الهيئة الوطنية للأمن السيبراني
Nat onal Cybersecurity Authority

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

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

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 29th of April to 7th of May. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٢٩ أبريل إلى ٧ مايو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2022-45802	apache - streampark	Streampark allows any users to upload a jar as application, but there is no mandatory verification of the uploaded file type, causing users to upload some high-risk files, and may upload them to any directory, Users of the affected versions should upgrade to Apache StreamPark 2.0.0 or later	2023-05-01	9.8	Critical
CVE-2023-20126	cisco - spa112_firmware	A vulnerability in the web-based management interface of Cisco SPA112 2-Port Phone Adapters could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. This vulnerability is due to a missing authentication process within the firmware upgrade function. An attacker could exploit this vulnerability by upgrading an affected device to a crafted version of firmware. A successful exploit could allow the attacker to execute arbitrary code on the affected device with full privileges. Cisco has not released firmware updates to address this vulnerability.	2023-05-04	9.8	Critical
CVE-2023-21494	samsung - multiple products	Potential buffer overflow vulnerability in auth api in mm_Authentication.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access.	2023-05-04	9.8	Critical
CVE-2023-21503	samsung - multiple products	Potential buffer overflow vulnerability in mm_LteInterRatManagement.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access.	2023-05-04	9.8	Critical
CVE-2023-21504	samsung - multiple products	Potential buffer overflow vulnerability in mm_Plmncoordination.c in Shannon baseband prior to SMR May-2023 Release 1 allows remote attackers to cause invalid memory access.	2023-05-04	9.8	Critical
CVE-2022-46365	apache - streampark	Apache StreamPark 1.0.0 before 2.0.0 When the user successfully logs in, to modify his profile, the username will be passed to the server-layer as a parameter, but not verified whether the user name is the currently logged user and whether the user is legal, This will allow malicious attackers to send any username to modify and reset the account, Users of the affected versions should upgrade to Apache StreamPark 2.0.0 or later.	2023-05-01	9.1	Critical
CVE-2023-22637	fortinet - multiple products	An improper neutralization of input during web page generation ('Cross-site Scripting') vulnerability [CWE-79] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions in License Management would permit an authenticated attacker to trigger remote code execution via crafted licenses.	2023-05-03	9	Critical
CVE-2023-0896	lenovo - smart_clock_essential_with_alexa_built_in_firmware	A default password was reported in Lenovo Smart Clock Essential with Alexa Built In that could allow unauthorized device access to an attacker with local network access.	2023-05-01	8.8	High
CVE-2023-0683	lenovo - thinkagile_hx5530_firmware	A valid, authenticated XCC user with read only access may gain elevated privileges through a specifically crafted API call.	2023-05-01	8.8	High

CVE-2023-25492	lenovo - thinkagile_hx5530_firmware	A valid, authenticated user may be able to trigger a denial of service of the XCC web user interface or other undefined behavior through a format string injection vulnerability in a web interface API.	2023-05-01	8.8	High
CVE-2023-22919	zyxel - nbg6604_firmware	The post-authentication command injection vulnerability in the Zyxel NBG6604 firmware version V1.01(ABIR.0)C0 could allow an authenticated attacker to execute some OS commands remotely by sending a crafted HTTP request.	2023-05-01	8.8	High
CVE-2023-32007	apache - multiple products	** UNSUPPORTED WHEN ASSIGNED ** The Apache Spark UI offers the possibility to enable ACLs via the configuration option spark.acls.enable. With an authentication filter, this checks whether a user has access permissions to view or modify the application. If ACLs are enabled, a code path in HttpSecurityFilter can allow someone to perform impersonation by providing an arbitrary user name. A malicious user might then be able to reach a permission check function that will ultimately build a Unix shell command based on their input, and execute it. This will result in arbitrary shell command execution as the user Spark is currently running as. This issue was disclosed earlier as CVE-2022-33891, but incorrectly claimed version 3.1.3 (which has since gone EOL) would not be affected. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. Users are recommended to upgrade to a supported version of Apache Spark, such as version 3.4.0.	2023-05-02	8.8	High
CVE-2023-2461	google - chrome	Use after free in OS Inputs in Google Chrome on ChromeOS prior to 113.0.5672.63 allowed a remote attacker who convinced a user to enage in specific UI interaction to potentially exploit heap corruption via crafted UI interaction. (Chromium security severity: Medium)	2023-05-03	8.8	High
CVE-2023-28742	f5 - multiple products	When DNS is provisioned, an authenticated remote command execution vulnerability exists in DNS iQuery mesh. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-05-03	8.8	High
CVE-2023-22640	fortinet - multiple products	A out-of-bounds write in Fortinet FortiOS version 7.2.0 through 7.2.3, FortiOS version 7.0.0 through 7.0.10, FortiOS version 6.4.0 through 6.4.11, FortiOS version 6.2.0 through 6.2.13, FortiOS all versions 6.0, FortiProxy version 7.2.0 through 7.2.1, FortiProxy version 7.0.0 through 7.0.7, FortiProxy all versions 2.0, FortiProxy all versions 1.2, FortiProxy all versions 1.1, FortiProxy all versions 1.0 allows an authenticated attacker to execute unauthorized code or commands via specifically crafted requests.	2023-05-03	8.8	High
CVE-2023-31099	zohocorp - multiple products	Zoho ManageEngine OPManager through 126323 allows an authenticated user to achieve remote code execution via probe servers.	2023-05-04	8.8	High
CVE-2023-24958	ibm - multiple products	A vulnerability in the IBM TS7700 Management Interface 8.51.2.12, 8.52.200.111, 8.52.102.13, and 8.53.0.63 could allow an authenticated user to submit a specially crafted URL leading to privilege escalation and remote code execution. IBM X-Force ID: 246320.	2023-05-04	8.8	High
CVE-2022-45048	apache - ranger	Authenticated users with appropriate privileges can create policies having expressions that can exploit code execution vulnerability. This issue affects Apache Ranger: 2.3.0. Users are recommended to update to version 2.4.0.	2023-05-05	8.8	High
CVE-2023-21505	samsung - samsung_core_services	Improper access control in Samsung Core Service prior to version 2.1.00.36 allows attacker to write arbitrary file in sandbox.	2023-05-04	8.6	High
CVE-2023-28656	f5 - multiple products	NGINX Management Suite may allow an authenticated attacker to gain access to configuration objects outside of their assigned environment. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-05-03	8.1	High
CVE-2021-40331	apache - ranger	An Incorrect Permission Assignment for Critical Resource vulnerability was found in the Apache Ranger Hive Plugin. Any user with SELECT privilege on a database can alter the ownership of the table in Hive when Apache Ranger Hive Plugin is enabled This issue affects Apache Ranger Hive Plugin: from 2.0.0 through 2.3.0. Users are recommended to upgrade to version 2.4.0 or later.	2023-05-05	8.1	High
CVE-2022-41736	ibm - spectrum_scale_container_native_storage_access	IBM Spectrum Scale Container Native Storage Access 5.1.2.1 through 5.1.6.0	2023-04-29	7.8	High

		contains an unspecified vulnerability that could allow a local user to obtain root privileges. IBM X-Force ID: 237810.			
CVE-2023-2235	linux - multiple products	A use-after-free vulnerability in the Linux Kernel Performance Events system can be exploited to achieve local privilege escalation. The perf_group_detach function did not check the event's siblings' attach_state before calling add_event_to_groups(), but remove_on_exec made it possible to call list_del_event() on before detaching from their group, making it possible to use a dangling pointer causing a use-after-free vulnerability. We recommend upgrading past commit fd0815f632c24878e325821943edccc7fde947a2.	2023-05-01	7.8	High
CVE-2023-2236	linux - multiple products	A use-after-free vulnerability in the Linux Kernel io_uring subsystem can be exploited to achieve local privilege escalation. Both io_install_fixed_file and its callers call fput in a file in case of an error, causing a reference underflow which leads to a use-after-free vulnerability. We recommend upgrading past commit 9d94c04c0db024922e886c9fd429659f22f48ea4.	2023-05-01	7.8	High
CVE-2022-4568	lenovo - system_update	A directory permissions management vulnerability in Lenovo System Update may allow elevation of privileges.	2023-05-01	7.8	High
CVE-2022-25713	qualcomm - ar8035_firmware	Memory corruption in Automotive due to Improper Restriction of Operations within the Bounds of a Memory Buffer while exporting a shared key.	2023-05-02	7.8	High
CVE-2022-33281	qualcomm - wcn685x-5_firmware	Memory corruption due to improper validation of array index in computer vision while testing EVA kernel without sending any frames.	2023-05-02	7.8	High
CVE-2022-33292	qualcomm - sg4150p_firmware	Memory corruption in Qualcomm IPC due to use after free while receiving the incoming packet and reposting it.	2023-05-02	7.8	High
CVE-2023-21642	qualcomm - qam8295p_firmware	Memory corruption in HAB Memory management due to broad system privileges via physical address.	2023-05-02	7.8	High
CVE-2023-21665	qualcomm - 315_5g_iot_modem_firmware	Memory corruption in Graphics while importing a file.	2023-05-02	7.8	High
CVE-2023-21666	qualcomm - wcn3998_firmware	Memory Corruption in Graphics while accessing a buffer allocated through the graphics pool.	2023-05-02	7.8	High
CVE-2023-28070	dell - alienware_command_center	Alienware Command Center Application, versions 5.5.43.0 and prior, contain an improper access control vulnerability. A local malicious user could potentially exploit this vulnerability during installation or update process leading to privilege escalation.	2023-05-03	7.8	High
CVE-2023-26203	fortinet - multiple products	A use of hard-coded credentials vulnerability [CWE-798] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions may allow an authenticated attacker to access to the database via shell commands.	2023-05-03	7.8	High
CVE-2023-27999	fortinet - multiple products	An improper neutralization of special elements used in an OS command vulnerability [CWE-78] in FortiADC 7.2.0, 7.1.0 through 7.1.1 may allow an authenticated attacker to execute unauthorized commands via specifically crafted arguments to existing commands.	2023-05-03	7.8	High
CVE-2023-21484	samsung - multiple products	Improper access control vulnerability in AppLock prior to SMR May-2023 Release 1 allows local attackers without proper permission to execute a privileged operation.	2023-05-04	7.8	High
CVE-2023-21488	samsung - multiple products	Improper access control vulnerablility in Tips prior to SMR May-2023 Release 1 allows local attackers to launch arbitrary activity in Tips.	2023-05-04	7.8	High
CVE-2023-21491	samsung - multiple products	Improper access control vulnerability in ThemeManager prior to SMR May-2023 Release 1 allows local attackers to write arbitrary files with system privilege.	2023-05-04	7.8	High
CVE-2023-21497	samsung - multiple products	Use of externally-controlled format string vulnerability in mPOS TUI trustlet prior to SMR May-2023 Release 1 allows local attackers to access the memory address.	2023-05-04	7.8	High
CVE-2023-21498	samsung - multiple products	Improper input validation vulnerability in setPartnerTAInfo in mPOS TUI trustlet prior to SMR May-2023 Release 1 allows local attackers to overwrite the trustlet memory.	2023-05-04	7.8	High
CVE-2023-21499	samsung - multiple products	Out-of-bounds write vulnerability in TA_Communication_mpos_encrypt_pin in mPOS TUI trustlet prior to SMR May-2023 Release 1 allows local attackers to execute arbitrary code.	2023-05-04	7.8	High
CVE-2023-21501	samsung - multiple products	Improper input validation vulnerability in mPOS fiserve trustlet prior to SMR May-2023 Release 1 allows local attackers to execute arbitrary code.	2023-05-04	7.8	High

CVE-2023-21502	samsung - multiple products	Improper input validation vulnerability in FactoryTest application prior to SMR May-2023 Release 1 allows local attackers to get privilege escalation via debugging commands.	2023-05-04	7.8	High
CVE-2023-21506	samsung - samsung_blockchain_keystore	Out-of-bounds Write vulnerability while processing BC_TUI_CMD_SEND_RESOURCE_DATA_ARRAY command in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to execute arbitrary code.	2023-05-04	7.8	High
CVE-2023-21508	samsung - samsung_blockchain_keystore	Out-of-bounds Write vulnerability while processing BC_TUI_CMD_SEND_RESOURCE_DATA command in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to execute arbitrary code.	2023-05-04	7.8	High
CVE-2023-21509	samsung - samsung_blockchain_keystore	Out-of-bounds Write vulnerability while processing BC_TUI_CMD_UPDATE_SCREEN in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to execute arbitrary code.	2023-05-04	7.8	High
CVE-2023-28068	dell - command_|_monitor	Dell Command Monitor, versions 10.9 and prior, contains an improper folder permission vulnerability. A local authenticated malicious user can potentially exploit this vulnerability leading to privilege escalation by writing to a protected directory when Dell Command Monitor is installed to a non-default path	2023-05-05	7.8	High
CVE-2023-30441	ibm - multiple products	IBM Runtime Environment, Java Technology Edition IBMJCEPlus and JSSE 8.0.7.0 through 8.0.7.11 components could expose sensitive information using a combination of flaws and configurations. IBM X-Force ID: 253188.	2023-04-29	7.5	High
CVE-2022-48186	lenovo - baiying	A certificate validation vulnerability exists in the Baiying Android application which could lead to information disclosure.	2023-05-01	7.5	High
CVE-2023-22921	zyxel - nbg-418n_firmware	A cross-site scripting (XSS) vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker with administrator privileges to store malicious scripts using a web management interface parameter, resulting in denial-of-service (DoS) conditions on an affected device.	2023-05-01	7.5	High
CVE-2023-22922	zyxel - nbg-418n_firmware	A buffer overflow vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote unauthenticated attacker to cause DoS conditions by sending crafted packets if Telnet is enabled on a vulnerable device.	2023-05-01	7.5	High
CVE-2022-33304	qualcomm - 9205_lte_modem_firmware	Transient DOS due to NULL pointer dereference in Modem while performing pullup for received TCP/UDP packet.	2023-05-02	7.5	High
CVE-2022-33305	qualcomm - 315_5g_iot_modem_firmware	Transient DOS due to NULL pointer dereference in Modem while sending invalid messages in DCCH.	2023-05-02	7.5	High
CVE-2022-34144	qualcomm - 315_5g_iot_modem_firmware	Transient DOS due to reachable assertion in Modem during OSI decode scheduling.	2023-05-02	7.5	High
CVE-2022-40505	qualcomm - 9205_lte_modem_firmware	Information disclosure due to buffer over-read in Modem while parsing DNS hostname.	2023-05-02	7.5	High
CVE-2022-40508	qualcomm - 315_5g_iot_modem_firmware	Transient DOS due to reachable assertion in Modem while processing config related to cross carrier scheduling, which is not supported.	2023-05-02	7.5	High
CVE-2022-40504	qualcomm - 315_5g_iot_modem_firmware	Transient DOS due to reachable assertion in Modem when UE received Downlink Data Indication message from the network.	2023-05-02	7.5	High
CVE-2023-24594	f5 - multiple products	When an SSL profile is configured on a Virtual Server, undisclosed traffic can cause an increase in CPU or SSL accelerator resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-05-03	7.5	High
CVE-2023-29163	f5 - multiple products	When UDP profile with idle timeout set to immediate or the value 0 is configured on a virtual server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-05-03	7.5	High
CVE-2022-45860	fortinet - multiple products	A weak authentication vulnerability [CWE-1390] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.2 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions in device registration page may allow an unauthenticated attacker to perform password spraying attacks with an increased chance of success.	2023-05-03	7.5	High
CVE-2023-25934	dell - elastic_cloud_storage	DELL ECS prior to 3.8.0.2 contains an improper verification of cryptographic signature vulnerability. A network attacker with an ability to intercept the request could potentially exploit this vulnerability to modify the body data of the request.	2023-05-04	7.5	High
CVE-2023-26285	ibm - multiple products	IBM MQ 9.2 CD, 9.2 LTS, 9.3 CD, and 9.3 LTS could allow a remote attacker to cause a denial of service due to an error processing invalid data. IBM X-Force ID: 248418.	2023-05-05	7.5	High
CVE-2023-29350	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability	2023-05-05	7.5	High

CVE-2022-22313	ibm - qradar_data_synchronization	IBM QRadar Data Synchronization App 1.0 through 3.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 217370.	2023-05-06	7.5	High
CVE-2022-45858	fortinet - multiple products	A use of a weak cryptographic algorithm vulnerability [CWE-327] in FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.0 all versions, 8.8.0 all versions, 8.7.0 all versions may increase the chances of an attacker to have access to sensitive information or to perform man-in-the-middle attacks.	2023-05-03	7.4	High
CVE-2023-23470	ibm - multiple products	IBM i 7.2, 7.3, 7.4, and 7.5 could allow an authenticated privileged administrator to gain elevated privileges in non-default configurations, as a result of improper SQL processing. By using a specially crafted SQL operation, the administrator could exploit the vulnerability to perform additional administrator operations. IBM X-Force ID: 244510.	2023-05-04	7.2	High
CVE-2023-2460	google - chrome	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to bypass file access checks via a crafted HTML page. (Chromium security severity: Medium)	2023-05-03	7.1	High
CVE-2023-28724	f5 - multiple products	NGINX Management Suite default file permissions are set such that an authenticated attacker may be able to modify sensitive files on NGINX Instance Manager and NGINX API Connectivity Manager. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-05-03	7.1	High
CVE-2023-27993	fortinet - multiple products	A relative path traversal [CWE-23] in Fortinet FortiADC version 7.2.0 and before 7.1.1 allows a privileged attacker to delete arbitrary directories from the underlying file system via crafted CLI commands.	2023-05-03	7.1	High
CVE-2023-21490	samsung - multiple products	Improper access control in GearManagerStub prior to SMR May-2023 Release 1 allows a local attacker to delete applications installed by watchmanager.	2023-05-04	7.1	High
CVE-2023-28092	hp - integrated_lights-out_firmware	A potential security vulnerability has been identified in HPE ProLiant RL300 Gen11 Server. The vulnerability could result in the system being vulnerable to exploits by attackers with physical access inside the server chassis.	2023-05-01	6.8	Medium
CVE-2023-21489	samsung - multiple products	Heap out-of-bounds write vulnerability in bootloader prior to SMR May-2023 Release 1 allows a physical attacker to execute arbitrary code.	2023-05-04	6.8	Medium
CVE-2023-32269	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.1.11. In net/netrom/af_netrom.c, there is a use-after-free because accept is also allowed for a successfully connected AF_NETROM socket. However, in order for an attacker to exploit this, the system must have netrom routing configured or the attacker must have the CAP_NET_ADMIN capability.	2023-05-05	6.7	Medium
CVE-2023-22923	zyxel - nbg-418n_firmware	A format string vulnerability in a binary of the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker to cause denial-of-service (DoS) conditions on an affected device.	2023-05-01	6.5	Medium
CVE-2023-2459	google - chrome	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to bypass permission restrictions via a crafted HTML page. (Chromium security severity: Medium)	2023-05-03	6.5	Medium
CVE-2023-28406	f5 - multiple products	A directory traversal vulnerability exists in an undisclosed page of the BIG-IP Configuration utility which may allow an authenticated attacker to read files with .xml extension. Access to restricted information is limited and the attacker does not control what information is obtained. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-05-03	6.5	Medium
CVE-2022-43919	ibm - multiple products	IBM MQ 9.2 CD, 9.2 LTS, 9.3 CD, and 9.3 LTS could allow an authenticated attacker with authorization to craft messages to cause a denial of service. IBM X-Force ID: 241354.	2023-05-05	6.5	Medium
CVE-2023-27378	f5 - multiple products	Multiple reflected cross-site scripting (XSS) vulnerabilities exist in undisclosed pages of the BIG-IP Configuration utility which allow an attacker to run JavaScript in the context of the currently logged-in user. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-05-03	6.1	Medium
CVE-2023-22372	f5 - multiple products	In the pre connection stage, an improper enforcement of message integrity vulnerability exists in BIG-IP Edge Client for Windows and Mac OS. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-05-03	5.9	Medium
CVE-2023-24461	f5 - multiple products	An improper certificate validation vulnerability exists in the BIG-IP Edge Client for Windows and macOS and may allow an attacker to impersonate a BIG-IP APM system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-05-03	5.9	Medium

CVE-2022-33273	qualcomm - aqt1000_firmware	Information disclosure due to buffer over-read in Trusted Execution Environment while QRKS report generation.	2023-05-02	5.5	Medium
CVE-2023-21493	samsung - multiple products	Improper access control vulnerability in SemShareFileProvider prior to SMR May-2023 Release 1 allows local attackers to access protected data.	2023-05-04	5.5	Medium
CVE-2023-21495	samsung - multiple products	Improper access control vulnerability in Knox Enrollment Service prior to SMR May-2023 Release 1 allow attacker install KSP app when device admin is set.	2023-05-04	5.5	Medium
CVE-2023-21496	samsung - multiple products	Active Debug Code vulnerability in ActivityManagerService prior to SMR May-2023 Release 1 allows attacker to use debug function via setting debug level.	2023-05-04	5.5	Medium
CVE-2023-21500	samsung - multiple products	Double free validation vulnerability in setPinPadImages in mPOS TUI trustlet prior to SMR May-2023 Release 1 allows local attackers to access the trustlet memory.	2023-05-04	5.5	Medium
CVE-2023-21507	samsung - samsung_blockchain_keystore	Out-of-bounds Read vulnerability while processing BC_TUI_CMD_SEND_RESOURCE_DATA_ARRAY command in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to read arbitrary memory.	2023-05-04	5.5	Medium
CVE-2023-21510	samsung - samsung_blockchain_keystore	Out-of-bounds Read vulnerability while processing BC_TUI_CMD_UPDATE_SCREEN in bc_tui trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to read arbitrary memory.	2023-05-04	5.5	Medium
CVE-2023-21511	samsung - samsung_blockchain_keystore	Out-of-bounds Read vulnerability while processing CMD_COLDWALLET_BTC_SET_PRV_UTXO in bc_core trustlet from Samsung Blockchain Keystore prior to version 1.3.12.1 allows local attacker to read arbitrary memory.	2023-05-04	5.5	Medium
CVE-2022-38707	ibm - cognos_command_center	IBM Cognos Command Center 10.2.4.1 could allow a local attacker to obtain sensitive information due to insufficient session expiration. IBM X-Force ID: 234179.	2023-05-05	5.5	Medium
CVE-2023-22874	ibm - multiple products	IBM MQ Clients 9.2 CD, 9.3 CD, and 9.3 LTS are vulnerable to a denial of service attack when processing configuration files. IBM X-Force ID: 244216.	2023-05-05	5.5	Medium
CVE-2023-30434	ibm - multiple products	IBM Storage Scale (IBM Spectrum Scale 5.1.0.0 through 5.1.2.9, 5.1.3.0 through 5.1.6.1 and IBM Elastic Storage Systems 6.1.0.0 through 6.1.2.5, 6.1.3.0 through 6.1.6.0) could allow a local user to cause a kernel panic. IBM X-Force ID: 252187.	2023-05-05	5.5	Medium
CVE-2020-4914	ibm - cloud_pak_system	IBM Cloud Pak System Suite 2.3.3.0 through 2.3.3.5 does not invalidate session after logout which could allow a local user to impersonate another user on the system. IBM X-Force ID: 191290.	2023-05-05	5.5	Medium
CVE-2022-43877	ibm - multiple products	IBM UrbanCode Deploy (UCD) versions up to 7.3.0.1 could disclose sensitive password information during a manual edit of the agentrelay.properties file. IBM X-Force ID: 240148.	2023-05-06	5.5	Medium
CVE-2022-43871	ibm - financial_transaction_manager_for_multiplatform	IBM Financial Transaction Manager for SWIFT Services 3.2.4 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: 239707.	2023-04-29	5.4	Medium
CVE-2022-45801	apache - streampark	Apache StreamPark 1.0.0 to 2.0.0 have a LDAP injection vulnerability. LDAP Injection is an attack used to exploit web based applications that construct LDAP statements based on user input. When an application fails to properly sanitize user input, it's possible to modify LDAP statements through techniques similar to SQL Injection. LDAP injection attacks could result in the granting of permissions to unauthorized queries, and content modification inside the LDAP tree. This risk may only occur when the user logs in with ldap, and the user name and password login will not be affected, Users of the affected versions should upgrade to Apache StreamPark 2.0.0 or later.	2023-05-01	5.4	Medium
CVE-2023-29240	f5 - big-iq_centralized_management	An authenticated attacker granted a Viewer or Auditor role on a BIG-IQ can upload arbitrary files using an undisclosed iControl REST endpoint. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2023-05-03	5.4	Medium
CVE-2022-43866	ibm - multiple products	IBM Maximo Asset Management 7.6.1.2 and 7.6.1.3 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: 239436.	2023-05-05	5.4	Medium
CVE-2023-22503	atlassian - multiple products	Affected versions of Atlassian Confluence Server and Data Center allow anonymous remote attackers to view the names of attachments and labels in a private Confluence space. This occurs via an Information Disclosure vulnerability in the macro preview feature.	2023-05-01	5.3	Medium

		This vulnerability was reported by Rojan Rijal of the Tinder Security Engineering team. The affected versions are before version 7.13.15, from version 7.14.0 before 7.19.7, and from version 7.20.0 before 8.2.0.			
CVE-2023-26268	apache - multiple products	Design documents with matching document IDs, from databases on the same cluster, may share a mutable Javascript environment when using these design document functions: * validate_doc_update * list * filter * filter views (using view functions as filters) * rewrite * update This doesn't affect map/reduce or search (Dreyfus) index functions. Users are recommended to upgrade to a version that is no longer affected by this issue (Apache CouchDB 3.3.2 or 3.2.3). Workaround: Avoid using design documents from untrusted sources which may attempt to cache or store data in the Javascript environment.	2023-05-02	5.3	Medium
CVE-2022-39161	ibm - multiple products	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0, and IBM WebSphere Application Server Liberty, when configured to communicate with the Web Server Plug-ins for IBM WebSphere Application Server, could allow an authenticated user to conduct spoofing attacks. A man-in-the-middle attacker could exploit this vulnerability using a certificate issued by a trusted authority to obtain sensitive information. IBM X-Force ID: 235069.	2023-05-03	5.3	Medium
CVE-2023-22924	zyxel - nbg-418n_firmware	A buffer overflow vulnerability in the Zyxel NBG-418N v2 firmware versions prior to V1.00(AARP.14)C0 could allow a remote authenticated attacker with administrator privileges to cause denial-of-service (DoS) conditions by executing crafted CLI commands on a vulnerable device.	2023-05-01	4.9	Medium
CVE-2018-25085	drupal - responsive_menus	A vulnerability classified as problematic was found in Responsive Menus 7.x-1.x-dev on Drupal. Affected by this vulnerability is the function responsive_menus_admin_form_submit of the file responsive_menus.module of the component Configuration Setting Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 7.x-1.7 is able to address this issue. The name of the patch is 3c554b31d32a367188f44d44857b061eac949fb8. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-227755.	2023-05-01	4.8	Medium
CVE-2022-43950	fortinet - multiple products	A URL redirection to untrusted site ('Open Redirect') vulnerability [CWE-601] in FortiNAC-F version 7.2.0, FortiNAC version 9.4.1 and below, 9.2 all versions, 9.1 all versions, 8.8 all versions, 8.7 all versions may allow an unauthenticated attacker to redirect users to any arbitrary website via a crafted URL.	2023-05-03	4.7	Medium
CVE-2023-29354	microsoft - edge_chromium	Microsoft Edge (Chromium-based) Security Feature Bypass Vulnerability	2023-05-05	4.7	Medium
CVE-2023-21485	samsung - multiple products	Improper export of android application components vulnerability in VideoPreviewActivity in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox.	2023-05-04	4.6	Medium
CVE-2023-21486	samsung - multiple products	Improper export of android application components vulnerability in ImagePreviewActivity in Call Settings to SMR May-2023 Release 1 allows physical attackers to access some media data stored in sandbox.	2023-05-04	4.6	Medium
CVE-2022-45859	fortinet - multiple products	An insufficiently protected credentials vulnerability [CWE-522] in FortiNAC-F 7.2.0, FortiNAC 9.4.1 and below, 9.2.6 and below, 9.1.8 and below, 8.8.0 all versions, 8.7.0 all versions may allow a local attacker with system access to retrieve users' passwords.	2023-05-03	4.4	Medium

CVE-2023-21492	samsung - multiple products	Kernel pointers are printed in the log file prior to SMR May-2023 Release 1 allows a privileged local attacker to bypass ASLR.	2023-05-04	4.4	Medium
CVE-2023-2462	google - chrome	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to obfuscate main origin data via a crafted HTML page. (Chromium security severity: Medium)	2023-05-03	4.3	Medium
CVE-2023-2463	google - chrome	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	2023-05-03	4.3	Medium
CVE-2023-2464	google - chrome	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed an attacker who convinced a user to install a malicious extension to perform an origin spoof in the security UI via a crafted HTML page. (Chromium security severity: Medium)	2023-05-03	4.3	Medium
CVE-2023-2465	google - chrome	Inappropriate implementation in CORS in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2023-05-03	4.3	Medium
CVE-2023-2466	google - chrome	Inappropriate implementation in Prompts in Google Chrome prior to 113.0.5672.63 allowed a remote attacker to spoof the contents of the security UI via a crafted HTML page. (Chromium security severity: Low)	2023-05-03	4.3	Medium
CVE-2023-2467	google - chrome	Inappropriate implementation in Prompts in Google Chrome on Android prior to 113.0.5672.63 allowed a remote attacker to bypass permissions restrictions via a crafted HTML page. (Chromium security severity: Low)	2023-05-03	4.3	Medium
CVE-2023-2468	google - chrome	Inappropriate implementation in PictureInPicture in Google Chrome prior to 113.0.5672.63 allowed a remote attacker who had compromised the renderer process to obfuscate the security UI via a crafted HTML page. (Chromium security severity: Low)	2023-05-03	4.3	Medium
CVE-2023-21487	samsung - multiple products	Improper access control vulnerability in Telephony framework prior to SMR May-2023 Release 1 allows local attackers to change a call setting.	2023-05-04	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.