الهيئـــة الوطنيـــة
للأمـــن السيبـــراني
National 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.

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 3rd of August to 9th of August. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

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

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من ٣ أغسطس إلى ٩ أغسطس. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2025-54253	adobe - experience_manager_forms	Adobe Experience Manager versions 6.5.23 and earlier are affected by a Misconfiguration vulnerability that could result in arbitrary code execution. An attacker could leverage this vulnerability to bypass security mechanisms and execute code. Exploitation of this issue does not require user interaction and scope is changed.	2025-08-05	10
CVE-2013-10069	d-link - multiple products	The web interface of multiple D-Link routers, including DIR-600 rev B (≤2.14b01) and DIR-300 rev B (≤2.13), contains an unauthenticated OS command injection vulnerability in command.php, which improperly handles the cmd POST parameter. A remote attacker can exploit this flaw without authentication to spawn a Telnet service on a specified port, enabling persistent interactive shell access as root.	2025-08-05	10
CVE-2025-53767	microsoft - azure_openai	Azure OpenAI Elevation of Privilege Vulnerability	2025-08-07	10
CVE-2025-36594	dell - multiple products	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.3.0.15, LTS2024 release Versions 7.13.1.0 through 7.13.1.25, LTS 2023 release versions 7.10.1.0 through 7.10.1.60, contain an Authentication Bypass by Spoofing vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to Protection mechanism bypass. Remote unauthenticated user can create account that potentially expose customer info, affect system integrity and availability.	2025-08-04	9.8
CVE-2025-48913	apache - multiple products	If untrusted users are allowed to configure JMS for Apache CXF, previously they could use RMI or LDAP URLs, potentially leading to code execution capabilities. This interface is now restricted to reject those protocols, removing this possibility. Users are recommended to upgrade to versions 3.6.8, 4.0.9 or 4.1.3, which fix this issue.	2025-08-08	9.8
CVE-2025-53606	apache - seata	Deserialization of Untrusted Data vulnerability in Apache Seata (incubating). This issue affects Apache Seata (incubating): 2.4.0. Users are recommended to upgrade to version 2.5.0, which fixes the issue.	2025-08-08	9.8
CVE-2025-54948	trendmicro - apex_one	A vulnerability in Trend Micro Apex One (on-premise) management console could allow a pre-authenticated remote attacker to upload malicious code and execute commands on affected installations.	2025-08-05	9.4
CVE-2025-54987	trendmicro - apex_one	A vulnerability in Trend Micro Apex One (on-premise) management console could allow a pre-authenticated remote attacker to upload malicious code and execute commands on affected installations. This vulnerability is essentially the same as CVE-2025-54948 but targets a different CPU architecture.	2025-08-05	9.4
CVE-2025-53792	microsoft - azure_portal	Azure Portal Elevation of Privilege Vulnerability	2025-08-07	9.1
CVE-2025-8731	trendnet - multiple products	A vulnerability was identified in TRENDnet TI-G160i, TI-PG102i and TPL-430AP up to 20250724. This affects an unknown part of the component SSH Service. The manipulation leads to use of default credentials. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The vendor explains: "For product TI-PG102i and TI-G160i, by default, the product's remote management options are all disabled. The root account is for troubleshooting purpose and the password is encrypted. However, we will remove the root account from the next firmware release. For product	2025-08-08	8.9

		TPL-430AP, the initial setup process requires user to set the password for the management GUI. Once that was done, the default password will be invalid."		
CVE-2025-54627	huawei - HarmonyOS	Out-of-bounds write vulnerability in the skia module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-08-06	8.8
CVE-2025-8576	google - chrome	Use after free in Extensions in Google Chrome prior to 139.0.7258.66 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: Medium)	2025-08-07	8.8
CVE-2025-8578	google - chrome	Use after free in Cast in Google Chrome prior to 139.0.7258.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2025-08-07	8.8
CVE-2025-52914	mitel - multiple products	A vulnerability in the Suite Applications Services component of Mitel MiCollab 10.0 through SP1 FP1 (10.0.1.101) could allow an authenticated attacker to conduct a SQL Injection attack due to insufficient validation of user input. A successful exploit could allow an attacker to execute arbitrary SQL database commands.	2025-08-08	8.8
CVE-2025-54254	adobe - experience_manager_forms	Adobe Experience Manager versions 6.5.23 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files on the local file system. Exploitation of this issue does not require user interaction.	2025-08-05	8.6
CVE-2025-26476	dell - multiple products	Dell ECS versions prior to 3.8.1.5/ ObjectScale version 4.0.0.0, contain a Use of Hard-coded Cryptographic Key vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access.	2025-08-04	8.4
CVE-2025-54652	huawei - HarmonyOS	Path traversal vulnerability in the virtualization base module. Successful exploitation of this vulnerability may affect the confidentiality of the virtualization module.	2025-08-06	8.4
CVE-2025-54653	huawei - HarmonyOS	Path traversal vulnerability in the virtualization file module. Successful exploitation of this vulnerability may affect the confidentiality of the virtualization file module.	2025-08-06	8.4
CVE-2025-21120	dell - multiple products	Dell Avamar, versions prior to 19.12 with patch 338905, excluding version 19.10SP1 with patch 338904, contains a Trusting HTTP Permission Methods on the Server-Side vulnerability in Security. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Information exposure.	2025-08-04	8.3
CVE-2025-54622	huawei - HarmonyOS	Binding authentication bypass vulnerability in the devicemanager module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-08-06	8.3
CVE-2025-53787	microsoft - 365_copilot_chat	Microsoft 365 Copilot BizChat Information Disclosure Vulnerability	2025-08-07	8.2
CVE-2025-54655	huawei - HarmonyOS	Race condition vulnerability in the virtualization base module. Successful exploitation of this vulnerability may affect the confidentiality and integrity of the virtualization graphics module.	2025-08-06	8.1
CVE-2025-3320	ibm - multiple products	IBM Tivoli Monitoring 6.3.0.7 through 6.3.0.7 Service Pack 20 is vulnerable to a heap-based buffer overflow, caused by improper bounds checking. A remote attacker could overflow a buffer and execute arbitrary code on the system or cause the server to crash.	2025-08-06	8.1
CVE-2025-3354	ibm - multiple products	IBM Tivoli Monitoring 6.3.0.7 through 6.3.0.7 Service Pack 20 is vulnerable to a heap-based buffer overflow, caused by improper bounds checking. A remote attacker could overflow a buffer and execute arbitrary code on the system or cause the server to crash.	2025-08-06	8.1
CVE-2025-54634	huawei - multiple products	Vulnerability of improper processing of abnormal conditions in huge page separation. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	8
CVE-2025-53786	microsoft - multiple products	On April 18th 2025, Microsoft announced Exchange Server Security Changes for Hybrid Deployments and accompanying non-security Hot Fix. Microsoft made these changes in the general interest of improving the security of hybrid Exchange deployments. Following further investigation, Microsoft identified specific security implications tied to the guidance and configuration steps outlined in the April announcement. Microsoft is issuing CVE-2025-53786 to document a vulnerability that is addressed by taking the steps documented with the April 18th announcement. Microsoft strongly recommends reading the information, installing the April 2025 (or later) Hot Fix and implementing the changes in your Exchange Server and hybrid environment.	2025-08-06	8
CVE-2025-36606	dell - unity_operating_environment	Dell Unity, version(s) 5.5 and prior, contain(s) an OS Command Injection Vulnerability in its svc_nfssupport utility. An authenticated attacker could potentially exploit this vulnerability, escaping the restricted shell and execute arbitrary operating system commands with root privileges.	2025-08-04	7.8
CVE-2025-36607	dell - unity_operating_environment	Dell Unity, version(s) 5.5 and prior, contain(s) an OS Command Injection Vulnerability in its svc_nas utility. An authenticated attacker could potentially exploit this vulnerability, escaping the restricted shell and execute arbitrary operating system commands with root privileges.	2025-08-04	7.8
CVE-2025-30099	dell - multiple products	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.1.0.10, LTS2024 release Versions 7.13.1.0 through 7.13.1.25, LTS 2023 release versions 7.10.1.0 through 7.10.1.50, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the DDSH CLI. A low privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary commands with root privileges.	2025-08-04	7.8
CVE-2025-38747	dell - SupportAssist OS Recovery	Dell SupportAssist OS Recovery, versions prior to 5.5.14.0, contain a Creation of Temporary File With Insecure Permissions vulnerability. A local authenticated attacker could potentially exploit this vulnerability, leading to Elevation of Privileges.	2025-08-06	7.8
CVE-2025-54607	huawei - HarmonyOS	Authentication management vulnerability in the ArkWeb module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-08-06	7.7
CVE-2025-38741	dell - Enterprise SONiC OS	Dell Enterprise SONiC OS, version 4.5.0, contains a cryptographic key vulnerability in SSH. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to unauthorized access to communication.	2025-08-04	7.5
CVE-2025-36604	dell - unity_operating_environment	Dell Unity, version(s) 5.5 and prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution.	2025-08-04	7.3
CVE-2025-54606	huawei - HarmonyOS	Status verification vulnerability in the lock screen module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	2025-08-06	7.3
CVE-2025-54611	huawei - multiple products	EXTRA_REFERRER resource read vulnerability in the Gallery module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-08-06	7.3
CVE-2025-8757	trendnet - TV-IP110WN	A vulnerability was found in TRENDnet TV-IP110WN 1.2.2 and classified as problematic. Affected by this issue is some unknown functionality of the file /server/boa.conf of the component Embedded	2025-08-09	7.3

		Boa Web Server. The manipulation leads to least privilege violation. Local access is required to approach this attack. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.		
CVE-2025-8758	trendnet - TEW-822DRE	A vulnerability was found in TRENDnet TEW-822DRE FW103B02. It has been classified as problematic. This affects an unknown part of the component vsftpd. The manipulation leads to least privilege violation. Attacking locally is a requirement. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-08-09	7.3
CVE-2025-38739	dell - Dell Digital Delivery	Dell Digital Delivery, versions prior to 5.6.1.0, contains an Insufficiently Protected Credentials vulnerability. A remote unauthenticated attacker could potentially exploit this vulnerability, leading to Information Disclosure.	2025-08-04	7.2
CVE-2025-36119	ibm - multiple products	IBM i 7.3, 7.4, 7.5, and 7.6 is affected by an authenticated user obtaining elevated privileges with IBM Digital Certificate Manager for i (DCM) due to a web session hijacking vulnerability. An authenticated user without administrator privileges could exploit this vulnerability to perform actions in DCM as an administrator.	2025-08-08	7.1
CVE-2025-26513	netapp - SAN Host Utilities for Windows	The installer for SAN Host Utilities for Windows versions prior to 8.0 is susceptible to a vulnerability which when successfully exploited could allow a local user to escalate their privileges.	2025-08-07	7
CVE-2025-4604	liferay - multiple products	The vulnerable code can bypass the Captcha check in Liferay Portal 7.4.3.80 through 7.4.3.132, and Liferay DXP 2024.Q1.1 through 2024.Q1.19, 2024.Q2.0 through 2024.Q2.13, 2024.Q3.0 through 2024.Q3.13, 2024.Q4.0 through 2024.Q4.7, 2025.Q1.0 through 2025.Q1.15 and 7.4 update 80 through update 92 and then attackers can run scripts in the Gogo shell	2025-08-04	6.9
CVE-2025-4576	liferay - multiple products	A reflected cross-site scripting (XSS) vulnerability in the Liferay Portal 7.4.0 through 7.4.3.133, and Liferay DXP 2025.Q1.0 through 2025.Q1.4 ,2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.15, 7.4 GA through update 92 allows an remote non-authenticated attacker to inject JavaScript into the modules/apps/blogs/blogs-web/src/main/resources/META-INF/resources/blogs/entry_cover_image_caption.jsp	2025-08-08	6.9
CVE-2025-54617	huawei - HarmonyOS	Stack-based buffer overflow vulnerability in the dms_fwk module. Impact: Successful exploitation of this vulnerability can cause RCE.	2025-08-06	6.8
CVE-2025-54630	huawei - HarmonyOS	:Vulnerability of insufficient data length verification in the DFA module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	6.8
CVE-2025-54632	huawei - multiple products	Vulnerability of insufficient data length verification in the HVB module. Impact: Successful exploitation of this vulnerability may affect service integrity.	2025-08-06	6.8
CVE-2025-30096	dell - multiple products	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.1.0.10, LTS2024 release Versions 7.13.1.0 through 7.13.1.25, LTS 2023 release versions 7.10.1.0 through 7.10.1.50, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the DDSH CLI. A high privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary commands with root privileges.	2025-08-04	6.7
CVE-2025-30097	dell - multiple products	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.1.0.10, LTS2024 release Versions 7.13.1.0 through 7.13.1.25, LTS 2023 release versions 7.10.1.0 through 7.10.1.50, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the DDSH CLI. A high privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary commands with root privileges	2025-08-04	6.7
CVE-2025-30098	dell - multiple products	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.1.0.10, LTS2024 release Versions 7.13.1.0 through 7.13.1.25, LTS 2023 release versions 7.10.1.0 through 7.10.1.50, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in the DDSH CLI. A high privileged attacker with local access could potentially exploit this vulnerability to execute arbitrary commands with root privileges.	2025-08-04	6.7
CVE-2025-54625	huawei - HarmonyOS	Race condition vulnerability in the kernel file system module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	6.7
CVE-2025-54629	huawei - multiple products	Race condition issue occurring in the physical page import process of the memory management module. Impact: Successful exploitation of this vulnerability may affect service integrity.	2025-08-06	6.7
CVE-2025-54631	huawei - multiple products	Vulnerability of insufficient data length verification in the partition module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	6.7
CVE-2025-54633	huawei - multiple products	Out-of-bounds read vulnerability in the register configuration of the DMA module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-08-06	6.7
CVE-2025-54641	huawei - multiple products	Issue of buffer overflow caused by insufficient data verification in the kernel acceleration module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	6.7
CVE-2025-54642	huawei - multiple products	Issue of buffer overflow caused by insufficient data verification in the kernel gyroscope module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	6.7
CVE-2025-54643	huawei - multiple products	Out-of-bounds array access issue due to insufficient data verification in the kernel ambient light module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-08-06	6.6
CVE-2025-54644	huawei - multiple products	Out-of-bounds array access issue due to insufficient data verification in the kernel ambient light module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-08-06	6.6
CVE-2025-8419	redhat - keycloak	A vulnerability was found in Keycloak-services. Special characters used during e-mail registration may perform SMTP Injection and unexpectedly send short unwanted e-mails. The email is limited to 64 characters (limited local part of the email), so the attack is limited to very shorts emails (subject and little data, the example is 60 chars). This flaw's only direct consequence is an unsolicited email being sent from the Keycloak server. However, this action could be a precursor for more sophisticated attacks.	2025-08-06	6.5

CVE-2025-53774	microsoft - 365_copilot_chat	Microsoft 365 Copilot BizChat Information Disclosure Vulnerability	2025-08-07	6.5
CVE-2025-36023	ibm - multiple products	IBM Cloud Pak for Business Automation 24.0.0 through 24.0.0 IF005 and 24.0.1 through 24.0.1 IF002 could allow an authenticated user to view sensitive user and system information due to an indirect object reference through a user-controlled key.	2025-08-08	6.5
CVE-2025-54623	huawei - HarmonyOS	Out-of-bounds read vulnerability in the devicemanager module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	6.3
CVE-2025-21017	samsung - blockchain_keystore	Out-of-bounds write in detaching crypto box in Blockchain Keystore prior to version 1.3.17.2 allows local privileged attackers to write out-of-bounds memory.	2025-08-06	6.3
CVE-2025-8759	trendnet - TN-200	A vulnerability was found in TRENDnet TN-200 1.02b02. It has been declared as problematic. This vulnerability affects unknown code of the component Lighttpd. The manipulation of the argument secdownload.secret with the input neV3rUseMe leads to use of hard-coded cryptographic key_x000D_ . The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2025-08-09	6.3
CVE-2025-54608	huawei - HarmonyOS	Vulnerability that allows setting screen rotation direction without permission verification in the screen management module. Impact: Successful exploitation of this vulnerability may cause device screen orientation to be arbitrarily set.	2025-08-06	6.2
CVE-2025-54614	huawei - multiple products	Input verification vulnerability in the home screen module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	6.2
CVE-2025-54615	huawei - multiple products	Vulnerability of insufficient information protection in the media library module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-08-06	6.2
CVE-2024-41177	apache - zeppelin	Incomplete Blacklist to Cross-Site Scripting vulnerability in Apache Zeppelin. This issue affects Apache Zeppelin: before 0.12.0. Users are recommended to upgrade to version 0.12.0, which fixes the issue.	2025-08-03	6.1
CVE-2025-36605	dell - unity_operating_environment	Dell Unity, version(s) 5.5 and prior, contain(s) an Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in the CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'). An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to the execution of malicious HTML or JavaScript code in a victim user's web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery.	2025-08-04	6.1
CVE-2024-52890	ibm - multiple products	IBM Engineering Lifecycle Optimization - Publishing 7.0.2 and 7.03 could be susceptible to cross-site scripting due to no validation of URIs.	2025-08-05	6.1
CVE-2025-21010	samsung - multiple products	Improper privilege management in SamsungAccount prior to SMR Aug-2025 Release 1 allows local privileged attackers to deactivate Samsung account.	2025-08-06	6
CVE-2025-54612	huawei - HarmonyOS	Iterator failure vulnerability in the card management module. Impact: Successful exploitation of this vulnerability may affect function stability.	2025-08-06	5.9
CVE-2025-54613	huawei - HarmonyOS	Iterator failure vulnerability in the card management module. Impact: Successful exploitation of this vulnerability may affect function stability.	2025-08-06	5.9
CVE-2025-54635	huawei - harmonyos	Vulnerability of returning released pointers in the distributed notification service. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	5.9
CVE-2025-36020	ibm - guardium_data_protection	IBM Guardium Data Protection could allow a remote attacker to obtain sensitive information due to cleartext transmission of sensitive credential information.	2025-08-06	5.9
CVE-2025-54618	huawei - HarmonyOS	Permission control vulnerability in the distributed clipboard module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-08-06	5.7
CVE-2025-54624	huawei - HarmonyOS	Unexpected injection event vulnerability in the multimodalinput module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	5.7
CVE-2025-21020	samsung - blockchain_keystore	Out-of-bounds write in creating bitmap images in Blockchain Keystore prior to version 1.3.17.2 allows local privileged attackers to write out-of-bounds memory.	2025-08-06	5.7
CVE-2025-21021	samsung - blockchain_keystore	Out-of-bounds write in drawing pinpad in Blockchain Keystore prior to version 1.3.17.2 allows local privileged attackers to write out-of-bounds memory.	2025-08-06	5.7
CVE-2024-58257	huawei - EnzoH-W5611T	EnzoH has an OS command injection vulnerability. Successful exploitation of this vulnerability may lead to arbitrary command execution.	2025-08-08	5.7
CVE-2025-54620	huawei - HarmonyOS	Deserialization vulnerability of untrusted data in the ability module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	5.5
CVE-2025-54638	huawei - multiple products	Issue of inconsistent read/write serialization in the ad module. Impact: Successful exploitation of this vulnerability may affect the availability of the ad service.	2025-08-06	5.5
CVE-2025-54639	huawei - HarmonyOS	ParcelMismatch vulnerability in attribute deserialization. Impact: Successful exploitation of this vulnerability may cause playback control screen display exceptions.	2025-08-06	5.5
CVE-2025-54640	huawei - HarmonyOS	ParcelMismatch vulnerability in attribute deserialization. Impact: Successful exploitation of this vulnerability may cause playback control screen display exceptions.	2025-08-06	5.5
CVE-2025-21019	samsung - health	Improper authorization in Samsung Health prior to version 6.30.1.003 allows local attackers to access data in Samsung Health. User interaction is required for triggering this vulnerability.	2025-08-06	5.5
CVE-2025-46958	adobe - multiple products	Adobe Experience Manager versions 6.5.22 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	2025-08-05	5.4
CVE-2025-54609	huawei - multiple products	Out-of-bounds access vulnerability in the audio codec module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	5.4

CVE-2025-54610	huawei - multiple products	Out-of-bounds access vulnerability in the audio codec module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	5.4
CVE-2025-54647	huawei - harmonyos	Out-of-bounds read vulnerability in the SSAP module of the NearLink protocol stack. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	5.4
CVE-2025-54648	huawei - harmonyos	Out-of-bounds read vulnerability in the SSAP module of the NearLink protocol stack. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	5.4
CVE-2025-20215	cisco - Cisco Webex Meetings	A vulnerability in the meeting-join functionality of Cisco Webex Meetings could have allowed an unauthenticated, network-proximate attacker to complete a meeting-join process in place of an intended targeted user, provided the requisite conditions were satisfied. Cisco has addressed this vulnerability in the Cisco Webex Meetings service, and no customer action is needed._x000D_ _x000D_ This vulnerability existed due to client certificate validation issues. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by monitoring local wireless or adjacent networks for client-join requests and attempting to interrupt and complete the meeting-join flow as another user who was currently joining a meeting. To successfully exploit the vulnerability, an attacker would need the capability to position themselves in a local wireless or adjacent network, to monitor and intercept the targeted network traffic flows, and to satisfy timing requirements in order to interrupt the meeting-join flow and exploit the vulnerability. A successful exploit could have allowed the attacker to join the meeting as another user. However, the Cisco Product Security Incident Response Team (PSIRT) is not aware of any malicious use of the vulnerability that is described in this advisory.	2025-08-06	5.4
CVE-2025-20331	cisco - multiple products	A vulnerability in the web-based management interface of Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to conduct a stored XSS attack against a user of the interface._x000D_ _x000D_ This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface of an affected system. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information. To exploit this vulnerability, the attacker must have at least a low-privileged account on the affected device.	2025-08-06	5.4
CVE-2024-52279	apache - zeppelin	Improper Input Validation vulnerability in Apache Zeppelin. The fix for JDBC URL validation in CVE-2024-31864 did not account for URL encoded input. This issue affects Apache Zeppelin: from 0.11.1 before 0.12.0. Users are recommended to upgrade to version 0.12.0, which fixes the issue.	2025-08-03	5.3
CVE-2024-51775	apache - zeppelin	Missing Origin Validation in WebSockets vulnerability in Apache Zeppelin. The attacker could access the Zeppelin server from another origin without any restriction, and get internal information about paragraphs. This issue affects Apache Zeppelin: from 0.11.1 before 0.12.0. Users are recommended to upgrade to version 0.12.0, which fixes the issue.	2025-08-03	5.3
CVE-2025-5988	red hat - multiple products	A flaw was found in the Ansible aap-gateway. Cross-site request forgery (CSRF) origin checking is not done on requests from the gateway to external components, such as the controller, hub, and eda.	2025-08-04	5.3
CVE-2025-54619	huawei - HarmonyOS	Iterator failure issue in the multi-mode input module. Impact: Successful exploitation of this vulnerability may cause iterator failures and affect availability.	2025-08-06	5.3
CVE-2025-54621	huawei - HarmonyOS	Iterator failure issue in the WantAgent module. Impact: Successful exploitation of this vulnerability may cause memory release failures.	2025-08-06	5.3
CVE-2025-54628	huawei - multiple products	Vulnerability of incomplete verification information in the communication module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	5.3
CVE-2025-4581	liferay - multiple products	Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.4 ,2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.15, 7.4 GA through update 92 allows a pre-authentication blind SSRF vulnerability in the portal-settings-authentication-opensso-web due to improper validation of user-supplied URLs. An attacker can exploit this issue to force the server to make arbitrary HTTP requests to internal systems, potentially leading to internal network enumeration or further exploitation.	2025-08-09	5.3
CVE-2025-7195	red hat - multiple products	Early versions of Operator-SDK provided an insecure method to allow operator containers to run in environments that used a random UID. Operator-SDK before 0.15.2 provided a script, user_setup, which modifies the permissions of the /etc/passwd file to 664 during build time. Developers who used Operator-SDK before 0.15.2 to scaffold their operator may still be impacted by this if the insecure user_setup script is still being used to build new container images. In affected images, the /etc/passwd file is created during build time with group-writable permissions and a group ownership of root (gid=0). An attacker who can execute commands within an affected container, even as a non-root user, may be able to leverage their membership in the root group to modify the /etc/passwd file. This could allow the attacker to add a new user with any arbitrary UID, including UID 0, leading to full root privileges within the container.	2025-08-07	5.2
CVE-2025-54646	huawei - multiple products	Vulnerability of inadequate packet length check in the BLE module. Impact: Successful exploitation of this vulnerability may affect performance.	2025-08-06	5.1
CVE-2025-8341	grafana - grafana-infinity-datasource	Grafana is an open-source platform for monitoring and observability. The Infinity datasource plugin, maintained by Grafana Labs, allows visualizing data from JSON, CSV, XML, GraphQL, and HTML endpoints.	2025-08-04	5

		If the plugin was configured to allow only certain URLs, an attacker could bypass this restriction using a specially crafted URL. This vulnerability is fixed in version 3.4.1.		
CVE-2025-54645	huawei - multiple products	Out-of-bounds array access issue due to insufficient data verification in the location service module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	5
CVE-2024-58255	huawei - EnzoH-W5611T	EnzoH has an OS command injection vulnerability. Successful exploitation of this vulnerability may lead to arbitrary command execution.	2025-08-08	5
CVE-2025-54651	huawei - multiple products	Race condition vulnerability in the kernel hufs module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-08-06	4.8
CVE-2025-8733	gnu - Bison	A vulnerability was found in GNU Bison up to 3.8.2. It has been rated as problematic. This issue affects the function __obstack_vprintf_internal of the file obprintf.c. The manipulation leads to reachable assertion. It is possible to launch the attack on the local host. The exploit has been disclosed to the public and may be used.	2025-08-08	4.8
CVE-2025-8734	gnu - Bison	A vulnerability classified as problematic has been found in GNU Bison up to 3.8.2. Affected is the function code_free of the file src/scan-code.c. The manipulation leads to double free. The attack needs to be approached locally. The exploit has been disclosed to the public and may be used.	2025-08-08	4.8
CVE-2025-8735	gnu - cflow	A vulnerability classified as problematic was found in GNU cflow up to 1.8. Affected by this vulnerability is the function yylex of the file c.c of the component Lexer. The manipulation leads to null pointer dereference. An attack has to be approached locally. The exploit has been disclosed to the public and may be used.	2025-08-08	4.8
CVE-2025-8736	gnu - cflow	A vulnerability, which was classified as critical, has been found in GNU cflow up to 1.8. Affected by this issue is the function yylex of the file c.c of the component Lexer. The manipulation leads to buffer overflow. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used.	2025-08-08	4.8
CVE-2025-8746	gnu - libopts	A vulnerability, which was classified as problematic, was found in GNU libopts up to 27.6. Affected is the function __strstr_sse2. The manipulation leads to memory corruption. Local access is required to approach this attack. The exploit has been disclosed to the public and may be used. This issue was initially reported to the tcpreplay project, but the code maintainer explains, that this "bug appears to be in libopts which is an external library." This vulnerability only affects products that are no longer supported by the maintainer.	2025-08-09	4.8
CVE-2025-54649	huawei - multiple products	Vulnerability of using incompatible types to access resources in the location service. Impact: Successful exploitation of this vulnerability may cause some location information attributes to be incorrect.	2025-08-06	4.5
CVE-2024-58256	huawei - EnzoH-W5611T	EnzoH has an OS command injection vulnerability. Successful exploitation of this vulnerability may lead to arbitrary command execution.	2025-08-08	4.5
CVE-2025-54626	huawei - HarmonyOS	Pointer dangling vulnerability in the cjwindow module. Impact: Successful exploitation of this vulnerability may affect function stability.	2025-08-06	4.4
CVE-2025-54636	huawei - multiple products	Issue of buffer overflow caused by insufficient data verification in the kernel drop detection module. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	4.4
CVE-2025-54637	huawei - multiple products	Out-of-bounds array access issue due to insufficient data verification in the kernel ambient light module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2025-08-06	4.4
CVE-2025-21018	samsung - blockchain_keystore	Out-of-bounds read in Blockchain Keystore prior to version 1.3.17.2 allows local privileged attackers to read out-of-bounds memory.	2025-08-06	4.4
CVE-2025-20332	cisco - Cisco Identity Services Engine Software	A vulnerability in the web-based management interface of Cisco ISE could allow an authenticated, remote attacker to modify parts of the configuration on an affected device._x000D_ _x000D_ This vulnerability is due to the lack of server-side validation of Administrator permissions. An attacker could exploit this vulnerability by submitting a crafted HTTP request to an affected system. A successful exploit could allow the attacker to modify descriptions of files on a specific page. To exploit this vulnerability, an attacker would need valid read-only Administrator&nbsp;credentials.	2025-08-06	4.3
CVE-2025-8577	google - chrome	Inappropriate implementation in Picture In Picture in Google Chrome prior to 139.0.7258.66 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2025-08-07	4.3
CVE-2025-8579	google - chrome	Inappropriate implementation in Picture In Picture in Google Chrome prior to 139.0.7258.66 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2025-08-07	4.3
CVE-2025-8580	google - chrome	Inappropriate implementation in Filesystems in Google Chrome prior to 139.0.7258.66 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2025-08-07	4.3
CVE-2025-8581	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 139.0.7258.66 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2025-08-07	4.3
CVE-2025-8582	google - chrome	Insufficient validation of untrusted input in Core in Google Chrome prior to 139.0.7258.66 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Low)	2025-08-07	4.3
CVE-2025-8583	google - chrome	Inappropriate implementation in Permissions in Google Chrome prior to 139.0.7258.66 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2025-08-07	4.3
CVE-2025-54650	huawei - HarmonyOS	Improper array index verification vulnerability in the audio codec module. Impact: Successful exploitation of this vulnerability may affect the audio decoding function.	2025-08-06	4.2
CVE-2025-54616	huawei - harmonyos	Out-of-bounds array access vulnerability in the ArkUI framework. Impact: Successful exploitation of this vulnerability may affect availability.	2025-08-06	4
CVE-2025-20990	samsung - multiple products	Improper access control in accessing system device node prior to SMR Aug-2025 Release 1 allows local attackers to access device identifier.	2025-08-06	4
CVE-2025-8556	red hat - multiple products	A flaw was found in CIRCL's implementation of the FourQ elliptic curve. This vulnerability allows an attacker to compromise session security via low-order point injection and incorrect point validation during Diffie-Hellman key exchange.	2025-08-06	3.7

CVE-2024-56339	ibm - multiple products	IBM WebSphere Application Server 9.0 and WebSphere Application Server Liberty 17.0.0.3 through 25.0.0.7 could allow a remote attacker to bypass security restrictions caused by a failure to honor security configuration.	2025-08-07	3.7
CVE-2025-38746	dell - SupportAssist OS Recovery	Dell SupportAssist OS Recovery, versions prior to 5.5.14.0, contains an Exposure of Sensitive Information to an Unauthorized Actor vulnerability. An unauthenticated attacker with physical access could potentially exploit this vulnerability, leading to Information Disclosure.	2025-08-06	3.5
CVE-2025-4599	liferay - multiple products	The fragment preview functionality in Liferay Portal 7.4.3.61 through 7.4.3.132, and Liferay DXP 2024.Q4.1 through 2024.Q4.5, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.13 and 7.4 update 61 through update 92 was found to be vulnerable to postMessage-based XSS because it allows a remote non-authenticated attacker to inject JavaScript into the fragment portlet URL.	2025-08-04	2
CVE-2025-4655	liferay - multiple products	SSRF vulnerability in FreeMarker templates in Liferay Portal 7.4.0 through 7.4.3.132, and Liferay DXP 2025.Q1.0 through 2025.Q1.5, 2024.Q4.0 through 2024.Q4.7, 2024.Q3.1 through 2024.Q3.13, 2024.Q2.0 through 2024.Q2.13, 2024.Q1.1 through 2024.Q1.15, 7.4 GA through update 92 allows template editors to bypass access validations via crafted URLs.	2025-08-09	2

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.