPS07951402.	2023-09-04	5.5	Medium
CVE-2023-20825	google - multiple products	In duraspeed, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privilege needed. User interaction is not needed for exploitation. Patch ID: ALPS07951402; Issue ID: ALPS07951413.	2023-09-04	5.5	Medium
CVE-2023-20826	google - multiple products	In cta, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure with no additional execution privilege needed. User interaction is not needed for exploitation. Patch ID: ALPS07978550; Issue ID: ALPS07978550.	2023-09-04	5.5	Medium
CVE-2023-32338	ibm - multiple products	IBM Sterling Secure Proxy and IBM Sterling External Authentication Server 6.0.3 and 6.1.0 stores user credentials in plain clear text which can be read by a local user with container access. IBM X-Force ID: 255585.	2023-09-05	5.5	Medium
CVE-2023-29261	ibm - multiple products	IBM Sterling Secure Proxy 6.0.3 and 6.1.0 could allow a local user with specific information about the system to obtain privileged information due to inadequate memory clearing during operations. IBM X-Force ID: 252139.	2023-09-05	5.5	Medium
CVE-2022-33220	qualcomm - aqt1000_firmware	Information disclosure in Automotive multimedia due to buffer over-read.	2023-09-05	5.5	Medium
CVE-2022-32920	apple - xcode	The issue was addressed with improved checks. This issue is fixed in Xcode 14.0. Parsing a file may lead to disclosure of user information.	2023-09-06	5.5	Medium
CVE-2023-27950	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.	2023-09-06	5.5	Medium
CVE-2023-32432	apple - multiple products	A privacy issue was addressed with improved handling of temporary files. This issue is fixed in macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, watchOS 9.5. An app may be able to access user-sensitive data.	2023-09-06	5.5	Medium
CVE-2023-32438	apple - multiple products	This issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in tvOS 16.3, macOS Ventura 13.2, watchOS 9.3, iOS 16.3 and iPadOS 16.3. An app may be able to bypass Privacy preferences.	2023-09-06	5.5	Medium
CVE-2023-30713	samsung - multiple products	Improper privilege management vulnerability in FolderLockNotifier in One UI Home prior to SMR Sep-2023 Release 1 allows local attackers to change some settings of the folder lock.	2023-09-06	5.5	Medium

CVE-2023-30716	samsung - multiple products	Improper access control vulnerability in SVCAgent prior to SMR Sep-2023 Release 1 allows attackers to trigger certain commands.	2023-09-06	5.5	Medium
CVE-2023-30720	samsung - multiple products	PendingIntent hijacking in LmsAssemblyTrackerCTC prior to SMR Sep-2023 Release 1 allows local attacker to gain arbitrary file access.	2023-09-06	5.5	Medium
CVE-2023-30725	samsung - gallery	Improper authentication in LocalProvier of Gallery prior to version 14.5.01.2 allows attacker to access the data in content provider.	2023-09-06	5.5	Medium
CVE-2023-30726	samsung - gamelauncher	PendingIntent hijacking vulnerability in GameLauncher prior to version 4.2.59.5 allows local attackers to access data.	2023-09-06	5.5	Medium
CVE-2023-30728	samsung - packageinstallerchn	Intent redirection vulnerability in PackageInstallerCHN prior to version 13.1.03.00 allows local attacker to access arbitrary file. This vulnerability requires user interaction.	2023-09-06	5.5	Medium
CVE-2023-30730	samsung - camera	Implicit intent hijacking vulnerability in Camera prior to versions 11.0.16.43 in Android 11, 12.1.00.30, 12.0.07.53, 12.1.03.10 in Android 12, and 13.0.01.43, 13.1.00.83 in Android 13 allows local attacker to access specific file.	2023-09-06	5.5	Medium
CVE-2021-36060	adobe - media_encoder	Adobe Media Encoder version 15.2 (and earlier) is affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-06	5.5	Medium
CVE-2021-39859	adobe - multiple products	Acrobat Reader DC versions 2021.005.20060 (and earlier), 2020.004.30006 (and earlier) and 2017.011.30199 (and earlier) are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-06	5.5	Medium
CVE-2021-40723	adobe - multiple products	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	5.5	Medium
CVE-2021-40790	adobe - multiple products	Adobe Premiere Pro versions 22.0 (and earlier) and 15.4.2 (and earlier) are affected by an Use-After-Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	5.5	Medium
CVE-2021-40791	adobe - multiple products	Adobe Premiere Pro versions 22.0 (and earlier) and 15.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	5.5	Medium
CVE-2021-42265	adobe - multiple products	Adobe Premiere Pro versions 22.0 (and earlier) and 15.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	5.5	Medium
CVE-2021-42734	adobe - photoshop	Adobe Photoshop version 22.5.1 ?and earlier?versions???are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	5.5	Medium
CVE-2023-32470	dell - digital_delivery	Dell Digital Delivery versions prior to 5.0.82.0 contain an Insecure Operation on Windows Junction / Mount Point vulnerability. A local malicious user could potentially exploit this vulnerability to create arbitrary folder leading to permanent Denial of Service (DOS).	2023-09-08	5.5	Medium
CVE-2023-39513	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability which allows an authenticated user to poison data stored in the _cacti_'s database. These data will be viewed by administrative _cacti_ accounts and execute JavaScript code in the victim's browser at view-time. The script under `host.php` is used to monitor and manage hosts in the _cacti_ app, hence displays useful information such as data queries and verbose logs. _CENSUS_ found that an adversary that is able to configure a data-query template with malicious code appended in the template path, in order to deploy a stored XSS attack against any user with the _General Administration>Sites/Devices/Data_ privileges. A user that possesses the _Template Editor>Data Queries_ permissions can	2023-09-05	5.4	Medium

		configure the data query template path in _cacti_. Please note that such a user may be a low privileged user. This configuration occurs through `http://<HOST>/cacti/data_queries.php` by editing an existing or adding a new data query template. If a template is linked to a device then the formatted template path will be rendered in the device's management page, when a _verbose data query_ is requested. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to update should manually filter HTML output.			
CVE-2023-39514	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability which allows an authenticated user to poison data stored in the _cacti_'s database. These data will be viewed by administrative _cacti_ accounts and execute JavaScript code in the victim's browser at view-time. The script under `graphs.php` displays graph details such as data-source paths, data template information and graph related fields. _CENSUS_ found that an adversary that is able to configure either a data-source template with malicious code appended in the data-source name or a device with a malicious payload injected in the device name, may deploy a stored XSS attack against any user with _General Administration>Graphs_ privileges. A user that possesses the _Template Editor>Data Templates_ permissions can configure the data-source name in _cacti_. Please note that this may be a _low privileged_ user. This configuration occurs through `http://<HOST>/cacti/data_templates.php` by editing an existing or adding a new data template. If a template is linked to a graph then the formatted template name will be rendered in the graph's management page. A user that possesses the _General Administration>Sites/Devices/Data_ permissions can configure the device name in _cacti_. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to upgrade should add manual HTML escaping.	2023-09-05	5.4	Medium
CVE-2023-39364	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. In Cacti 1.2.24, users with console access can be redirected to an arbitrary website after a change password performed via a specifically crafted URL. The `auth_changepassword.php` file accepts `ref` as a URL parameter and reflects it in the form used to perform the change password. It's value is used to perform a redirect via `header` PHP function. A user can be tricked in performing the change password operation, e.g., via a phishing message, and then interacting with the malicious website where the redirection has been performed, e.g., downloading malwares, providing credentials, etc. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-09-05	5.4	Medium
CVE-2023-36387	apache - superset	An improper default REST API permission for Gamma users in Apache Superset up to and including 2.1.0 allows for an authenticated Gamma user to test database connections.	2023-09-06	5.4	Medium
CVE-2023-36388	apache - superset	Improper REST API permission in Apache Superset up to and including 2.1.0 allows for an authenticated Gamma users to test network connections, possible SSRF.	2023-09-06	5.4	Medium
CVE-2023-41931	jenkins - job_configuration_ history	Jenkins Job Configuration History Plugin 1227.v7a_79fc4dc01f and earlier does not property sanitize or escape the timestamp value from history entries when rendering a history entry on the history view, resulting in a stored cross-site scripting (XSS) vulnerability.	2023-09-06	5.4	Medium
CVE-2023-41940	jenkins - tap	Jenkins TAP Plugin 2.3 and earlier does not escape TAP file contents, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control TAP file contents.	2023-09-06	5.4	Medium
CVE-2023-32332	ibm - multiple products	IBM Maximo Application Suite 8.9, 8.10 and IBM Maximo Asset Management 7.6.1.2, 7.6.1.3 are vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 255072.	2023-09-08	5.4	Medium
CVE-2022-22402	ibm - aspera_faspex	IBM Aspera Faspex 5.0.5 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: 222571.	2023-09-08	5.4	Medium
CVE-2023-32370	apple - macos	A logic issue was addressed with improved validation. This issue is fixed in macOS Ventura 13.3. Content Security Policy to block domains with wildcards may fail.	2023-09-06	5.3	Medium
CVE-2023-34352	apple - multiple products	A permissions issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Ventura 13.4, tvOS 16.5, iOS 16.5 and iPadOS 16.5, watchOS 9.5. An attacker may be able to leak user account emails.	2023-09-06	5.3	Medium

متاح

CVE-2023-41934	jenkins - pipeline_maven_integration	Jenkins Pipeline Maven Integration Plugin 1330.v18e473854496 and earlier does not properly mask (i.e., replace with asterisks) usernames of credentials specified in custom Maven settings in Pipeline build logs if "Treat username as secret" is checked.	2023-09-06	5.3	Medium
CVE-2023-37367	samsung - exynos_9820_firmware	An issue was discovered in Samsung Exynos Mobile Processor, Automotive Processor, and Modem (Exynos 9820, Exynos 980, Exynos 850, Exynos 1080, Exynos 2100, Exynos 2200, Exynos 1280, Exynos 1380, Exynos 1330, Exynos Modem 5123, Exynos Modem 5300, and Exynos Auto T5123. In the NAS Task, an improperly implemented security check for standard can disallow desired services for a while via consecutive NAS messages.	2023-09-08	5.3	Medium
CVE-2023-24965	ibm - aspera_faspex	IBM Aspera Faspex 5.0.5 does not restrict or incorrectly restricts access to a resource from an unauthorized actor. IBM X-Force ID: 246713.	2023-09-08	5.3	Medium
CVE-2022-22409	ibm - aspera_faspex	IBM Aspera Faspex 5.0.5 could allow a remote attacker to gather sensitive information about the web application, caused by an insecure configuration. IBM X-Force ID: 222592.	2023-09-08	5.3	Medium
CVE-2023-30706	samsung - multiple products	Improper authorization in Samsung Keyboard prior to SMR Sep-2023 Release 1 allows attacker to read arbitrary file with system privilege.	2023-09-06	4.9	Medium
CVE-2023-39366	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability allows an authenticated user to poison data stored in the _cacti_'s database. These data will be viewed by administrative _cacti_ accounts and execute JavaScript code in the victim's browser at view-time. The `data_sources.php` script displays the data source management information (e.g. data source path, polling configuration etc.) for different data visualizations of the _cacti_ app. CENSUS found that an adversary that is able to configure a malicious Device name, can deploy a stored XSS attack against any user of the same (or broader) privileges. A user that possesses the _General Administration>Sites/Devices/Data_ permissions can configure the device names in _cacti_. This configuration occurs through `http://<HOST>/cacti/host.php`, while the rendered malicious payload is exhibited at `http://<HOST>/cacti/data_sources.php`. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to update should manually filter HTML output.	2023-09-05	4.8	Medium
CVE-2023-39510	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability allows an authenticated user to poison data stored in the _cacti_'s database. These data will be viewed by administrative _cacti_ accounts and execute JavaScript code in the victim's browser at view-time. The`reports_admin.php` script displays reporting information about graphs, devices, data sources etc. CENSUS found that an adversary that is able to configure a malicious Device name, can deploy a stored XSS attack against any user of the same (or broader) privileges. A user that possesses the _General Administration>Sites/Devices/Data_ permissions can configure the device names in _cacti_. This configuration occurs through `http://<HOST>/cacti/host.php`, while the rendered malicious payload is exhibited at `http://<HOST>/cacti/reports_admin.php` when the a graph with the maliciously altered device name is linked to the report. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to update should manually filter HTML output.	2023-09-05	4.8	Medium
CVE-2023-39512	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability which allows an authenticated user to poison data stored in the _cacti_'s database. These data will be viewed by administrative _cacti_ accounts and execute JavaScript code in the victim's browser at view-time. The script under `data_sources.php` displays the data source management information (e.g. data source path, polling configuration, device name related to the datasource etc.) for different data visualizations of the _cacti_ app. _CENSUS_ found that an adversary that is able to configure a malicious device name, can deploy a stored XSS attack against any user of the same (or broader) privileges. A user that possesses the _General Administration>Sites/Devices/Data_ permissions can configure the device names in _cacti_. This configuration occurs through `http://<HOST>/cacti/host.php`, while the rendered malicious payload is exhibited at `http://<HOST>/cacti/data_sources.php`. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to update should manually filter HTML output.	2023-09-05	4.8	Medium

CVE-2023-39515	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability allows an authenticated user to poison data stored in the cacti's database. These data will be viewed by administrative cacti accounts and execute JavaScript code in the victim's browser at view-time. The script under `data_debug.php` displays data source related debugging information such as _data source paths, polling settings, meta-data on the data source_. _CENSUS_ found that an adversary that is able to configure a malicious data-source path, can deploy a stored XSS attack against any user that has privileges related to viewing the `data_debug.php` information. A user that possesses the _General Administration>Sites/Devices/Data_ permissions can configure the data source path in _cacti_. This configuration occurs through `http://<HOST>/cacti/data_sources.php`. This vulnerability has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to update should manually filter HTML output.	2023-09-05	4.8	Medium
CVE-2023-39516	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability which allows an authenticated user to poison data stored in the _cacti_'s database. These data will be viewed by administrative _cacti_ accounts and execute JavaScript code in the victim's browser at view-time. The script under `data_sources.php` displays the data source management information (e.g. data source path, polling configuration etc.) for different data visualizations of the _cacti_ app. CENSUS found that an adversary that is able to configure a malicious data-source path, can deploy a stored XSS attack against any user of the same (or broader) privileges. A user that possesses the 'General Administration>Sites/Devices/Data' permissions can configure the data source path in Cacti. This configuration occurs through `http://<HOST>/cacti/data_sources.php`. The same page can be used for previewing the data source path. This issue has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to upgrade should manually escape HTML output.	2023-09-05	4.8	Medium
CVE-2023-39511	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. Affected versions are subject to a Stored Cross-Site-Scripting (XSS) Vulnerability which allows an authenticated user to poison data stored in the _cacti_'s database. These data will be viewed by administrative _cacti_ accounts and execute JavaScript code in the victim's browser at view-time. The script under `reports_admin.php` displays reporting information about graphs, devices, data sources etc. _CENSUS_ found that an adversary that is able to configure a malicious device name, related to a graph attached to a report, can deploy a stored XSS attack against any super user who has privileges of viewing the `reports_admin.php` page, such as administrative accounts. A user that possesses the _General Administration>Sites/Devices/Data_ permissions can configure the device names in _cacti_. This configuration occurs through `http://<HOST>/cacti/host.php`, while the rendered malicious payload is exhibited at `http://<HOST>/cacti/reports_admin.php` when the a graph with the maliciously altered device name is linked to the report. This issue has been addressed in version 1.2.25. Users are advised to upgrade. Users unable to upgrade should manually filter HTML output.	2023-09-06	4.8	Medium
CVE-2023-30714	samsung - multiple products	Improper authorization vulnerability in FolderContainerDragDelegate in One UI Home prior to SMR Sep-2023 Release 1 allows physical attackers to change some settings of the folder lock.	2023-09-06	4.6	Medium
CVE-2022-47352	google - multiple products	In camera driver, there is a possible out of bounds read due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-09-04	4.4	Medium
CVE-2022-47353	google - android	In vdsp device, there is a possible system crash due to improper input validation.This could lead to local denial of service with System execution privileges needed	2023-09-04	4.4	Medium
CVE-2022-48452	google - multiple products	In Ifaa service, there is a possible missing permission check. This could lead to local denial of service with System execution privileges needed	2023-09-04	4.4	Medium
CVE-2022-48453	google - multiple products	In camera driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-09-04	4.4	Medium
CVE-2023-38467	google - multiple products	In urild service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-09-04	4.4	Medium
CVE-2023-38468	google - multiple products	In urild service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	2023-09-04	4.4	Medium

متاح

CVE-2023-20823	google - multiple products	In cmdq, there is a possible out of bounds read due to an incorrect status check. This could lead to local denial of service with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08021592; Issue ID: ALPS08021592.	2023-09-04	4.4	Medium
CVE-2023-20833	google - multiple products	In keyinstall, there is a possible information disclosure 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: ALPS08017756; Issue ID: ALPS08017764.	2023-09-04	4.4	Medium
CVE-2023-20836	google - multiple products	In camsys, 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: ALPS07505629; Issue ID: ALPS07505629.	2023-09-04	4.4	Medium
CVE-2023-32808	google - android	In bluetooth driver, there is a possible read and write access to registers due to improper access control of register interface. This could lead to local leak of sensitive information with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07849751; Issue ID: ALPS07849751.	2023-09-04	4.4	Medium
CVE-2023-32809	google - android	In bluetooth driver, there is a possible read and write access to registers due to improper access control of register interface. This could lead to local leak of sensitive information with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07849753; Issue ID: ALPS07849753.	2023-09-04	4.4	Medium
CVE-2023-32814	google - android	In gnss service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08031947; Issue ID: ALPS08031947.	2023-09-04	4.4	Medium
CVE-2023-32816	google - android	In gnss service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08044040; Issue ID: ALPS08044032.	2023-09-04	4.4	Medium
CVE-2023-32817	google - android	In gnss service, there is a possible out of bounds read due to improper input validation. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08044040; Issue ID: ALPS08044035.	2023-09-04	4.4	Medium
CVE-2023-30721	samsung - multiple products	Insertion of sensitive information into log vulnerability in Locksettings prior to SMR Sep-2023 Release 1 allows a privileged local attacker to get lock screen match information from the log.	2023-09-06	4.4	Medium
CVE-2022-27599	qnap - qvr_pro_client	An insertion of sensitive information into Log file vulnerability has been reported to affect product. If exploited, the vulnerability possibly provides local authenticated administrators with an additional, less-protected path to acquiring the information via unspecified vectors. We have already fixed the vulnerability in the following version: Windows 10 SP1, Windows 11, Mac OS, and Mac M1: QVR Pro Client 2.3.0.0420 and later	2023-09-08	4.4	Medium
CVE-2023-30534	cacti - cacti	Cacti is an open source operational monitoring and fault management framework. There are two instances of insecure deserialization in Cacti version 1.2.24. While a viable gadget chain exists in Cacti's vendor directory (phpseclib), the necessary gadgets are not included, making them inaccessible and the insecure deserializations not exploitable. Each instance of insecure deserialization is due to using the unserialize function without sanitizing the user input. Cacti has a "safe" deserialization that attempts to sanitize the content and check for specific values before calling unserialize, but it isn't used in these instances. The vulnerable code lies in graphs_new.php, specifically within the host_new_graphs_save function. This issue has been addressed in version 1.2.25. Users are advised to upgrade. There are no known workarounds for this vulnerability.	2023-09-05	4.3	Medium
CVE-2023-28208	apple - multiple products	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. A user may send a text from a secondary eSIM despite configuring a contact to use a primary eSIM.	2023-09-06	4.3	Medium
CVE-2023-27523	apache - superset	Improper data authorization check on Jinja templated queries in Apache Superset up to and including 2.1.0 allows for an authenticated user to issue queries on database tables they may not have access to.	2023-09-06	4.3	Medium
CVE-2023-27526	apache - superset	A non Admin authenticated user could incorrectly create resources using the import charts feature, on Apache Superset up to and including 2.1.0.	2023-09-06	4.3	Medium
CVE-2023-39264	apache - superset	By default, stack traces for errors were enabled, which resulted in the exposure of internal traces on REST API endpoints to	2023-09-06	4.3	Medium

متاح

		users. This vulnerability exists in Apache Superset versions up to and including 2.1.0.			
CVE-2023-41930	jenkins - job_configuration_history	Jenkins Job Configuration History Plugin 1227.v7a_79fc4dc01f and earlier does not restrict the 'name' query parameter when rendering a history entry, allowing attackers to have Jenkins render a manipulated configuration history that was not created by the plugin.	2023-09-06	4.3	Medium
CVE-2023-41941	jenkins - aws_codecommit_trigger	A missing permission check in Jenkins AWS CodeCommit Trigger Plugin 3.0.12 and earlier allows attackers with Overall/Read permission to enumerate credentials IDs of AWS credentials stored in Jenkins.	2023-09-06	4.3	Medium
CVE-2023-41942	jenkins - aws_codecommit_trigger	A cross-site request forgery (CSRF) vulnerability in Jenkins AWS CodeCommit Trigger Plugin 3.0.12 and earlier allows attackers to clear the SQS queue.	2023-09-06	4.3	Medium
CVE-2023-41947	jenkins - frugal_testing	A missing permission check in Jenkins Frugal Testing Plugin 1.1 and earlier allows attackers with Overall/Read permission to connect to Frugal Testing using attacker-specified credentials.	2023-09-06	4.3	Medium
CVE-2023-32672	apache - superset	An Incorrect authorisation check in SQLLab in Apache Superset versions up to and including 2.1.0. This vulnerability allows an authenticated user to query tables that they do not have proper access to within Superset. The vulnerability can be exploited by leveraging a SQL parsing vulnerability.	2023-09-06	4.3	Medium
CVE-2023-36635	fortinet - multiple products	An improper access control in Fortinet FortiSwitchManager version 7.2.0 through 7.2.2 7.0.0 through 7.0.1 may allow a remote authenticated read-only user to modify the interface settings via the API.	2023-09-07	4.3	Medium
CVE-2023-41946	jenkins - frugal_testing	A cross-site request forgery (CSRF) vulnerability in Jenkins Frugal Testing Plugin 1.1 and earlier allows attackers to connect to Frugal Testing using attacker-specified credentials, and to retrieve test IDs and names from Frugal Testing, if a valid credential corresponds to the attacker-specified username.	2023-09-06	3.5	Low
CVE-2023-28195	apple - macos	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.3. An app may be able to read sensitive location information.	2023-09-06	3.3	Low
CVE-2023-30711	samsung - multiple products	Improper authentication in Phone and Messaging Storage SMR SEP-2023 Release 1 allows attacker to insert arbitrary data to the provider.	2023-09-06	3.3	Low
CVE-2023-30715	samsung - multiple products	Improper access control vulnerability in Weather prior to SMR Sep-2023 Release 1 allows attackers to access location information set in Weather without permission.	2023-09-06	3.3	Low
CVE-2023-30717	samsung - multiple products	Sensitive information exposure vulnerability in SVCAgent prior to SMR Sep-2023 Release 1 allows attackers to get unresettable identifiers.	2023-09-06	3.3	Low
CVE-2023-30718	samsung - multiple products	Improper export of android application components vulnerability in WifiApAutoHotspotEnablingActivity prior to SMR Sep-2023 Release 1 allows local attacker to change a Auto Hotspot setting.	2023-09-06	3.3	Low
CVE-2023-30719	samsung - multiple products	Exposure of Sensitive Information vulnerability in InboundSmsHandler prior to SMR Sep-2023 Release 1 allows local attackers to access certain message data.	2023-09-06	3.3	Low
CVE-2023-30724	samsung - gallery	Improper authentication in GallerySearchProvider of Gallery prior to version 14.5.01.2 allows attacker to access search history.	2023-09-06	3.3	Low
CVE-2023-38605	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Ventura 13.5. An app may be able to determine a user’s current location.	2023-09-06	3.3	Low
CVE-2023-40392	apple - multiple products	A privacy issue was addressed with improved private data redaction for log entries. This issue is fixed in macOS Ventura 13.5. An app may be able to read sensitive location information.	2023-09-06	3.3	Low
CVE-2021-43751	adobe - multiple products	Adobe Premiere Pro versions 22.0 (and earlier) and 15.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	3.3	Low
CVE-2021-44189	adobe - multiple products	Adobe After Effects versions 22.0 (and earlier) and 18.4.2 (and earlier) are affected by an Use-After-Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	3.3	Low
CVE-2021-44190	adobe - multiple products	Adobe After Effects versions 22.0 (and earlier) and 18.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	3.3	Low
CVE-2021-44191	adobe - multiple products	Adobe After Effects versions 22.0 (and earlier) and 18.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could	2023-09-07	3.3	Low

		leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.			
CVE-2021-44192	adobe - multiple products	Adobe After Effects versions 22.0 (and earlier) and 18.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	3.3	Low
CVE-2021-44193	adobe - multiple products	Adobe After Effects versions 22.0 (and earlier) and 18.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	3.3	Low
CVE-2021-44194	adobe - multiple products	Adobe After Effects versions 22.0 (and earlier) and 18.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	3.3	Low
CVE-2021-44195	adobe - multiple products	Adobe After Effects versions 22.0 (and earlier) and 18.4.2 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2023-09-07	3.3	Low
CVE-2023-40353	samsung - exynos_980_firmware	An issue was discovered in Exynos Mobile Processor 980 and 2100. An integer overflow at a buffer index can prevent the execution of requested services via a crafted application.	2023-09-08	3.3	Low

Where NCA provides the vulnerability information as published by NIST's NVD. In addition, it is the entity's or individual's responsibility to ensure the implementation of appropriate recommendations.

وحيث تقدم الهيئة تفاصيل الثغرات كما تم نشرها من قبل NIST's NVD. وإذ تبقى مسؤولية الجهة أو الشخص قائمة للتأكد من تطبيق التوصيات المناسبة.
