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 ٢١ مايو إلى ٢٧ 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

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 21st of May to 27th 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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score	Severity
CVE-2023-33250	linux - linux_kernel	The Linux kernel 6.3 has a use-after-free in iopt_unmap_iova_range in drivers/iommu/iommufd/io_pagetable.c.	2023-05-21	9.8	Critical
CVE-2020-36694	linux - linux_kernel	An issue was discovered in netfilter in the Linux kernel before 5.10. There can be a use-after-free in the packet processing context, because the per-CPU sequence count is mishandled during concurrent iptables rules replacement. This could be exploited with the CAP_NET_ADMIN capability in an unprivileged namespace. NOTE: cc00bca was reverted in 5.12.	2023-05-21	9.8	Critical
CVE-2023-32336	ibm - infosphere_information_server	IBM InfoSphere Information Server 11.7 is affected by a remote code execution vulnerability due to insecure deserialization in an RMI service. IBM X-Force ID: 255285.	2023-05-22	9.8	Critical
CVE-2022-46680	schneider-electric - powerlogic_ion9000_firmware	A CWE-319: Cleartext transmission of sensitive information vulnerability exists that could cause disclosure of sensitive information, denial of service, or modification of data if an attacker is able to intercept network traffic.	2023-05-22	9.8	Critical
CVE-2023-31062	apache - inlong	Improper Privilege Management Vulnerabilities in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.2.0 through 1.6.0. When the attacker has access to a valid (but unprivileged) account, the exploit can be executed using Burp Suite by sending a login request and following it with a subsequent HTTP request using the returned cookie. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7836 https://github.com/apache/inlong/pull/7836 to solve it.	2023-05-22	9.8	Critical
CVE-2023-31098	apache - inlong	Weak Password Requirements vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.1.0 through 1.6.0. When users change their password to a simple password (with any character or symbol), attackers can easily guess the user's password and access the account. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7805 https://github.com/apache/inlong/pull/7805 to solve it.	2023-05-22	9.8	Critical
CVE-2023-33246	apache - rocketmq	For RocketMQ versions 5.1.0 and below, under certain conditions, there is a risk of remote command execution. Several components of RocketMQ, including NameServer, Broker, and Controller, are leaked on the extranet and lack permission verification, an attacker can exploit this vulnerability by using the update configuration function to execute commands as the system users that RocketMQ is running as. Additionally, an attacker can achieve the same effect by forging the RocketMQ protocol content.	2023-05-24	9.8	Critical

		To prevent these attacks, users are recommended to upgrade to version 5.1.1 or above for using RocketMQ 5.x or 4.9.6 or above for using RocketMQ 4.x .			
CVE-2023-31457	mitel - mivoice_connect	A vulnerability in the Headquarters server component of Mitel MiVoice Connect versions 19.3 SP2 (22.24.1500.0) and earlier could allow an unauthenticated attacker with internal network access to execute arbitrary scripts due to improper access control.	2023-05-24	9.8	Critical
CVE-2023-31458	mitel - mivoice_connect	A vulnerability in the Edge Gateway component of Mitel MiVoice Connect versions 19.3 SP2 (22.24.1500.0) and earlier could allow an unauthenticated attacker with internal network access to authenticate with administrative privileges, because initial installation does not enforce a password change. A successful exploit could allow an attacker to make arbitrary configuration changes and execute arbitrary commands.	2023-05-24	9.8	Critical
CVE-2021-46887	huawei - multiple products	Lack of length check vulnerability in the HW_KEYMASTER module. Successful exploitation of this vulnerability may cause out-of-bounds read.	2023-05-26	9.8	Critical
CVE-2022-48478	huawei - harmonyos	The facial recognition TA of some products lacks memory length verification. Successful exploitation of this vulnerability may cause exceptions of the facial recognition service.	2023-05-26	9.8	Critical
CVE-2022-48479	huawei - harmonyos	The facial recognition TA of some products has the out-of-bounds memory read vulnerability. Successful exploitation of this vulnerability may cause exceptions of the facial recognition service.	2023-05-26	9.8	Critical
CVE-2023-21514	samsung - galaxy_store	Improper scheme validation from InstantPlay Deeplink in Galaxy Store prior to version 4.5.49.8 allows attackers to execute javascript API to install APK from Galaxy Store.	2023-05-26	9.8	Critical
CVE-2023-21516	samsung - galaxy_store	XSS vulnerability from InstantPlay in Galaxy Store prior to version 4.5.49.8 allows attackers to execute javascript API to install APK from Galaxy Store.	2023-05-26	9.6	Critical
CVE-2023-31065	apache - inlong	Insufficient Session Expiration vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0. An old session can be used by an attacker even after the user has been deleted or the password has been changed. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7836 https://github.com/apache/inlong/pull/7836 , https://github.com/apache/inlong/pull/7884 https://github.com/apache/inlong/pull/7884 to solve it.	2023-05-22	9.1	Critical
CVE-2023-31066	apache - inlong	Files or Directories Accessible to External Parties vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0. Different users in InLong could delete, edit, stop, and start others' sources! Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7775 https://github.com/apache/inlong/pull/7775 to solve it.	2023-05-22	9.1	Critical
CVE-2023-31459	mitel - mivoice_connect	A vulnerability in the Connect Mobility Router component of Mitel MiVoice Connect versions 9.6.2208.101 and earlier could allow an unauthenticated attacker with internal network access to authenticate with administrative privileges, because the initial installation does not enforce a password change. A successful exploit could allow an attacker to make arbitrary configuration changes and execute arbitrary commands.	2023-05-24	8.8	High
CVE-2022-47161	wordpress - health_check_\&_troubleshooting	Cross-Site Request Forgery (CSRF) vulnerability in The WordPress.Org community Health Check & Troubleshooting plugin <= 1.5.1 versions.	2023-05-25	8.8	High
CVE-2022-47174	wordpress - performance_lab	Cross-Site Request Forgery (CSRF) vulnerability in WordPress Performance Team Performance Lab plugin <= 2.2.0 versions.	2023-05-25	8.8	High
CVE-2023-21515	samsung - galaxy_store	InstantPlay which included vulnerable script which could execute javascript in Galaxy Store prior to version 4.5.49.8 allows attackers to execute javascript API to install APK from Galaxy Store.	2023-05-26	8.8	High
CVE-2023-23693	dell - vxrail_hyperconverged_infrastructure	Dell VxRail, versions prior to 7.0.450, contains an OS command injection Vulnerability in DCManager command-line utility. A local high privileged attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker.	2023-05-23	8.2	High
CVE-2023-33945	liferay - multiple products	SQL injection vulnerability in the upgrade process for SQL Server in Liferay Portal 7.3.1 through 7.4.3.17, and Liferay DXP 7.3 before update 6, and 7.4 before update 18 allows attackers to execute arbitrary SQL commands via the name of a database table's primary key index. This vulnerability is only exploitable when chained with other attacks. To exploit this vulnerability, the attacker must modify the database and wait for the application to be upgraded.	2023-05-24	8.1	High

CVE-2023-30440	ibm - multiple products	IBM PowerVM Hypervisor FW860.00 through FW860.B3, FW950.00 through FW950.70, FW1010.00 through FW1010.50, FW1020.00 through FW1020.30, and FW1030.00 through FW1030.10 could allow a local attacker with control a partition that has been assigned SRIOV virtual function (VF) to cause a denial of service to a peer partition or arbitrary data corruption. IBM X-Force ID: 253175.	2023-05-23	7.9	High
CVE-2023-25537	dell - poweredge_r740_firmware	Dell PowerEdge 14G server BIOS versions prior to 2.18.1 and Dell Precision BIOS versions prior to 2.18.2, contain an Out of Bounds write vulnerability. A local attacker with low privileges could potentially exploit this vulnerability leading to exposure of some SMRAM stack/data/code in System Management Mode, leading to arbitrary code execution or escalation of privilege.	2023-05-22	7.8	High
CVE-2023-23694	dell - vxrail_hyperconverged_infrastructure	Dell VxRail versions earlier than 7.0.450, contain(s) an OS command injection vulnerability in VxRail Manager. A local authenticated attacker could potentially exploit this vulnerability, leading to the execution of arbitrary OS commands on the application's underlying OS, with the privileges of the vulnerable application. Exploitation may lead to a system take over by an attacker.	2023-05-23	7.8	High
CVE-2023-28709	apache - multiple products	The fix for CVE-2023-24998 was incomplete for Apache Tomcat 11.0.0-M2 to 11.0.0-M4, 10.1.5 to 10.1.7, 9.0.71 to 9.0.73 and 8.5.85 to 8.5.87. If non-default HTTP connector settings were used such that the maxParameterCount could be reached using query string parameters and a request was submitted that supplied exactly maxParameterCount parameters in the query string, the limit for uploaded request parts could be bypassed with the potential for a denial of service to occur.	2023-05-22	7.5	High
CVE-2023-31058	apache - inlong	Deserialization of Untrusted Data Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0. Attackers would bypass the 'autoDeserialize' option filtering by adding blanks. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick	2023-05-22	7.5	High
CVE-2023-31206	apache - inlong	Exposure of Resource to Wrong Sphere Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0. Attackers can change the immutable name and type of nodes of InLong. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick [1] to solve it.	2023-05-22	7.5	High
CVE-2023-31453	apache - inlong	Incorrect Permission Assignment for Critical Resource Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.2.0 through 1.6.0. The attacker can delete others' subscriptions, even if they are not the owner of the deleted subscription. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick [1] to solve it.	2023-05-22	7.5	High
CVE-2023-31454	apache - inlong	Incorrect Permission Assignment for Critical Resource Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.2.0 through 1.6.0. The attacker can bind any cluster, even if he is not the cluster owner.	2023-05-22	7.5	High
CVE-2023-31064	apache - inlong	Files or Directories Accessible to External Parties vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.2.0 through 1.6.0. the user in InLong could cancel an application that doesn't belongs to it. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7799 https://github.com/apache/inlong/pull/7799 to solve it.	2023-05-22	7.5	High
CVE-2023-31103	apache - inlong	Exposure of Resource to Wrong Sphere Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.4.0 through 1.6.0. Attackers can change the immutable name and type of cluster of InLong. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7891 https://github.com/apache/inlong/pull/7891 to solve it.	2023-05-22	7.5	High
CVE-2023-33948	liferay - multiple products	The Dynamic Data Mapping module in Liferay Portal 7.4.3.67, and Liferay DXP 7.4 update 67 does not limit Document and Media files which can be downloaded from a Form, which allows remote attackers to download any file from Document and Media via a crafted URL.	2023-05-24	7.5	High
CVE-2023-33949	liferay - multiple products	In Liferay Portal 7.3.0 and earlier, and Liferay DXP 7.2 and earlier the default configuration does not require users to verify their email address, which allows remote attackers to create accounts using fake email addresses or email addresses which they don't control. The portal property `company.security.strangers.verify` should be set to true.	2023-05-24	7.5	High
CVE-2023-33950	liferay - multiple products	Pattern Redirects in Liferay Portal 7.4.3.48 through 7.4.3.76, and Liferay DXP 7.4 update 48 through 76 allows regular expressions that are vulnerable to ReDoS attacks to be used as patterns, which	2023-05-24	7.5	High

		allows remote attackers to consume an excessive amount of server resources via crafted request URLs.			
CVE-2021-46881	huawei - multiple products	The video framework has memory overwriting caused by addition overflow. Successful exploitation of this vulnerability may affect availability.	2023-05-26	7.5	High
CVE-2021-46882	huawei - multiple products	The video framework has memory overwriting caused by addition overflow. Successful exploitation of this vulnerability may affect availability.	2023-05-26	7.5	High
CVE-2021-46883	huawei - multiple products	The video framework has memory overwriting caused by addition overflow. Successful exploitation of this vulnerability may affect availability.	2023-05-26	7.5	High
CVE-2021-46884	huawei - multiple products	The video framework has memory overwriting caused by addition overflow. Successful exploitation of this vulnerability may affect availability.	2023-05-26	7.5	High
CVE-2021-46885	huawei - multiple products	The video framework has memory overwriting caused by addition overflow. Successful exploitation of this vulnerability may affect availability.	2023-05-26	7.5	High
CVE-2021-46886	huawei - multiple products	The video framework has memory overwriting caused by addition overflow. Successful exploitation of this vulnerability may affect availability.	2023-05-26	7.5	High
CVE-2022-48480	huawei - multiple products	Integer overflow vulnerability in some phones. Successful exploitation of this vulnerability may affect service confidentiality.	2023-05-26	7.5	High
CVE-2023-0116	huawei - multiple products	The reminder module lacks an authentication mechanism for broadcasts received. Successful exploitation of this vulnerability may affect availability.	2023-05-26	7.5	High
CVE-2023-25599	mitel - multiple products	A vulnerability in the conferencing component of Mitel MiVoice Connect through 19.3 SP2 and 20.x, 21.x, and 22.x through 22.24.1500.0 could allow an unauthenticated attacker to conduct a reflected cross-site scripting (XSS) attack due to insufficient validation for the test_presenter.php page. A successful exploit could allow an attacker to execute arbitrary scripts.	2023-05-24	7.4	High
CVE-2023-31460	mitel - mivoice_connect	A vulnerability in the Connect Mobility Router component of MiVoice Connect versions 9.6.2208.101 and earlier could allow an authenticated attacker with internal network access to conduct a command injection attack due to insufficient restriction on URL parameters.	2023-05-24	7.2	High
CVE-2023-31101	apache - multiple products	Insecure Default Initialization of Resource Vulnerability in Apache Software Foundation Apache InLong.This issue affects Apache InLong: from 1.5.0 through 1.6.0. Users registered in InLong who joined later can see deleted users' data. Users are advised to upgrade to Apache InLong's 1.7.0 or cherry-pick https://github.com/apache/inlong/pull/7836 https://github.com/apache/inlong/pull/7836 to solve it.	2023-05-22	6.5	Medium
CVE-2023-22504	atlassian - multiple products	Affected versions of Atlassian Confluence Server allow remote attackers who have read permissions to a page, but not write permissions, to upload attachments via a Broken Access Control vulnerability in the attachments feature. The affected versions are before version 7.19.9.	2023-05-25	6.5	Medium
CVE-2023-1664	redhat - multiple products	A flaw was found in Keycloak. This flaw depends on a non-default configuration "Revalidate Client Certificate" to be enabled and the reverse proxy is not validating the certificate before Keycloak. Using this method an attacker may choose the certificate which will be validated by the server. If this happens and the KC_SPI_TRUSTSTORE_FILE_FILE variable is missing/misconfigured, any trustfile may be accepted with the logging information of "Cannot validate client certificate trust: Truststore not available". This may not impact availability as the attacker would have no access to the server, but consumer applications Integrity or Confidentiality may be impacted considering a possible access to them. Considering the environment is correctly set to use "Revalidate Client Certificate" this flaw is avoidable.	2023-05-26	6.5	Medium
CVE-2023-31664	wso2 - api_manager	A reflected cross-site scripting (XSS) vulnerability in /authenticationendpoint/login.do of WSO2 API Manager before 4.2.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the tenantDomain parameter.	2023-05-23	6.1	Medium
CVE-2023-33938	liferay - multiple products	Cross-site scripting (XSS) vulnerability in the App Builder module's custom object details page in Liferay Portal 7.3.0 through 7.4.0, and Liferay DXP 7.3 before update 14 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into an App Builder custom object's `Name` field.	2023-05-24	6.1	Medium
CVE-2023-33941	liferay - multiple products	Multiple cross-site scripting (XSS) vulnerabilities in the Plugin for OAuth 2.0 module's OAuth2ProviderApplicationRedirect class in Liferay Portal 7.4.3.41 through 7.4.3.52, and Liferay DXP 7.4 update 41 through 52 allow remote attackers to inject arbitrary web script or HTML via the (1) code, or (2) error parameter.	2023-05-24	6.1	Medium
CVE-2023-33944	liferay - multiple products	Cross-site scripting (XSS) vulnerability in Layout module in Liferay Portal 7.3.4 through 7.4.3.68, and Liferay DXP 7.3 before update 24, and 7.4 before update 69 allows remote attackers to inject	2023-05-24	6.1	Medium

		arbitrary web script or HTML via a crafted payload injected into a container type layout fragment's `URL` text field.			
CVE-2023-25598	mitel - mivoice_connect	A vulnerability in the conferencing component of Mitel MiVoice Connect through 19.3 SP2 and 20.x, 21.x, and 22.x through 22.24.1500.0 could allow an unauthenticated attacker to conduct a reflected cross-site scripting (XSS) attack due to insufficient validation for the home.php page. A successful exploit could allow an attacker to execute arbitrary scripts.	2023-05-24	6.1	Medium
CVE-2022-46907	apache - jspwiki	A carefully crafted request on several JSPWiki plugins could trigger an XSS vulnerability on Apache JSPWiki, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. Apache JSPWiki users should upgrade to 2.12.0 or later.	2023-05-25	6.1	Medium
CVE-2023-20868	vmware - nsx-t_data_center	NSX-T contains a reflected cross-site scripting vulnerability due to a lack of input validation. A remote attacker can inject HTML or JavaScript to redirect to malicious pages.	2023-05-26	6.1	Medium
CVE-2023-0459	linux - linux_kernel	Copy_from_user on 64-bit versions of the Linux kernel does not implement the __uaccess_begin_nospec allowing a user to bypass the "access_ok" check and pass a kernel pointer to copy_from_user(). This would allow an attacker to leak information. We recommend upgrading beyond commit 74e19ef0ff8061ef55957c3abd71614ef0f42f47	2023-05-25	5.5	Medium
CVE-2023-33937	liferay - multiple products	Stored cross-site scripting (XSS) vulnerability in Form widget configuration in Liferay Portal 7.1.0 through 7.3.0, and Liferay DXP 7.1 before fix pack 18, and 7.2 before fix pack 5 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a form's `name` field.	2023-05-24	5.4	Medium
CVE-2023-33939	liferay - multiple products	Cross-site scripting (XSS) vulnerability in the Modified Facet widget in Liferay Portal 7.1.0 through 7.4.3.12, and Liferay DXP 7.1 before fix pack 27, 7.2 before fix pack 18, 7.3 before update 4, and 7.4 before update 9 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a facet label.	2023-05-24	5.4	Medium
CVE-2023-33940	liferay - multiple products	Cross-site scripting (XSS) vulnerability in IFrame type Remote Apps in Liferay Portal 7.4.0 through 7.4.3.30, and Liferay DXP 7.4 before update 31 allows remote attackers to inject arbitrary web script or HTML via the Remote App's IFrame URL.	2023-05-24	5.4	Medium
CVE-2023-33942	liferay - multiple products	Cross-site scripting (XSS) vulnerability in the Web Content Display widget's article selector in Liferay Liferay Portal 7.4.3.50, and Liferay DXP 7.4 update 50 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a web content article's `Title` field.	2023-05-24	5.4	Medium
CVE-2023-33943	liferay - multiple products	Cross-site scripting (XSS) vulnerability in the Account module in Liferay Portal 7.4.3.21 through 7.4.3.62, and Liferay DXP 7.4 update 21 through 62 allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a user's (1) First Name, (2) Middle Name, (3) Last Name, or (4) Job Title text field.	2023-05-24	5.4	Medium
CVE-2023-0117	huawei - emui	The online authentication provided by the hwKitAssistant lacks strict identity verification of applications. Successful exploitation of this vulnerability may affect availability of features,such as MeeTime.	2023-05-26	5.3	Medium
CVE-2023-27311	netapp - blue_xp_connector	NetApp Blue XP Connector versions prior to 3.9.25 expose information via a directory listing. A new Connector architecture resolves this issue - obtaining the fix requires redeploying a fresh Connector.	2023-05-26	5.3	Medium
CVE-2023-33288	linux - linux_kernel	An issue was discovered in the Linux kernel before 6.2.9. A use-after-free was found in bq24190_remove in drivers/power/supply/bq24190_charger.c. It could allow a local attacker to crash the system due to a race condition.	2023-05-22	4.7	Medium
CVE-2023-2898	linux - linux_kernel	There is a null-pointer-dereference flaw found in f2fs_write_end_io in fs/f2fs/data.c in the Linux kernel. This flaw allows a local privileged user to cause a denial of service problem.	2023-05-26	4.7	Medium
CVE-2023-33946	liferay - multiple products	The Object module in Liferay Portal 7.4.3.4 through 7.4.3.48, and Liferay DXP 7.4 before update 49 does properly isolate objects in difference virtual instances, which allows remote authenticated users in one virtual instance to view objects in a different virtual instance via OAuth 2 scope administration page.	2023-05-24	4.3	Medium
CVE-2023-33947	liferay - multiple products	The Object module in Liferay Portal 7.4.3.4 through 7.4.3.60, and Liferay DXP 7.4 before update 61 does not segment object definition by virtual instance in search which allows remote authenticated users in one virtual instance to view object definition from a second virtual instance by searching for the object definition.	2023-05-24	4.3	Medium
CVE-2023-31225	huawei - multiple products	The Gallery app has the risk of hijacking attacks. Successful exploitation of this vulnerability may cause download failures and affect product availability.	2023-05-26	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.