الهيئة الوطنية
للأمن السيبراني
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 4th of January to 10th of January. 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 National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 4 يناير إلى 10 يناير. 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-2025-69258	trendmicro - multiple products	A LoadLibraryEX vulnerability in Trend Micro Apex Central could allow an unauthenticated remote attacker to load an attacker-controlled DLL into a key executable, leading to execution of attacker-supplied code under the context of SYSTEM on affected installations.	2026-01-08	9.8
CVE-2025-12543	red hat - multiple products	A flaw was found in the Undertow HTTP server core, which is used in WildFly, JBoss EAP, and other Java applications. The Undertow library fails to properly validate the Host header in incoming HTTP requests.As a result, requests containing malformed or malicious Host headers are processed without rejection, enabling attackers to poison caches, perform internal network scans, or hijack user sessions.	2026-01-07	9.6
CVE-2026-0625	d-link - multiple products	Multiple D-Link DSL/DIR/DNS devices contain an authentication bypass and improper access control vulnerability in the dnscfg.cgi endpoint that allows an unauthenticated attacker to access DNS configuration functionality. By directly requesting this endpoint, an attacker can modify the device's DNS settings without valid credentials, enabling DNS hijacking ("DNSChanger") attacks that redirect user traffic to attacker-controlled infrastructure. In 2019, D-Link reported that this behavior was leveraged by the "GhostDNS" malware ecosystem targeting consumer and carrier routers. All impacted products were subsequently designated end-of-life/end-of-service, and no longer receive security updates. Exploitation evidence was observed by the Shadowserver Foundation on 2025-11-27 (UTC).	2026-01-05	9.3
CVE-2025-27807	samsung - exynos_990_firmware	An issue was discovered in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2100, 1280, 2200, 1330, 1380, 1480, 2400, 1580, 9110, W920, W930, W1000, Modem 5123, Modem 5300, Modem 5400. The lack of a length check leads to out-of-bounds writes via malformed NAS packets.	2026-01-05	9.1
CVE-2025-68637	apache - uniffle	The Uniffle HTTP client is configured to trust all SSL certificates and disables hostname verification by default. This insecure configuration exposes all REST API communication between the Uniffle CLI/client and the Uniffle Coordinator service to potential Man-in-the-Middle (MITM) attacks. This issue affects all versions from before 0.10.0. Users are recommended to upgrade to version 0.10.0, which fixes the issue.	2026-01-07	9.1
CVE-2025-59468	veeam - veeam_backup_\&_replication	This vulnerability allows a Backup Administrator to perform remote code execution (RCE) as the postgres user by sending a_x000D_ malicious password parameter.	2026-01-08	9
CVE-2025-59469	veeam - veeam_backup_\&_replication	This vulnerability allows a Backup or Tape Operator to write files as root.	2026-01-08	9
CVE-2025-59470	veeam - veeam_backup_\&_replication	This vulnerability allows a Backup Operator to perform remote code execution (RCE) as the postgres user by sending a malicious interval or order parameter.	2026-01-08	9
CVE-2025-15471	trendnet - TEW-713RE	A vulnerability was detected in TRENDnet TEW-713RE 1.02. The impacted element is an unknown function of the file /goformX/formFSrvX. The manipulation of the argument SZCMD results in os command injection. It is possible to launch the attack remotely. The exploit is now public and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-01-07	8.9

CVE-2025-66518	apache software foundation - Apache Kyuubi	Any client who can access to Apache Kyuubi Server via Kyuubi frontend protocols can bypass server-side config kyuubi.session.local.dir.allow.list and use local files which are not listed in the config. This issue affects Apache Kyuubi: from 1.6.0 through 1.10.2. Users are recommended to upgrade to version 1.10.3 or upper, which fixes the issue.	2026-01-05	8.8
CVE-2026-0628	google - chrome	Insufficient policy enforcement in WebView tag in Google Chrome prior to 143.0.7499.192 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: High)	2026-01-07	8.8
CVE-2026-0719	red hat - multiple products	A flaw was identified in the NTLM authentication handling of the libsoup HTTP library, used by GNOME and other applications for network communication. When processing extremely long passwords, an internal size calculation can overflow due to improper use of signed integers. This results in incorrect memory allocation on the stack, followed by unsafe memory copying. As a result, applications using libsoup may crash unexpectedly, creating a denial-of-service risk.	2026-01-08	8.6
CVE-2025-14025	red hat - multiple products	A flaw was found in Ansible Automation Platform (AAP). Read-only scoped OAuth2 API Tokens in AAP, are enforced at the Gateway level for Gateway-specific operations. However, this vulnerability allows read-only tokens to perform write operations on backend services (e.g., Controller, Hub, EDA). If this flaw were exploited, an attacker‘s capabilities would only be limited by role based access controls (RBAC).	2026-01-08	8.5
CVE-2025-49495	samsung - exynos_1380_firmware	An issue was discovered in the WiFi driver in Samsung Mobile Processor Exynos 1380, 1480, 2400, 1580. Mishandling of an NL80211 vendor command leads to a buffer overflow.	2026-01-05	8.4
CVE-2025-53966	samsung - exynos_1380_firmware	An issue was discovered in Samsung Mobile Processor Exynos 1380, 1480, 2400, and 1580. Incorrect Handling of the NL80211 vendor command leads to a buffer overflow during handling of an IOCTL message.	2026-01-05	8.4
CVE-2025-62235	apache - nimble	Authentication Bypass by Spoofing vulnerability in Apache NimBLE. Receiving specially crafted Security Request could lead to removal of original bond and re-bond with impostor. This issue affects Apache NimBLE: through 1.8.0. Users are recommended to upgrade to version 1.9.0, which fixes the issue.	2026-01-10	8.1
CVE-2025-20778	google - multiple products	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10184870; Issue ID: MSV-4729.	2026-01-06	7.8
CVE-2025-20780	google - multiple products	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10184061; Issue ID: MSV-4712.	2026-01-06	7.8
CVE-2025-20781	google - multiple products	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10182914; Issue ID: MSV-4699.	2026-01-06	7.8
CVE-2025-20795	google - multiple products	In KeyInstall, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10276761; Issue ID: MSV-5141.	2026-01-06	7.8
CVE-2025-20796	google - android	In imgsys, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS10314745; Issue ID: MSV-5553.	2026-01-06	7.8
CVE-2025-20797	google - multiple products	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10315812; Issue ID: MSV-5534.	2026-01-06	7.8
CVE-2025-20798	google - multiple products	In battery, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10315812; Issue ID: MSV-5533.	2026-01-06	7.8
CVE-2025-20799	google - multiple products	In c2ps, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10274607; Issue ID: MSV-5049.	2026-01-06	7.8
CVE-2025-20800	google - multiple products	In mminfra, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10267349; Issue ID: MSV-5033.	2026-01-06	7.8
CVE-2025-47343	qualcomm - video_collaboration_vc3_platform_firmware	Memory corruption while processing a video session to set video parameters.	2026-01-07	7.8
CVE-2025-55125	veeam - veeam_backup_\&_replication	This vulnerability allows a Backup or Tape Operator to perform remote code execution (RCE) as root by creating a malicious_x000D_ backup configuration file.	2026-01-08	7.8
CVE-2025-36589	dell - Unisphere for PowerMax	Dell Unisphere for PowerMax, version(s) 9.2.4.x, contain(s) an Improper Restriction of XML External Entity Reference vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access to data and resources outside of the intended sphere of control.	2026-01-06	7.6
CVE-2025-43706	samsung - exynos_1080_firmware	An issue was discovered in L2 in Samsung Mobile Processor, Wearable Processor, and Modem Exynos 980, 990, 850, 1080, 2400, 1580, 9110, W920, W930, Modem 5123, and Modem 5400. Incorrect handling of RRC packets leads to a Denial of Service.	2026-01-05	7.5
CVE-2025-69259	trendmicro - multiple products	A message unchecked NULL return value vulnerability in Trend Micro Apex Central could allow a remote attacker to create a denial-of-service condition on affected installations._x000D_ _x000D_ Please note: authentication is not required in order to exploit this vulnerability..	2026-01-08	7.5
CVE-2025-69260	trendmicro - multiple products	A message out-of-bounds read vulnerability in Trend Micro Apex Central could allow a remote attacker to create a denial-of-service condition on affected installations._x000D_	2026-01-08	7.5

		_x000D_ Please note: authentication is not required in order to exploit this vulnerability.		
CVE-2025-52435	apache - nimble	J2EE Misconfiguration: Data Transmission Without Encryption vulnerability in Apache NimBLE. Improper handling of Pause Encryption procedure on Link Layer results in a previously encrypted connection being left in un-encrypted state allowing an eavesdropper to observe the remainder of the exchange. This issue affects Apache NimBLE: through <= 1.8.0. Users are recommended to upgrade to version 1.9.0, which fixes the issue.	2026-01-10	7.5
CVE-2025-53477	apache - nimble	NULL Pointer Dereference vulnerability in Apache Nimble. Missing validation of HCI connection complete or HCI command TX buffer could lead to NULL pointer dereference. This issue requires disabled asserts and broken or bogus Bluetooth controller and thus severity is considered low. This issue affects Apache NimBLE: through 1.8.0. Users are recommended to upgrade to version 1.9.0, which fixes the issue.	2026-01-10	7.5
CVE-2025-15472	trendnet - tew-811dru_firmware	A flaw has been found in TRENDnet TEW-811DRU 1.0.2.0. This affects the function setDeviceURL of the file uapply.cgi of the component httpd . This manipulation of the argument DeviceURL causes os command injection. The attack can be initiated remotely. The exploit has been published and may be used. The vendor was contacted early about this disclosure but did not respond in any way.	2026-01-07	7.3
CVE-2026-20971	samsung - multiple products	Use After Free in PROCA driver prior to SMR Jan-2026 Release 1 allows local attackers to potentially execute arbitrary code.	2026-01-09	7.3
CVE-2025-66376	zimbra - Collaboration	Zimbra Collaboration (ZCS) 10 before 10.0.18 and 10.1 before 10.1.13 allows Classic UI stored XSS via Cascading Style Sheets (CSS) @import directives in an HTML e-mail message.	2026-01-05	7.2
CVE-2025-9611	microsoft - Playwright	Microsoft Playwright MCP Server versions prior to 0.0.40 fails to validate the Origin header on incoming connections. This allows an attacker to perform a DNS rebinding attack via a victim's web browser and send unauthorized requests to a locally running MCP server, resulting in unintended invocation of MCP tool endpoints.	2026-01-07	7.2
CVE-2025-20779	google - multiple products	In display, there is a possible use after free due to a race condition. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10184084; Issue ID: MSV-4720.	2026-01-06	7
CVE-2025-20801	google - multiple products	In seninf, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10251210; Issue ID: MSV-4926.	2026-01-06	7
CVE-2026-20970	samsung - multiple products	Improper access control in SLocation prior to SMR Jan-2026 Release 1 allows local attackers to execute the privileged APIs.	2026-01-09	6.8
CVE-2025-20782	google - multiple products	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10182882; Issue ID: MSV-4685.	2026-01-06	6.7
CVE-2025-20783	google - multiple products	In display, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10182882; Issue ID: MSV-4684.	2026-01-06	6.7
CVE-2025-20784	google - multiple products	In display, there is a possible memory corruption due to uninitialized data. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10182882; Issue ID: MSV-4683.	2026-01-06	6.7
CVE-2025-20785	google - multiple products	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10149882; Issue ID: MSV-4677.	2026-01-06	6.7
CVE-2025-20786	google - multiple products	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10149882; Issue ID: MSV-4673.	2026-01-06	6.7
CVE-2025-20787	google - multiple products	In display, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10149879; Issue ID: MSV-4658.	2026-01-06	6.7
CVE-2025-20802	google - android	In geniezone, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10238968; Issue ID: MSV-4914.	2026-01-06	6.7
CVE-2025-20803	google - android	In dpe, there is a possible memory corruption due to an integer overflow. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS10199779; Issue ID: MSV-4504.	2026-01-06	6.7
CVE-2025-20804	google - android	In dpe, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is needed for exploitation. Patch ID: ALPS10198951; Issue ID: MSV-4503.	2026-01-06	6.7
CVE-2025-20805	google - android	In dpe, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10114696; Issue ID: MSV-4480.	2026-01-06	6.7
CVE-2025-20806	google - android	In dpe, there is a possible memory corruption due to use after free. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10114835; Issue ID: MSV-4479.	2026-01-06	6.7
CVE-2025-20807	google - android	In dpe, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10114841; Issue ID: MSV-4451.	2026-01-06	6.7
CVE-2026-20968	samsung - multiple products	Use after free in DualDAR prior to SMR Jan-2026 Release 1 allows local privileged attackers to execute arbitrary code.	2026-01-09	6.7

CVE-2025-68280	apache software foundation - Apache SIS	Improper Restriction of XML External Entity Reference vulnerability in Apache SIS. It is possible to write XML files in such a way that, when parsed by Apache SIS, an XML file reveals to the attacker the content of a local file on the server running Apache SIS. This vulnerability impacts the following SIS services: * Reading of GeoTIFF files having the GEO_METADATA tag defined by the Defense Geospatial Information Working Group (DGIWG). * Parsing of ISO 19115 metadata in XML format. * Parsing of Coordinate Reference Systems defined in the GML format. * Parsing of files in GPS Exchange Format (GPX). This issue affects Apache SIS from versions 0.4 through 1.5 inclusive. Users are recommended to upgrade to version 1.6, which will fix the issue. In the meantime, the security vulnerability can be avoided by launching Java with the javax.xml.accessExternalDTD system property sets to a comma-separated list of authorized protocols. For example: java -Djavax.xml.accessExternalDTD="" ...	2026-01-05	6.5
CVE-2025-46645	dell - multiple products	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.4.0.0, LTS2025 release version 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.40, LTS 2023 release versions 7.10.1.0 through 7.10.1.70, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Command execution.	2026-01-09	6.5
CVE-2025-46298	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in tvOS 26.2, Safari 26.2, watchOS 26.2, visionOS 26.2, iOS 26.2 and iPadOS 26.2, macOS Tahoe 26.2. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-01-09	6.5
CVE-2025-46696	dell - multiple products	Dell Secure Connect Gateway (SCG) 5.0 Appliance and Application, version(s) versions 5.26 to 5.30, contain(s) an Execution with Unnecessary Privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-01-06	6.4
CVE-2025-52516	samsung - exynos_1330_firmware	An issue was discovered in the Camera in Samsung Mobile Processor and Wearable Processor Exynos 1330, 1380, 1480, 2400, 1580, 2500. An invalid kernel address dereference in the issimian device driver leads to a denial of service.	2026-01-05	6.2
CVE-2025-46644	dell - multiple products	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.4.0.0, LTS2025 release version 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.40, LTS2023 release versions 7.10.1.0 through 7.10.1.70, contain an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Command execution.	2026-01-09	6
CVE-2025-52517	samsung - exynos_2500_firmware	An issue was discovered in the Camera in Samsung Mobile Processor and Wearable Processor Exynos 1330, 1380, 1480, 2400, 1580, 2500. A race condition in the issimian device driver results in a double free, leading to a denial of service.	2026-01-05	5.9
CVE-2026-20026	cisco - multiple products	Multiple&nbsp;Cisco products are affected by a vulnerability in the processing of DCE/RPC requests that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to leak sensitive information or to restart, resulting in an interruption of packet inspection._x000D_ _x000D_ This vulnerability is due to an error in buffer handling logic when processing DCE/RPC requests, which can result in a buffer use-after-free read. An attacker could exploit this vulnerability by sending a large number of DCE/RPC requests through an established connection that is inspected by Snort 3. A successful exploit could allow the attacker to unexpectedly restart the Snort 3 Detection Engine, which could cause a denial of service (DoS).	2026-01-07	5.8
CVE-2025-62224	microsoft - Microsoft Edge for Android	User interface (ui) misrepresentation of critical information in Microsoft Edge for Android allows an authorized attacker to perform spoofing over a network.	2026-01-07	5.5
CVE-2025-46297	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26.2. An app may be able to access protected files within an App Sandbox container.	2026-01-09	5.5
CVE-2025-14596	intel - quartus_prime	Uncontrolled Search Path Element vulnerability in Altera Quartus Prime Pro Installer (SFX) on Windows allows Search Order Hijacking.This issue affects Quartus Prime Pro: from 24.1 through 24.3.1.	2026-01-07	5.4
CVE-2025-14599	intel - multiple products	Uncontrolled Search Path Element vulnerability in Altera Quartus Prime Standard Installer (SFX)	2026-01-07	5.4

		on Windows, Altera Quartus Prime Lite Installer (SFX) on Windows allows Search Order Hijacking.This issue affects Quartus Prime Standard: from 23.1 through 24.1; Quartus Prime Lite: from 23.1 through 24.1.		
CVE-2025-14605	intel - quartus_prime	Uncontrolled Search Path Element vulnerability in Altera Quartus Prime Pro on Windows (System Console modules) allows Search Order Hijacking.This issue affects Quartus Prime Pro: from 17.0 through 25.1.1.	2026-01-07	5.4
CVE-2025-14612	intel - quartus_prime	Insecure Temporary File vulnerability in Altera Quartus Prime Pro Installer (SFX) on Windows allows : Use of Predictable File Names.This issue affects Quartus Prime Pro: from 24.1 through 25.1.1.	2026-01-07	5.4
CVE-2025-14614	intel - multiple products	Insecure Temporary File vulnerability in Altera Quartus Prime Standard Installer (SFX) on Windows, Altera Quartus Prime Lite Installer (SFX) on Windows allows Explore for Predictable Temporary File Names.This issue affects Quartus Prime Standard: from 23.1 through 24.1; Quartus Prime Lite: from 23.1 through 24.1.	2026-01-07	5.4
CVE-2025-14625	intel - multiple products	Uncontrolled Search Path Element vulnerability in Altera Quartus Prime Standard on Windows (Nios II Command Shell modules), Altera Quartus Prime Lite on Windows (Nios II Command Shell modules) allows Search Order Hijacking.This issue affects Quartus Prime Standard: from 19.1 through 24.1; Quartus Prime Lite: from 19.1 through 24.1.	2026-01-07	5.4
CVE-2026-20027	cisco - multiple products	Multiple Cisco products are affected by a vulnerability in the processing of DCE/RPC requests that could allow an unauthenticated, remote attacker to cause the Snort 3 Detection Engine to leak sensitive information or to restart, resulting in an interruption of packet inspection._x000D_ _x000D_ This vulnerability is due to an error in buffer handling logic when processing DCE/RPC requests, which can result in a buffer out-of-bounds read. An attacker could exploit this vulnerability by sending a large number of DCE/RPC requests through an established connection that is inspected by Snort 3. A successful exploit could allow the attacker to obtain sensitive information in the Snort 3 data stream.	2026-01-07	5.3
CVE-2026-0707	red hat - Red Hat Build of Keycloak	A flaw was found in Keycloak. The Keycloak Authorization header parser is overly permissive regarding the formatting of the "Bearer" authentication scheme. It accepts non-standard characters (such as tabs) as separators and tolerates case variations that deviate from RFC 6750 specifications.	2026-01-08	5.3
CVE-2025-52515	samsung - exynos_1330_firmware	An issue was discovered in the Camera in Samsung Mobile Processor and Wearable Processor Exynos 1330, 1380, 1480, 2400, 1580, 2500. A race condition in the issimian device driver results in an out-of-bounds access, leading to a denial of service.	2026-01-05	5.1
CVE-2026-20976	samsung - galaxy_store	Improper input validation in Galaxy Store prior to version 4.6.02 allows local attacker to execute arbitrary script.	2026-01-09	5.1
CVE-2026-20029	cisco - Cisco Identity Services Engine Software	A vulnerability in the licensing features of&nbsp;Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) could allow an authenticated, remote attacker with administrative privileges to gain access to sensitive information.&nbsp;_x000D_ _x000D_ This vulnerability is due to improper parsing of XML that is processed by the web-based management interface of Cisco ISE and Cisco ISE-PIC. An attacker could exploit this vulnerability by uploading a malicious file to the application. A successful exploit could allow the attacker to read arbitrary files from the underlying operating system that could include sensitive data that should otherwise be inaccessible even to administrators. To exploit this vulnerability, the attacker must have valid administrative credentials.	2026-01-07	4.9
CVE-2026-20972	samsung - multiple products	Improper Export of Android Application Components in UwbTest prior to SMR Jan-2026 Release 1 allows local attackers to enable UWB.	2026-01-09	4.8
CVE-2025-46286	apple - multiple products	A logic issue was addressed with improved validation. This issue is fixed in iOS 26.2 and iPadOS 26.2. Restoring from a backup may prevent passcode from being required immediately after Face ID enrollment.	2026-01-09	4.3
CVE-2025-46299	apple - multiple products	A memory initialization issue was addressed with improved memory handling. This issue is fixed in tvOS 26.2, Safari 26.2, watchOS 26.2, visionOS 26.2, iOS 26.2 and iPadOS 26.2, macOS Tahoe 26.2. Processing maliciously crafted web content may disclose internal states of the app.	2026-01-09	4.3
CVE-2025-53470	apache - nimble	Out-of-bounds Read vulnerability in Apache NimBLE HCI H4 driver. Specially crafted HCI event could lead to invalid memory read in H4 driver. This issue affects Apache NimBLE: through 1.8. This issue requires a broken or bogus Bluetooth controller and thus severity is considered low. Users are recommended to upgrade to version 1.9, which fixes the issue.	2026-01-10	3.1
CVE-2025-46676	dell - multiple products	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.4.0.0, LTS2025 release version 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.40, LTS 2023 release versions 7.10.1.0 through 7.10.1.70, contain an Exposure of Sensitive Information to an Unauthorized Actor vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Information disclosure.	2026-01-09	2.7

CVE-2026-20969	samsung - multiple products	Improper input validation in SecSettings prior to SMR Jan-2026 Release 1 allows local attacker to access file with system privilege. User interaction is required for triggering this vulnerability.	2026-01-09	2.3
CVE-2025-46643	dell - multiple products	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.4.0.0, LTS2025 release version 8.3.1.10, LTS2024 release versions 7.13.1.0 through 7.13.1.40, LTS 2023 release versions 7.10.1.0 through 7.10.1.70, contain a Heap-based Buffer Overflow vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Denial of service.	2026-01-09	2.3
CVE-2026-20975	samsung - cloud	Improper handling of insufficient permission in Samsung Cloud prior to version 5.6.11 allows local attackers to access specific files in arbitrary path.	2026-01-09	2.1
83				
84				
85				
86				
87				
88				
89				
90				
91				
92				
93				
94				
95				
96				
97				
98				
99				
100				
101				
102				
103				
104				
105				
106				
107				
108				
109				
110				
111				
112				
113				
114				
115				
116				
117				
118				
119				
120				
121				
122				
123				
124				
125				
126				
127				
128				
129				
130				
131				
132				
133				
134				
135				
136				
137				
138				
139				
140				
141				
142				
143				
144				
145				
146				
147				
148				
149				
150				

151				
152				
153				
154				
155				
156				
157				
158				
159				
160				
161				
162				
163				
164				
165				
166				
167				
168				
169				
170				
171				
172				
173				
174				
175				
176				
177				
178				
179				
180				
181				
182				
183				
184				
185				
186				
187				
188				
189				
190				
191				
192				
193				
194				
195				
196				
197				
198				
199				
200				
201				
202				
203				
204				
205				
206				
207				
208				
209				
210				
211				
212				
213				
214				
215				
216				
217				
218				
219				
220				
221				
222				
223				
224				
225				
226				
227				

228				
229				
230				
231				
232				
233				
234				
235				
236				
237				
238				
239		عام		
240				
241				
242				
243				
244				
245				
246				
247				
248				
249				
250				
251				
252				
253				
254				
255				
256				
257				
258				
259				
260				
261				
262				
263				
264				
265				
266				
267				
268				
269				
270				
271				
272				
273				
274				
275				
276				
277				
278				
279				
280				
281				
282				
283				
284				
285				
286				
287				
288				
289				
290				
290				
291				
292				
293				
294				
295				
296				
297				
298				

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.