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

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

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 5th of November to 11th of November. 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-2023-22388	qualcomm - 315_5g_iot_modem_firmware	Memory Corruption in Multi-mode Call Processor while processing bit mask API.	2023-11-07	9.8	Critical
CVE-2023-33045	qualcomm - ar8035_firmware	Memory corruption in WLAN Firmware while parsing a NAN management frame carrying a S3 attribute.	2023-11-07	9.8	Critical
CVE-2023-38547	veeam - multiple products	A vulnerability in Veeam ONE allows an unauthenticated user to gain information about the SQL server connection Veeam ONE uses to access its configuration database. This may lead to remote code execution on the SQL server hosting the Veeam ONE configuration database.	2023-11-07	9.8	Critical
CVE-2023-42531	samsung - multiple products	Improper access control vulnerability in SmsController prior to SMR Nov-2023 Release1 allows attacker to bypass restrictions on starting activities from the background.	2023-11-07	9.8	Critical
CVE-2023-42536	samsung - multiple products	An improper input validation in saped_dec in libsaped prior to SMR Nov-2023 Release 1 allows attacker to cause out-of-bounds read and write.	2023-11-07	9.8	Critical
CVE-2023-42537	samsung - multiple products	An improper input validation in get_head_crc in libsaped prior to SMR Nov-2023 Release 1 allows attacker to cause out-of-bounds read and write.	2023-11-07	9.8	Critical
CVE-2023-42538	samsung - multiple products	An improper input validation in saped_rec_silence in libsaped prior to SMR Nov-2023 Release 1 allows attacker to cause out-of-bounds read and write.	2023-11-07	9.8	Critical
CVE-2023-5913	microfocus - multiple products	Incorrect Privilege Assignment vulnerability in opentext Fortify ScanCentral DAST. The vulnerability could be exploited to gain elevated privileges.This issue affects Fortify ScanCentral DAST versions 21.1, 21.2, 21.2.1, 22.1, 22.1.1, 22.2, 23.1.	2023-11-08	9.8	Critical
CVE-2023-47248	apache - pyarrow	Deserialization of untrusted data in IPC and Parquet readers in PyArrow versions 0.14.0 to 14.0.0 allows arbitrary code execution. An application is vulnerable if it reads Arrow IPC, Feather or Parquet data from untrusted sources (for example user-supplied input files). This vulnerability only affects PyArrow, not other Apache Arrow implementations or bindings. It is recommended that users of PyArrow upgrade to 14.0.1. Similarly, it is recommended that downstream libraries upgrade their dependency requirements to PyArrow 14.0.1 or later. PyPI packages are already available, and we hope that conda-forge packages will be available soon. If it is not possible to upgrade, we provide a separate package `pyarrow-hotfix` that disables the vulnerability on older PyArrow versions. See https://pypi.org/project/pyarrow-hotfix/ for instructions.	2023-11-09	9.8	Critical
CVE-2023-5801	huawei - multiple products	Vulnerability of identity verification being bypassed in the face unlock module. Successful exploitation of this vulnerability will affect integrity and confidentiality.	2023-11-08	9.1	Critical
CVE-2023-47004	redislabs - redisgraph	Buffer Overflow vulnerability in Redis RedisGraph v.2.x through v.2.12.8 and fixed in v.2.12.9 allows an attacker to execute arbitrary code via the code logic after valid authentication.	2023-11-06	8.8	High

CVE-2023-28572	qualcomm - csrb31024_firmware	Memory corruption in WLAN HOST while processing the WLAN scan descriptor list.	2023-11-07	8.8	High
CVE-2023-39913	apache - uimaj	Deserialization of Untrusted Data, Improper Input Validation vulnerability in Apache UIMA Java SDK, Apache UIMA Java SDK, Apache UIMA Java SDK, Apache UIMA Java SDK.This issue affects Apache UIMA Java SDK: before 3.5.0. Users are recommended to upgrade to version 3.5.0, which fixes the issue. There are several locations in the code where serialized Java objects are deserialized without verifying the data. This affects in particular: * the deserialization of a Java-serialized CAS, but also other binary CAS formats that include TSI information using the CasIOUtils class; * the CAS Editor Eclipse plugin which uses the the CasIOUtils class to load data; * the deserialization of a Java-serialized CAS of the Vinci Analysis Engine service which can receive using Java-serialized CAS objects over network connections; * the CasAnnotationViewerApplet and the CasTreeViewerApplet; * the checkpointing feature of the CPE module. Note that the UIMA framework by default does not start any remotely accessible services (i.e. Vinci) that would be vulnerable to this issue. A user or developer would need to make an active choice to start such a service. However, users or developers may use the CasIOUtils in their own applications and services to parse serialized CAS data. They are affected by this issue unless they ensure that the data passed to CasIOUtils is not a serialized Java object. When using Vinci or using CasIOUtils in own services/applications, the unrestricted deserialization of Java-serialized CAS files may allow arbitrary (remote) code execution. As a remedy, it is possible to set up a global or context-specific ObjectInputFilter (cf. https://openjdk.org/jeps/290 and https://openjdk.org/jeps/415) if running UIMA on a Java version that supports it. Note that Java 1.8 does not support the ObjectInputFilter, so there is no remedy when running on this out-of-support platform. An upgrade to a recent Java version is strongly recommended if you need to secure an UIMA version that is affected by this issue. To mitigate the issue on a Java 9+ platform, you can configure a filter pattern through the "jdk.serialFilter" system property using a semicolon as a separator: To allow deserializing Java-serialized binary CASes, add the classes: * org.apache.uima.cas.impl.CASCompleteSerializer * org.apache.uima.cas.impl.CASMgrSerializer * org.apache.uima.cas.impl.CASSerializer * java.lang.String To allow deserializing CPE Checkpoint data, add the following classes (and any custom classes your application uses to store its checkpoints): * org.apache.uima.collection.impl.cpm.CheckpointData * org.apache.uima.util.ProcessTrace * org.apache.uima.util.impl.ProcessTrace_impl * org.apache.uima.collection.base_cpm.SynchPoint Make sure to use "!*" as the final component to the filter pattern to disallow deserialization of any classes not listed in the pattern. Apache UIMA 3.5.0 uses tightly scoped ObjectInputFilters when reading Java-serialized data depending on the type of data being expected. Configuring a global filter is not necessary with this version.	2023-11-08	8.8	High
CVE-2023-5996	google - chrome	Use after free in WebAudio in Google Chrome prior to 119.0.6045.123 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2023-11-08	8.8	High
CVE-2023-40054	solarwinds - network_configuration_manager	The Network Configuration Manager was susceptible to a Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows a low-level user to perform the actions with SYSTEM privileges. We found this issue was not resolved in CVE-2023-33226	2023-11-09	8.8	High
CVE-2023-40055	solarwinds - network_configuration_manager	The Network Configuration Manager was susceptible to a Directory Traversal Remote Code Execution Vulnerability. This vulnerability allows a low-level user to perform the actions with	2023-11-09	8.8	High

		SYSTEM privileges. We found this issue was not resolved in CVE-2023-33227			
CVE-2023-39295	qnap - qumagie	An OS command injection vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to execute commands via a network. We have already fixed the vulnerability in the following version: QuMagie 2.1.3 and later	2023-11-10	8.8	High
CVE-2023-41284	qnap - qumagie	A SQL injection vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: QuMagie 2.1.4 and later	2023-11-10	8.8	High
CVE-2023-41285	qnap - qumagie	A SQL injection vulnerability has been reported to affect QuMagie. If exploited, the vulnerability could allow authenticated users to inject malicious code via a network. We have already fixed the vulnerability in the following version: QuMagie 2.1.4 and later	2023-11-10	8.8	High
CVE-2023-32837	google - android	In video, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08235273; Issue ID: ALPS08250357.	2023-11-06	7.8	High
CVE-2023-21671	qualcomm - fastconnect_6700_firmware	Memory Corruption in Core during syscall for Sectools Fuse comparison feature.	2023-11-07	7.8	High
CVE-2023-24852	qualcomm - 315_5g_iot_modem_firmware	Memory Corruption in Core due to secure memory access by user while loading modem image.	2023-11-07	7.8	High
CVE-2023-28545	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in TZ Secure OS while loading an app ELF.	2023-11-07	7.8	High
CVE-2023-28556	qualcomm - 315_5g_iot_modem_firmware	Cryptographic issue in HLOS during key management.	2023-11-07	7.8	High
CVE-2023-28570	qualcomm - aqt1000_firmware	Memory corruption while processing audio effects.	2023-11-07	7.8	High
CVE-2023-28574	qualcomm - ar8035_firmware	Memory corruption in core services when Diag handler receives a command to configure event listeners.	2023-11-07	7.8	High
CVE-2023-33031	qualcomm - apq8017_firmware	Memory corruption in Automotive Audio while copying data from ADSP shared buffer to the VOC packet data buffer.	2023-11-07	7.8	High
CVE-2023-33055	qualcomm - aqt1000_firmware	Memory Corruption in Audio while invoking callback function in driver from ADSP.	2023-11-07	7.8	High
CVE-2023-33059	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in Audio while processing the VOC packet data from ADSP.	2023-11-07	7.8	High
CVE-2023-33074	qualcomm - wcn6750_firmware	Memory corruption in Audio when SSR event is triggered after music playback is stopped.	2023-11-07	7.8	High
CVE-2023-30739	samsung - multiple products	Arbitrary File Descriptor Write vulnerability in libsec-ril prior to SMR Nov-2023 Release 1 allows local attacker to execute arbitrary code.	2023-11-07	7.8	High
CVE-2023-42528	samsung - multiple products	Improper Input Validation vulnerability in ProcessNvBuffering of libsec-ril prior to SMR Nov-2023 Release 1 allows local attacker to execute arbitrary code.	2023-11-07	7.8	High
CVE-2023-42529	samsung - multiple products	Out-of-bound write vulnerability in libsec-ril prior to SMR Nov-2023 Release 1 allows local attackers to execute arbitrary code.	2023-11-07	7.8	High
CVE-2023-42535	samsung - multiple products	Out-of-bounds Write in read_block of vold prior to SMR Nov-2023 Release 1 allows local attacker to execute arbitrary code.	2023-11-07	7.8	High
CVE-2023-4632	lenovo - system_update	An uncontrolled search path vulnerability was reported in Lenovo System Update that could allow an attacker with local access to execute code with elevated privileges.	2023-11-08	7.8	High
CVE-2023-5678	openssl - multiple products	Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to enerate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack.	2023-11-06	7.5	High

		DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the "-pubcheck" option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.			
CVE-2023-33047	qualcomm - ar8035_firmware	Transient DOS in WLAN Firmware while parsing no-inherit IES.	2023-11-07	7.5	High
CVE-2023-33048	qualcomm - ar8035_firmware	Transient DOS in WLAN Firmware while parsing t2lm buffers.	2023-11-07	7.5	High
CVE-2023-33056	qualcomm - ar8035_firmware	Transient DOS in WLAN Firmware when firmware receives beacon including T2LM IE.	2023-11-07	7.5	High
CVE-2023-33061	qualcomm - ar8035_firmware	Transient DOS in WLAN Firmware while parsing WLAN beacon or probe-response frame.	2023-11-07	7.5	High
CVE-2023-42530	samsung - multiple products	Improper access control vulnerability in SecSettings prior to SMR Nov-2023 Release 1 allows attackers to enable Wi-Fi and Wi-Fi Direct without User Interaction.	2023-11-07	7.5	High
CVE-2023-42532	samsung - multiple products	Improper Certificate Validation in FotaAgent prior to SMR Nov-2023 Release1 allows remote attacker to intercept the network traffic including Firmware information.	2023-11-07	7.5	High
CVE-2023-42543	samsung - bixby_voice	Improper verification of intent by broadcast receiver vulnerability in Bixby Voice prior to version 3.3.35.12 allows attackers to access arbitrary data with Bixby Voice privilege.	2023-11-07	7.5	High
CVE-2023-42545	samsung - phone	Use of implicit intent for sensitive communication vulnerability in Phone prior to versions 12.7.20.12 in Android 11, 13.1.48, 13.5.28 in Android 12, and 14.7.38 in Android 13 allows attackers to access location data.	2023-11-07	7.5	High
CVE-2023-0436	mongodb - multiple products	The affected versions of MongoDB Atlas Kubernetes Operator may print sensitive information like GCP service account keys and API integration secrets while DEBUG mode logging is enabled. This issue affects MongoDB Atlas Kubernetes Operator versions: 1.5.0, 1.6.0, 1.6.1, 1.7.0. Please note that this is reported on an EOL version of the product, and users are advised to upgrade to the latest supported version. Required Configuration: DEBUG logging is not enabled by default, and must be configured by the end-user. To check the log-level of the Operator, review the flags passed in your deployment configuration (eg. https://github.com/mongodb/mongodb-atlas-kubernetes/blob/main/config/manager/manager.yaml#L27 https://github.com/mongodb/mongodb-atlas-kubernetes/blob/main/config/manager/manager.yaml#L27)	2023-11-07	7.5	High
CVE-2023-46768	huawei - multiple products	Multi-thread vulnerability in the idmap module. Successful exploitation of this vulnerability may cause features to perform abnormally.	2023-11-08	7.5	High
CVE-2023-46769	huawei - multiple products	Use-After-Free (UAF) vulnerability in the dubai module. Successful exploitation of this vulnerability will affect availability.	2023-11-08	7.5	High
CVE-2023-46770	huawei - multiple products	Out-of-bounds vulnerability in the sensor module. Successful exploitation of this vulnerability may cause mistouch prevention errors on users' mobile phones.	2023-11-08	7.5	High
CVE-2023-44115	huawei - multiple products	Vulnerability of improper permission control in the Booster module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2023-11-08	7.5	High
CVE-2023-41111	samsung - exynos_9810_firmware	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem (Exynos 9810, 9610, 9820, 980, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Modem 5123, Modem 5300, and Auto T5123). Improper handling of a length parameter inconsistency can cause abnormal termination of a mobile phone. This occurs in the RLC task and RLC module.	2023-11-08	7.5	High
CVE-2023-41112	samsung - exynos_9810_firmware	An issue was discovered in Samsung Mobile Processor, Wearable Processor, Automotive Processor, and Modem (Exynos 9810, 9610, 9820, 980, 850, 1080, 2100, 2200, 1280, 1380, 1330, 9110, W920, Modem 5123, Modem 5300, and Auto T5123). A buffer copy, without checking the size of the input, can cause abnormal termination of a mobile phone. This occurs in the RLC task and RLC module.	2023-11-08	7.5	High

CVE-2023-44098	huawei - multiple products	Vulnerability of missing encryption in the card management module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-11-08	7.5	High
CVE-2023-46771	huawei - multiple products	Security vulnerability in the face unlock module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-11-08	7.5	High
CVE-2023-46760	huawei - multiple products	Out-of-bounds write vulnerability in the kernel driver module. Successful exploitation of this vulnerability may cause process exceptions.	2023-11-08	7.5	High
CVE-2023-46761	huawei - multiple products	Out-of-bounds write vulnerability in the kernel driver module. Successful exploitation of this vulnerability may cause process exceptions.	2023-11-08	7.5	High
CVE-2023-46762	huawei - multiple products	Out-of-bounds write vulnerability in the kernel driver module. Successful exploitation of this vulnerability may cause process exceptions.	2023-11-08	7.5	High
CVE-2023-46765	huawei - multiple products	Vulnerability of uncaught exceptions in the NFC module. Successful exploitation of this vulnerability can affect NFC availability.	2023-11-08	7.5	High
CVE-2023-46766	huawei - multiple products	Out-of-bounds write vulnerability in the kernel driver module. Successful exploitation of this vulnerability may cause process exceptions.	2023-11-08	7.5	High
CVE-2023-46767	huawei - multiple products	Out-of-bounds write vulnerability in the kernel driver module. Successful exploitation of this vulnerability may cause process exceptions.	2023-11-08	7.5	High
CVE-2023-46772	huawei - emui	Vulnerability of parameters being out of the value range in the QMI service module. Successful exploitation of this vulnerability may cause errors in reading file data.	2023-11-08	7.5	High
CVE-2023-46774	huawei - multiple products	Vulnerability of uncaught exceptions in the NFC module. Successful exploitation of this vulnerability can affect NFC availability.	2023-11-08	7.5	High
CVE-2023-46757	huawei - harmonyos	The remote PIN module has a vulnerability that causes incorrect information storage locations.Successful exploitation of this vulnerability may affect confidentiality.	2023-11-08	7.5	High
CVE-2023-46758	huawei - multiple products	Permission management vulnerability in the multi-screen interaction module. Successful exploitation of this vulnerability may cause service exceptions of the device.	2023-11-08	7.5	High
CVE-2023-46759	huawei - multiple products	Permission control vulnerability in the call module. Successful exploitation of this vulnerability may affect service confidentiality.	2023-11-08	7.5	High
CVE-2023-36014	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	2023-11-10	7.3	High
CVE-2023-36024	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-11-10	7.1	High
CVE-2023-32832	google - multiple products	In video, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08235273; Issue ID: ALPS08235273.	2023-11-06	7	High
CVE-2023-42533	samsung - multiple products	Improper Input Validation with USB Gadget Interface prior to SMR Nov-2023 Release 1 allows a physical attacker to execute arbitrary code in Kernel.	2023-11-07	6.8	Medium
CVE-2023-42554	samsung - pass	Improper Authentication vulnerabiity in Samsung Pass prior to version 4.3.00.17 allows physical attackers to bypass authentication.	2023-11-07	6.8	Medium
CVE-2023-32818	google - multiple products	In vdec, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08163896 & ALPS08013430; Issue ID: ALPS07867715.	2023-11-06	6.7	Medium
CVE-2023-32834	google - multiple products	In secmem, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08161762; Issue ID: ALPS08161762.	2023-11-06	6.7	Medium
CVE-2023-32835	google - multiple products	In keyinstall, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08157918; Issue ID: ALPS08157918.	2023-11-06	6.7	Medium
CVE-2023-32836	google - multiple products	In display, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS08126725; Issue ID: ALPS08126725.	2023-11-06	6.7	Medium
CVE-2023-32838	google - multiple products	In dpe, there is a possible out of bounds write due to a missing valid range checking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07310805; Issue ID: ALPS07310805.	2023-11-06	6.7	Medium
CVE-2023-32839	google - multiple products	In dpe, there is a possible out of bounds write due to a missing valid range checking. This could lead to local escalation of privilege	2023-11-06	6.7	Medium

		with System execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07262576; Issue ID: ALPS07262576.			
CVE-2023-3282	paloaltonetworks - cortex_xsoar	A local privilege escalation (PE) vulnerability in the Palo Alto Networks Cortex XSOAR engine software running on a Linux operating system enables a local attacker to execute programs with elevated privileges if the attacker has shell access to the engine.	2023-11-08	6.7	Medium
CVE-2023-43567	lenovo - ideacentre_c5-14imb05_firmware	A buffer overflow was reported in the LemSecureBootForceKey module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	Medium
CVE-2023-43569	lenovo - ideacentre_c5-14imb05_firmware	A buffer overflow was reported in the OemSmi module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	Medium
CVE-2023-43570	lenovo - ideacentre_c5-14imb05_firmware	A potential vulnerability was reported in the SMI callback function of the OemSmi driver that may allow a local attacker with elevated permissions to execute arbitrary code.	2023-11-08	6.7	Medium
CVE-2023-5075	lenovo - ideapad_duet_3_10igl5_firmware	A buffer overflow was reported in the FmpSipoCapsuleDriver driver in the IdeaPad Duet 3-10IGL5 that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	Medium
CVE-2023-5078	lenovo - thinkpad_x13_gen_3_firmware	A vulnerability was reported in some ThinkPad BIOS that could allow a physical or local attacker with elevated privileges to tamper with BIOS firmware.	2023-11-08	6.7	Medium
CVE-2023-43571	lenovo - ideacentre_c5-14imb05_firmware	A buffer overflow was reported in the BiosExtensionLoader module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	Medium
CVE-2023-43573	lenovo - ideacentre_c5-14imb05_firmware	A buffer overflow was reported in the LEMALLDriversConnectedEventHook module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	Medium
CVE-2023-43575	lenovo - ideacentre_c5-14imb05_firmware	A buffer overflow was reported in the UltraFunctionTable module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	Medium
CVE-2023-43576	lenovo - ideacentre_c5-14imb05_firmware	A buffer overflow was reported in the WMISwSmi module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	Medium
CVE-2023-43577	lenovo - ideacentre_c5-14imb05_firmware	A buffer overflow was reported in the ReFlash module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	Medium
CVE-2023-43578	lenovo - ideacentre_c5-14imb05_firmware	A buffer overflow was reported in the SmiFlash module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	Medium
CVE-2023-43579	lenovo - ideacentre_c5-14imb05_firmware	A buffer overflow was reported in the SmuV11Dxe driver in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	Medium
CVE-2023-43580	lenovo - ideacentre_c5-14imb05_firmware	A buffer overflow was reported in the SmuV11DxeVMR module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	Medium
CVE-2023-43581	lenovo - ideacentre_c5-14imb05_firmware	A buffer overflow was reported in the Update_WMI module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to execute arbitrary code.	2023-11-08	6.7	Medium
CVE-2023-45075	lenovo - ideacentre_c5-14imb05_firmware	A memory leakage vulnerability was reported in the SWSMI_Shadow DXE driver that may allow a local attacker with elevated privileges to write to NVRAM variables.	2023-11-08	6.7	Medium
CVE-2023-45076	lenovo - ideacentre_c5-14imb05_firmware	A memory leakage vulnerability was reported in the 534D0140 DXE driver that may allow a local attacker with elevated privileges to write to NVRAM variables.	2023-11-08	6.7	Medium
CVE-2023-45077	lenovo - ideacentre_c5-14imb05_firmware	A memory leakage vulnerability was reported in the 534D0740 DXE driver that may allow a local attacker with elevated privileges to write to NVRAM variables.	2023-11-08	6.7	Medium
CVE-2023-45078	lenovo - ideacentre_c5-14imb05_firmware	A memory leakage vulnerability was reported in the DustFilterAlertSmm SMM driver that may allow a local attacker with elevated privileges to write to NVRAM variables.	2023-11-08	6.7	Medium
CVE-2023-45079	lenovo - ideacentre_c5-14imb05_firmware	A memory leakage vulnerability was reported in the NvmramSmm SMM driver that may allow a local attacker with elevated privileges to write to NVRAM variables.	2023-11-08	6.7	Medium
CVE-2023-42669	samba - multiple products	A vulnerability was found in Samba's "rpcecho" development server, a non-Windows RPC server used to test Samba's DCE/RPC stack elements. This vulnerability stems from an RPC function that can be blocked indefinitely. The issue arises because the "rpcecho" service operates with only one worker in the main RPC task, allowing calls to the "rpcecho" server to be blocked for a specified time, causing service disruptions. This disruption is triggered by a "sleep()" call in the "dcesrv_echo_TestSleep()" function under specific conditions. Authenticated users or attackers can exploit this vulnerability to make calls to the "rpcecho" server, requesting it to block for a specified duration, effectively disrupting most services and leading to a complete denial of service on the AD DC.	2023-11-06	6.5	Medium

		The DoS affects all other services as "rpcecho" runs in the main RPC task.			
CVE-2023-36409	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Information Disclosure Vulnerability	2023-11-07	6.5	Medium
CVE-2023-40453	docker - machine	Docker Machine through 0.16.2 allows an attacker, who has control of a worker node, to provide crafted version data, which might potentially trick an administrator into performing an unsafe action (via escape sequence injection), or might have a data size that causes a denial of service to a bastion node. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	2023-11-07	6.5	Medium
CVE-2023-42546	samsung - account	Use of implicit intent for sensitive communication vulnerability in startAgreeToDisclaimerActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	2023-11-07	6.5	Medium
CVE-2023-42547	samsung - account	Use of implicit intent for sensitive communication vulnerability in startEmailValidationActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	2023-11-07	6.5	Medium
CVE-2023-42548	samsung - account	Use of implicit intent for sensitive communication vulnerability in startMandatoryCheckActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	2023-11-07	6.5	Medium
CVE-2023-42549	samsung - account	Use of implicit intent for sensitive communication vulnerability in startNameValidationActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	2023-11-07	6.5	Medium
CVE-2023-42550	samsung - account	Use of implicit intent for sensitive communication vulnerability in startSignIn in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	2023-11-07	6.5	Medium
CVE-2023-42551	samsung - account	Use of implicit intent for sensitive communication vulnerability in startTncActivity in Samsung Account prior to version 14.5.00.7 allows attackers to access arbitrary file with Samsung Account privilege.	2023-11-07	6.5	Medium
CVE-2023-4154	samba - multiple products	A design flaw was found in Samba's DirSync control implementation, which exposes passwords and secrets in Active Directory to privileged users and Read-Only Domain Controllers (RODCs). This flaw allows RODCs and users possessing the GET_CHANGES right to access all attributes, including sensitive secrets and passwords. Even in a default setup, RODC DC accounts, which should only replicate some passwords, can gain access to all domain secrets, including the vital krbtgt, effectively eliminating the RODC / DC distinction. Furthermore, the vulnerability fails to account for error conditions (fail open), like out-of-memory situations, potentially granting access to secret attributes, even under low-privileged attacker influence.	2023-11-07	6.5	Medium
CVE-2023-4061	redhat - multiple products	A flaw was found in wildfly-core. A management user could use the resolve-expression in the HAL Interface to read possible sensitive information from the Wildfly system. This issue could allow a malicious user to access the system and obtain possible sensitive information from the system.	2023-11-08	6.5	Medium
CVE-2023-39198	linux - multiple products	A race condition was found in the QXL driver in the Linux kernel. The qxl_mode_dumb_create() function dereferences the qobj returned by the qxl_gem_object_create_with_handle(), but the handle is the only one holding a reference to it. This flaw allows an attacker to guess the returned handle value and trigger a use-after-free issue, potentially leading to a denial of service or privilege escalation.	2023-11-09	6.4	Medium
CVE-2023-36027	microsoft - multiple products	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-11-10	6.3	Medium
CVE-2023-5771	proofpoint - multiple products	Proofpoint Enterprise Protection contains a stored XSS vulnerability in the AdminUI. An unauthenticated attacker can send a specially crafted email with HTML in the subject which triggers XSS when viewing quarantined messages. This issue affects Proofpoint Enterprise Protection: from 8.20.0 before patch 4796, from 8.18.6 before patch 4795 and all other prior versions.	2023-11-06	6.1	Medium
CVE-2022-48613	huawei - multiple products	Race condition vulnerability in the kernel module. Successful exploitation of this vulnerability may cause variable values to be read with the condition evaluation bypassed.	2023-11-08	5.9	Medium
CVE-2023-32825	google - android	In bluethooth service, there is a possible out of bounds reads due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: ALPS07884130; Issue ID: ALPS07884130.	2023-11-06	5.5	Medium
CVE-2023-5090	linux - multiple products	A flaw was found in KVM. An improper check in svm_set_x2apic_msr_interception() may allow direct access to host x2apic msrs when the guest resets its apic, potentially leading to a denial of service condition.	2023-11-06	5.5	Medium

CVE-2023-4910	redhat - 3scale_api_management	A flaw was found In 3Scale Admin Portal. If a user logs out from the personal tokens page and then presses the back button in the browser, the tokens page is rendered from the browser cache.	2023-11-06	5.5	Medium
CVE-2023-5748	synology - ssl_vpn_client	Buffer copy without checking size of input ('Classic Buffer Overflow') vulnerability in cgi component in Synology SSL VPN Client before 1.4.7-0687 allows local users to conduct denial-of-service attacks via unspecified vectors.	2023-11-07	5.5	Medium
CVE-2023-35140	zyxel - gs1900-48hpv2_firmware	The improper privilege management vulnerability in the Zyxel GS1900-24EP switch firmware version V2.70(ABTO.5) could allow an authenticated local user with read-only access to modify system settings on a vulnerable device.	2023-11-07	5.5	Medium
CVE-2023-28553	qualcomm - ar8035_firmware	Information Disclosure in WLAN Host when processing WMI event command.	2023-11-07	5.5	Medium
CVE-2023-28554	qualcomm - aqt1000_firmware	Information Disclosure in Qualcomm IPC while reading values from shared memory in VM.	2023-11-07	5.5	Medium
CVE-2023-28563	qualcomm - aqt1000_firmware	Information disclosure in IOE Firmware while handling WMI command.	2023-11-07	5.5	Medium
CVE-2023-28566	qualcomm - aqt1000_firmware	Information disclosure in WLAN HAL while handling the WMI state info command.	2023-11-07	5.5	Medium
CVE-2023-28568	qualcomm - aqt1000_firmware	Information disclosure in WLAN HAL when reception status handler is called.	2023-11-07	5.5	Medium
CVE-2023-28569	qualcomm - aqt1000_firmware	Information disclosure in WLAN HAL while handling command through WMI interfaces.	2023-11-07	5.5	Medium
CVE-2023-42527	samsung - multiple products	Improper input validation vulnerability in ProcessWriteFile of libsec-ril prior to SMR Nov-2023 Release 1 allows local attackers to expose sensitive information.	2023-11-07	5.5	Medium
CVE-2023-42534	samsung - multiple products	Improper input validation vulnerability in ChooserActivity prior to SMR Nov-2023 Release 1 allows local attackers to read arbitrary files with system privilege.	2023-11-07	5.5	Medium
CVE-2023-42539	samsung - health	PendingIntent hijacking vulnerability in ChallengeNotificationManager in Samsung Health prior to version 6.25 allows local attackers to access data.	2023-11-07	5.5	Medium
CVE-2023-42540	samsung - account	Improper access control vulnerability in Samsung Account prior to version 14.5.01.1 allows attackers to access sensitive information via implicit intent.	2023-11-07	5.5	Medium
CVE-2023-42544	samsung - quick_share	Improper access control vulnerability in Quick Share prior to 13.5.52.0 allows local attacker to access local files.	2023-11-07	5.5	Medium
CVE-2023-42555	samsung - easysetup	Use of implicit intent for sensitive communication vulnerability in EasySetup prior to version 11.1.13 allows attackers to get the bluetooth address of user device.	2023-11-07	5.5	Medium
CVE-2023-4891	lenovo - view_driver	A potential use-after-free vulnerability was reported in the Lenovo View driver that could result in denial of service.	2023-11-08	5.5	Medium
CVE-2023-6039	linux - multiple products	A use-after-free flaw was found in lan78xx_disconnect in drivers/net/usb/lan78xx.c in the network sub-component, net/usb/lan78xx in the Linux Kernel. This flaw allows a local attacker to crash the system when the LAN78XX USB device detaches.	2023-11-09	5.5	Medium
CVE-2023-45167	ibm - multiple products	IBM AIX's 7.3 Python implementation could allow a non-privileged local user to exploit a vulnerability to cause a denial of service. IBM X-Force ID: 267965.	2023-11-10	5.5	Medium
CVE-2023-36769	microsoft - multiple products	Microsoft OneNote Spoofing Vulnerability	2023-11-06	5.4	Medium
CVE-2023-38549	veeam - multiple products	A vulnerability in Veeam ONE allows an unprivileged user who has access to the Veeam ONE Web Client the ability to acquire the NTLM hash of the account used by the Veeam ONE Reporting Service. Note: The criticality of this vulnerability is reduced as it requires interaction by a user with the Veeam ONE Administrator role.	2023-11-07	5.4	Medium
CVE-2023-43057	ibm - multiple products	IBM QRadar SIEM 7.5.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 267484.	2023-11-11	5.4	Medium
CVE-2023-42541	samsung - push_service	Improper authorization in PushClientProvider of Samsung Push Service prior to version 3.4.10 allows attacker to access unique id.	2023-11-07	5.3	Medium
CVE-2023-42553	samsung - email	Improper authorization verification vulnerability in Samsung Email prior to version 6.1.90.4 allows attackers to read sandbox data of email.	2023-11-07	5.3	Medium
CVE-2023-46819	apache - ofbiz	Missing Authentication in Apache Software Foundation Apache OFBiz when using the Solr plugin. This issue affects Apache OFBiz: before 18.12.09. Users are recommended to upgrade to version 18.12.09	2023-11-07	5.3	Medium
CVE-2023-46755	huawei - multiple products	Vulnerability of input parameters being not strictly verified in the input. Successful exploitation of this vulnerability may cause the launcher to restart.	2023-11-08	5.3	Medium
CVE-2023-46763	huawei - multiple products	Vulnerability of background app permission management in the framework module. Successful exploitation of this vulnerability may cause background apps to start maliciously.	2023-11-08	5.3	Medium

CVE-2023-46764	huawei - multiple products	Unauthorized startup vulnerability of background apps. Successful exploitation of this vulnerability may cause background apps to start maliciously.	2023-11-08	5.3	Medium
CVE-2023-46756	huawei - multiple products	Permission control vulnerability in the window management module. Successful exploitation of this vulnerability may cause malicious pop-up windows.	2023-11-08	5.3	Medium
CVE-2023-46851	apache - allura	Allura Discussion and Allura Forum importing does not restrict URL values specified in attachments. Project administrators can run these imports, which could cause Allura to read local files and expose them. Exposing internal files then can lead to other exploits, like session hijacking, or remote code execution. This issue affects Apache Allura from 1.0.1 through 1.15.0. Users are recommended to upgrade to version 1.16.0, which fixes the issue. If you are unable to upgrade, set "disable_entry_points.allura.importers = forge-tracker, forge-discussion" in your .ini config file.	2023-11-07	4.9	Medium
CVE-2023-43568	lenovo - ideacentre_c5-14imb05_firmware	A buffer over-read was reported in the LemSecureBootForceKey module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to disclose sensitive information.	2023-11-08	4.4	Medium
CVE-2023-43572	lenovo - ideacentre_c5-14imb05_firmware	A buffer over-read was reported in the BiosExtensionLoader module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to disclose sensitive information.	2023-11-08	4.4	Medium
CVE-2023-43574	lenovo - ideacentre_c5-14imb05_firmware	A buffer over-read was reported in the LEMALLDriversConnectedEventHook module in some Lenovo Desktop products that may allow a local attacker with elevated privileges to disclose sensitive information.	2023-11-08	4.4	Medium
CVE-2023-38548	veeam - multiple products	A vulnerability in Veeam ONE allows an unprivileged user who has access to the Veeam ONE Web Client the ability to acquire the NTLM hash of the account used by the Veeam ONE Reporting Service.	2023-11-07	4.3	Medium
CVE-2023-41723	veeam - multiple products	A vulnerability in Veeam ONE allows a user with the Veeam ONE Read-Only User role to view the Dashboard Schedule. Note: The criticality of this vulnerability is reduced because the user with the Read-Only role is only able to view the schedule and cannot make changes.	2023-11-07	4.3	Medium
CVE-2023-4956	redhat - quay	A flaw was found in Quay. Clickjacking is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they intend to click on the top-level page. During the pentest, it has been detected that the config-editor page is vulnerable to clickjacking. This flaw allows an attacker to trick an administrator user into clicking on buttons on the config-editor panel, possibly reconfiguring some parts of the Quay instance.	2023-11-07	4.3	Medium
CVE-2023-41270	samsung - ue40d7000_firmware	Improper Restriction of Excessive Authentication Attempts vulnerability in Samsung Smart TV UE40D7000 version T-GAPDEUC-1033.2 and before allows attackers to cause a denial of service via WPS attack tools.	2023-11-08	4.3	Medium
CVE-2023-42542	samsung - push_service	Improper access control vulnerability in Samsung Push Service prior to 3.4.10 allows local attackers to get register ID to identify the device.	2023-11-07	3.3	Low
CVE-2023-42552	samsung - firewall	Implicit intent hijacking vulnerability in Firewall application prior to versions 12.1.00.24 in Android 11, 13.1.00.16 in Android 12 and 14.1.00.7 in Android 13 allows 3rd party application to tamper the database of Firewall.	2023-11-07	3.3	Low

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

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