الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

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 1 فبراير إلى 7 فبراير. 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

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 1st of February to 7th of February. 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
CVE-2026-25592	microsoft - semantic-kernel	Semantic Kernel is an SDK used to build, orchestrate, and deploy AI agents and multi-agent systems. Prior to 1.70.0, an Arbitrary File Write vulnerability has been identified in Microsoft's Semantic Kernel .NET SDK, specifically within the SessionsPythonPlugin. The problem has been fixed in Microsoft.SemanticKernel.Core version 1.70.0. As a mitigation, users can create a Function Invocation Filter which checks the arguments being passed to any calls to DownloadFileAsync or UploadFileAsync and ensures the provided localFilePath is allow listed.	2026-02-06	9.9
CVE-2026-20418	google - matter	In Thread, there is a possible out of bounds write due to a missing bounds check. This could lead to remote escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Patch ID: WCNCR00465153; Issue ID: MSV-4927.	2026-02-02	9.8
CVE-2025-13375	ibm - multiple products	IBM Common Cryptographic Architecture (CCA) 7.5.52 and 8.4.82 could allow an unauthenticated user to execute arbitrary commands with elevated privileges on the system.	2026-02-04	9.8
CVE-2026-24300	microsoft - azure_front_door	Azure Front Door Elevation of Privilege Vulnerability	2026-02-05	9.8
CVE-2026-21643	fortinet - FortiClientEMS	An improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiClientEMS 7.4.4 may allow an unauthenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.	2026-02-06	9.8
CVE-2026-1709	red hat - multiple products	A flaw was found in Keylime. The Keylime registrar, since version 7.12.0, does not enforce client-side Transport Layer Security (TLS) authentication. This authentication bypass vulnerability allows unauthenticated clients with network access to perform administrative operations, including listing agents, retrieving public Trusted Platform Module (TPM) data, and deleting agents, by connecting without presenting a client certificate.	2026-02-06	9.4
CVE-2026-0106	google - android	In vpu_mmap of vpu_ioctl, there is a possible arbitrary address mmap due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-02-05	9.3
CVE-2026-1861	google - chrome	Heap buffer overflow in libvpx in Google Chrome prior to 144.0.7559.132 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-02-03	8.8
CVE-2026-1862	google - chrome	Type Confusion in V8 in Google Chrome prior to 144.0.7559.132 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-02-03	8.8
CVE-2026-20098	cisco - Cisco Meeting Management	A vulnerability in the Certificate Management feature of Cisco Meeting Management could allow an authenticated, remote attacker to upload arbitrary files, execute arbitrary commands, and elevate privileges to root on an affected system._x000D_ _x000D_ This vulnerability is due to improper input validation in certain sections of the web-based management interface. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could allow the attacker to upload arbitrary files to the affected system. The malicious files could overwrite system files that are processed by the root system account and allow arbitrary command execution with root privileges. To exploit this vulnerability, the attacker must have valid credentials for a user account with at least the role of video operator.	2026-02-04	8.8
CVE-2026-1761	red hat - multiple products	A flaw was found in libsoup. This stack-based buffer overflow vulnerability occurs during the parsing of multipart HTTP responses due to an incorrect length calculation. A remote attacker can exploit this by sending a specially crafted multipart HTTP response, which can lead to memory corruption. This issue may result in application crashes or arbitrary code execution in applications that process untrusted server responses, and it does not require authentication or user interaction.	2026-02-02	8.6

CVE-2026-22229	tp-link - archer_be230_firmware	A command injection vulnerability may be exploited after the admin's authentication via the import of a crafted VPN client configuration file on the TP-Link Archer BE230 v1.2. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	2026-02-02	8.6
CVE-2025-62673	tp-link - archer_ax53_firmware	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tdpserver modules) allows adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted network packet containing a maliciously formed field.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	2026-02-03	8.6
CVE-2025-13379	ibm - aspera_console	IBM Aspera Console 3.4.0 through 3.4.8 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify, or delete information in the back-end database.	2026-02-05	8.6
CVE-2026-24302	microsoft - azure_arc	Azure Arc Elevation of Privilege Vulnerability	2026-02-05	8.6
CVE-2020-37045	veritas - NetBackup	Veritas NetBackup 7.0 contains an unquoted service path vulnerability in the NetBackup INET Daemon service that allows local users to potentially execute arbitrary code. Attackers can exploit the unquoted path in C:\Program Files\Veritas\NetBackup\bin\bpinetd.exe to inject malicious code that would execute with elevated LocalSystem privileges.	2026-02-01	8.5
CVE-2026-0630	tp-link - archer_be230_firmware	An OS Command Injection vulnerability in TP-Link Archer BE230 v1.2(web modules) allows adjacent authenticated attacker to execute arbitrary code. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID.This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	2026-02-02	8.5
CVE-2026-0631	tp-link - archer_be230_firmware	An OS Command Injection vulnerability in TP-Link Archer BE230 v1.2(vpn modules) allows an adjacent authenticated attacker to execute arbitrary code. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID.This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	2026-02-02	8.5
CVE-2026-22221	tp-link - archer_be230_firmware	An OS Command Injection vulnerability in TP-Link Archer BE230 v1.2(vpn modules) allows adjacent authenticated attacker execute arbitrary code. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID.This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	2026-02-02	8.5
CVE-2026-22222	tp-link - archer_be230_firmware	An OS Command Injection vulnerability in TP-Link Archer BE230 v1.2(web modules) allows adjacent authenticated attacker to execute arbitrary code. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID.This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	2026-02-02	8.5
CVE-2026-22223	tp-link - archer_be230_firmware	An OS Command Injection vulnerability in TP-Link Archer BE230 v1.2(vpn modules) allows adjacent authenticated attacker execute arbitrary code. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID.This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	2026-02-02	8.5

CVE-2026-22224	tp-link - archer_be230_firmware	A command injection vulnerability may be exploited after the admin's authentication in the cloud communication interface on the TP-Link Archer BE230 v1.2. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	2026-02-02	8.5
CVE-2026-22225	tp-link - archer_be230_firmware	A command injection vulnerability may be exploited after the admin's authentication in the VPN Connection Service on the Archer BE230 v1.2. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	2026-02-02	8.5
CVE-2026-22226	tp-link - archer_be230_firmware	A command injection vulnerability may be exploited after the admin's authentication in the VPN server configuration module on the TP-Link Archer BE230 v1.2. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	2026-02-02	8.5
CVE-2026-22227	tp-link - archer_be230_firmware	A command injection vulnerability may be exploited after the admin's authentication via the configuration backup restoration function of the TP-Link Archer BE230 v1.2. Successful exploitation could allow an attacker to gain full administrative control of the device, resulting in severe compromise of configuration integrity, network security, and service availability. This CVE covers one of multiple distinct OS command injection issues identified across separate code paths. Although similar in nature, each instance is tracked under a unique CVE ID. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	2026-02-02	8.5
CVE-2026-20979	samsung - multiple products	Improper privilege management in Settings prior to SMR Feb-2026 Release 1 allows local attackers to launch arbitrary activity with Settings privilege.	2026-02-04	8.4
CVE-2026-20983	samsung - multiple products	Improper export of android application components in Samsung Dialer prior to SMR Feb-2026 Release 1 allows local attackers to launch arbitrary activity with Samsung Dialer privilege.	2026-02-04	8.4
CVE-2026-24926	huawei - harmonyos	Out-of-bounds write vulnerability in the camera module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-02-06	8.4
CVE-2026-24930	huawei - multiple products	UAF concurrency vulnerability in the graphics module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-02-06	8.4
CVE-2026-1642	f5 - multiple products	A vulnerability exists in NGINX OSS and NGINX Plus when configured to proxy to upstream Transport Layer Security (TLS) servers. An attacker with a man-in-the-middle (MITM) position on the upstream server side—along with conditions beyond the attacker's control—may be able to inject plain text data into the response from an upstream proxied server. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-02-04	8.2
CVE-2026-22548	f5 - multiple products	When a BIG-IP Advanced WAF or ASM security policy is configured on a virtual server, undisclosed requests along with conditions beyond the attacker's control can cause the bd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-02-04	8.2
CVE-2026-21532	microsoft - azure_functions	Azure Function Information Disclosure Vulnerability	2026-02-05	8.2
CVE-2026-1530	red hat - multiple products	A flaw was found in fog-kubevirt. This vulnerability allows a remote attacker to perform a Man-in-the-Middle (MITM) attack due to disabled certificate validation. This enables the attacker to intercept and potentially alter sensitive communications between Satellite and OpenShift, resulting in information disclosure and data integrity compromise.	2026-02-02	8.1
CVE-2026-1531	red hat - multiple products	A flaw was found in foreman_kubevirt. When configuring the connection to OpenShift, the system disables SSL verification if a Certificate Authority (CA) certificate is not explicitly set. This insecure default allows a remote attacker, capable of intercepting network traffic between Satellite and OpenShift, to perform a Man-in-the-Middle (MITM) attack. Such an attack could lead to the disclosure or alteration of sensitive information.	2026-02-02	8.1
CVE-2026-20409	google - android	In imgsys, 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: ALPS10363246; Issue ID: MSV-5779.	2026-02-02	7.8
CVE-2026-20411	google - multiple products	In cameraisp, there is a possible escalation of privilege due to use after free. This could lead to local denial of service if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10351676; Issue ID: MSV-5737.	2026-02-02	7.8

CVE-2026-20412	google - multiple products	In cameraisp, 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: ALPS10351676; Issue ID: MSV-5733.	2026-02-02	7.8
CVE-2025-47358	qualcomm - fastconnect_6900_firmware	Memory Corruption when user space address is modified and passed to mem_free API, causing kernel memory to be freed inadvertently.	2026-02-02	7.8
CVE-2025-47359	qualcomm - qca6391_firmware	Memory Corruption when multiple threads simultaneously access a memory free API.	2026-02-02	7.8
CVE-2025-47397	qualcomm - ar8031_firmware	Memory Corruption when initiating GPU memory mapping using scatter-gather lists due to unchecked IOMMU mapping errors.	2026-02-02	7.8
CVE-2025-47398	qualcomm - qcm6490_firmware	Memory Corruption while deallocating graphics processing unit memory buffers due to improper handling of memory pointers.	2026-02-02	7.8
CVE-2025-47399	qualcomm - cologne_firmware	Memory Corruption while processing IOCTL call to update sensor property settings with invalid input parameters.	2026-02-02	7.8
CVE-2025-14914	ibm - websphere_application_server	IBM WebSphere Application Server Liberty 17.0.0.3 through 26.0.0.1 could allow a privileged user to upload a zip archive containing path traversal sequences resulting in an overwrite of files leading to arbitrary code execution.	2026-02-02	7.6
CVE-2025-59439	samsung - exynos_990_firmware	An issue was discovered in Samsung Mobile Processor, Wearable Processor and Modem Exynos 980, 990, 850, 1080, 9110, W920, W930, W1000 and Modem 5123. Incorrect handling of NAS Registration messages leads to a Denial of Service because of Improper Handling of Exceptional Conditions.	2026-02-03	7.5
CVE-2026-24735	apache - answer	Exposure of Private Personal Information to an Unauthorized Actor vulnerability in Apache Answer. This issue affects Apache Answer: through 1.7.1. An unauthenticated API endpoint incorrectly exposes full revision history for deleted content. This allows unauthorized user to retrieve restricted or sensitive information. Users are recommended to upgrade to version 2.0.0, which fixes the issue.	2026-02-04	7.5
CVE-2026-20119	cisco - multiple products	A vulnerability in the text rendering subsystem of Cisco TelePresence Collaboration Endpoint (CE) Software and Cisco RoomOS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device._x000D_ _x000D_ This vulnerability is due to insufficient validation of input received by an affected device. An attacker could exploit this vulnerability by getting the affected device to render crafted text, for example, a crafted meeting invitation. As indicated in the CVSS score, no user interaction is required, such as accepting the meeting invitation. A successful exploit could allow the attacker to cause the affected device to reload, resulting in a DoS condition.	2026-02-04	7.5
CVE-2025-15557	tp-link - tapo_h100_firmware	An Improper Certificate Validation vulnerability in TP-Link Tapo H100 v1 and Tapo P100 v1 allows an on-path attacker on the same network segment to intercept and modify encrypted device-cloud communications. This may compromise the confidentiality and integrity of device-to-cloud communication, enabling manipulation of device data or operations.	2026-02-05	7.5
CVE-2025-58077	tp-link - archer_ax53_firmware	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted set of network packets containing an excessive number of host entries This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	2026-02-03	7.3
CVE-2025-58455	tp-link - archer_ax53_firmware	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted network packet whose length exceeds the maximum expected value.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	2026-02-03	7.3
CVE-2025-59482	tp-link - archer_ax53_firmware	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted network packet containing a field whose length exceeds the maximum expected value.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	2026-02-03	7.3
CVE-2025-59487	tp-link - archer_ax53_firmware	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code. The vulnerability arises from improper validation of a packet field whose offset is used to determine the write location in memory. By crafting a packet with a manipulated field offset, an attacker can redirect writes to arbitrary memory locations.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	2026-02-03	7.3
CVE-2025-61944	tp-link - archer_ax53_firmware	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted network packet containing an excessive number of fields with zero-length values.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	2026-02-03	7.3
CVE-2025-61983	tp-link - archer_ax53_firmware	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted network packet containing an excessive number of fields with zero-length values.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	2026-02-03	7.3
CVE-2025-62404	tp-link - archer_ax53_firmware	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary code via a specially crafted network packet whose length exceeds the maximum expected value.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	2026-02-03	7.3
CVE-2025-62405	tp-link - archer_ax53_firmware	Heap-based Buffer Overflow vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows authenticated adjacent attackers to cause a segmentation fault or potentially execute arbitrary	2026-02-03	7.3

		code via a specially crafted network packet containing a field whose length exceeds the maximum expected value.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.		
CVE-2026-24925	huawei - multiple products	Heap-based buffer overflow vulnerability in the image module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-02-06	7.3
CVE-2025-11730	zyxel - multiple products	A post-authentication command injection vulnerability in the Dynamic DNS (DDNS) configuration CLI command in Zyxel ATP series firmware versions from V5.35 through V5.41, USG FLEX series firmware versions from V5.35 through V5.41, USG FLEX 50(W) series firmware versions from V5.35 through V5.41, and USG20(W)-VPN series firmware versions from V5.35 through V5.41 could allow an authenticated attacker with administrator privileges to execute operating system (OS) commands on an affected device by supplying a specially crafted string as an argument to the CLI command.	2026-02-05	7.2
CVE-2026-23572	teamviewer - multiple products	Improper access control in the TeamViewer Full and Host clients (Windows, macOS, Linux) prior version 15.74.5 allows an authenticated user to bypass additional access controls with “Allow after confirmation” configuration in a remote session. An exploit could result in unauthorized access prior to local confirmation. The user needs to be authenticated for the remote session via ID/password, Session Link, or Easy Access as a prerequisite to exploit this vulnerability.	2026-02-05	7.2
CVE-2025-47366	qualcomm - ar8035_firmware	Cryptographic issue when a Trusted Zone with outdated code is triggered by a HLOS providing incorrect input.	2026-02-02	7.1
CVE-2025-13096	ibm - multiple products	IBM Business Automation Workflow containers V25.0.0 through V25.0.0-IF007, V24.0.1 - V24.0.1-IF007, V24.0.0 - V24.0.0-IF007 and IBM Business Automation Workflow traditional V25.0.0, V24.0.1, V24.0.0 is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources.	2026-02-02	7.1
CVE-2025-62501	tp-link - archer_ax53_firmware	SSH Hostkey misconfiguration vulnerability in TP-Link Archer AX53 v1.0 (tmpserver modules) allows attackers to obtain device credentials through a specially crafted man-in-the-middle (MITM) attack. This could enable unauthorized access if captured credentials are reused.This issue affects Archer AX53 v1.0: through 1.3.1 Build 20241120.	2026-02-03	7
CVE-2026-20980	samsung - multiple products	Improper input validation in PACM prior to SMR Feb-2026 Release 1 allows physical attacker to execute arbitrary commands.	2026-02-04	7
CVE-2026-20977	samsung - multiple products	Improper access control in Emergency Sharing prior to SMR Feb-2026 Release 1 allows local attackers to interrupt its functioning.	2026-02-04	6.9
CVE-2026-22549	f5 - multiple products	A vulnerability exists in F5 BIG-IP Container Ingress Services that may allow excessive permissions to read cluster secrets. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-02-04	6.9
CVE-2026-24922	huawei - harmonyos	Buffer overflow vulnerability in the HDC module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-02-06	6.9
CVE-2025-47363	qualcomm - qam8255p_firmware	Memory corruption when calculating oversized partition sizes without proper checks.	2026-02-02	6.8
CVE-2025-47364	qualcomm - qam8255p_firmware	Memory corruption while calculating offset from partition start point.	2026-02-02	6.8
CVE-2026-23794	apache - multiple products	Reflected XSS in Apache Syncope's Enduser Login page. An attacker that tricks a legitimate user into clicking a malicious link and logging in to Syncope Enduser could steal that user's credentials. This issue affects Apache Syncope: from 3.0 through 3.0.15, from 4.0 through 4.0.3. Users are recommended to upgrade to version 3.0.16 / 4.0.4, which fix this issue.	2026-02-03	6.8
CVE-2026-22220	tp-link - archer_be230_firmware	A lack of proper input validation in the HTTP processing path in TP-Link Archer BE230 v1.2 (web modules) may allow a crafted request to cause the device’s web service to become unresponsive, resulting in a denial of service condition. A network adjacent attacker with high privileges could cause the device’s web interface to temporarily stop responding until it recovers or is rebooted. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	2026-02-03	6.8
CVE-2026-22228	tp-link - archer_be230_firmware	An authenticated user with high privileges may trigger a denial-of-service condition in TP-Link Archer BE230 v1.2 by restoring a crafted configuration file containing an excessively long parameter. Restoring such a file can cause the device to become unresponsive, requiring a reboot to restore normal operation. This issue affects Archer BE230 v1.2 < 1.2.4 Build 20251218 rel.70420.	2026-02-03	6.8
CVE-2026-20982	samsung - multiple products	Path traversal in ShortcutService prior to SMR Feb-2026 Release 1 allows privileged local attacker to create file with system privilege.	2026-02-04	6.8
CVE-2026-24918	huawei - multiple products	Address read vulnerability in the communication module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-02-06	6.8
CVE-2026-20410	google - android	In imgsys, 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: ALPS10362552; Issue ID: MSV-5760.	2026-02-02	6.7
CVE-2026-20413	google - android	In imgsys, 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: ALPS10362725; Issue ID: MSV-5694.	2026-02-02	6.7
CVE-2026-20414	google - android	In imgsys, there is a possible escalation of privilege 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: ALPS10362999; Issue ID: MSV-5625.	2026-02-02	6.7
CVE-2025-47402	qualcomm - sa8620p_firmware	Transient DOS when processing a received frame with an excessively large authentication information element.	2026-02-02	6.5
CVE-2024-51451	ibm - concert	IBM Concert 1.0.0 through 2.1.0 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking.	2026-02-04	6.5
CVE-2025-14150	ibm - webMethods Integration (on	IBM webMethods Integration (on prem) - Integration Server 10.15 through IS_10.15_Core_Fix2411.1 to IS_11.1_Core_Fix8 IBM webMethods Integration could disclose sensitive user information in server responses.	2026-02-05	6.5

	prem) - Integration Server			
CVE-2026-0391	microsoft - Microsoft Edge (Chromium-based)	User interface (ui) misrepresentation of critical information in Microsoft Edge for Android allows an unauthorized attacker to perform spoofing over a network.	2026-02-05	6.5
CVE-2026-24917	huawei - multiple products	UAF vulnerability in the security module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-02-06	6.5
CVE-2025-36436	ibm - Cloud Pak for Business Automation	IBM Cloud Pak for Business Automation 25.0.0 through 25.0.0 Interim Fix 002, 24.0.1 through 24.0.1 Interim Fix 005, and 24.0.0 through 24.0.0 Interim Fix 007 is vulnerable to stored cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-02-02	6.4
CVE-2024-43181	ibm - concert	IBM Concert 1.0.0 through 2.1.0 does not invalidate session after logout which could allow an authenticated user to impersonate another user on the system.	2026-02-04	6.3
CVE-2026-24923	huawei - harmonyos	Permission control vulnerability in the HDC module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-02-06	6.3
CVE-2026-1757	red hat - multiple products	A flaw was identified in the interactive shell of the xmllint utility, part of the libxml2 project, where memory allocated for user input is not properly released under certain conditions. When a user submits input consisting only of whitespace, the program skips command execution but fails to free the allocated buffer. Repeating this action causes memory to continuously accumulate. Over time, this can exhaust system memory and terminate the xmllint process, creating a denial-of-service condition on the local system.	2026-02-02	6.2
CVE-2025-58340	samsung - exynos_980_firmware	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 1330, 1380, 1480, 1580, W920, W930 and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/send_delts write operation, leading to kernel memory exhaustion.	2026-02-03	6.2
CVE-2025-58341	samsung - exynos_980_firmware	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 1330, 1380, 1480, 1580, W920, W930 and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/ap_cert_disable_ht_vht write operation, leading to kernel memory exhaustion.	2026-02-03	6.2
CVE-2025-58342	samsung - exynos_980_firmware	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 1330, 1380, 1480, 1580, W920, W930 and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/uapsd write operation, leading to kernel memory exhaustion.	2026-02-03	6.2
CVE-2025-58344	samsung - exynos_980_firmware	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 1330, 1380, 1480, 1580, W920, W930 and W1000. There is unbounded memory allocation in a /proc/driver/unifi0/conn_log_event_burst_to_us write operation, leading to kernel memory exhaustion.	2026-02-03	6.2
CVE-2026-24915	huawei - multiple products	Out-of-bounds read issue in the media subsystem. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	2026-02-06	6.2
CVE-2026-24920	huawei - multiple products	Permission control vulnerability in the AMS module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-02-06	6.2
CVE-2026-24924	huawei - harmonyos	Vulnerability of improper permission control in the print module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-02-06	6.1
CVE-2025-36238	ibm - PowerVM Hypervisor	IBM PowerVM Hypervisor FW1110.00 through FW1110.03, FW1060.00 through FW1060.51, and FW950.00 through FW950.F0 could allow a local user with administration privileges to obtain sensitive information from a Virtual TPM through a series of PowerVM service procedures.	2026-02-02	6
CVE-2026-24919	huawei - multiple products	Out-of-bounds write vulnerability in the DFX module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-02-06	6
CVE-2025-36253	ibm - concert	IBM Concert 1.0.0 through 2.1.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information.	2026-02-02	5.9
CVE-2025-15551	tp-link - archer_mr200_firmware	The response coming from TP-Link Archer MR200 v5.2, C20 v6, TL-WR850N v3, and TL-WR845N v4 for any request is getting executed by the JavaScript function like eval directly without any check. Attackers can exploit this vulnerability via a Man-in-the-Middle (MitM) attack to execute JavaScript code on the router's admin web portal without the user's permission or knowledge.	2026-02-05	5.9
CVE-2026-24916	huawei - harmonyos	Identity authentication bypass vulnerability in the window module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-02-06	5.9
CVE-2026-24929	huawei - harmonyos	Out-of-bounds read vulnerability in the graphics module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-02-06	5.9
CVE-2026-24931	huawei - multiple products	Vulnerability of improper criterion security check in the card module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-02-06	5.9
CVE-2026-20978	samsung - multiple products	Improper authorization in KnoxGuardManager prior to SMR Feb-2026 Release 1 allows local attackers to bypass the persistence configuration of the application.	2026-02-04	5.8
CVE-2026-24928	huawei - multiple products	Out-of-bounds write vulnerability in the file system module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-02-06	5.8
CVE-2026-20415	google - android	In imgsys, there is a possible memory corruption due to improper locking. This could lead to local denial of service if a malicious actor has already obtained the System privilege. User interaction is not needed for exploitation. Patch ID: ALPS10363254; Issue ID: MSV-5617.	2026-02-02	5.5
CVE-2025-58343	samsung - exynos_980_firmware	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 1330, 1380, 1480, 1580, W920, W930 and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/create_tspec write operation, leading to kernel memory exhaustion.	2026-02-03	5.5
CVE-2025-58345	samsung - exynos_980_firmware	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 1330, 1380, 1480, 1580, W920, W930 and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/ap_certif_11ax_mode write operation, leading to kernel memory exhaustion.	2026-02-03	5.5

CVE-2025-58346	samsung - exynos_980_firmware	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 1330, 1380, 1480, 1580, W920, W930 and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/send_addts write operation, leading to kernel memory exhaustion.	2026-02-03	5.5
CVE-2025-58347	samsung - exynos_980_firmware	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 1330, 1380, 1480, 1580, W920, W930 and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/p2p_certif write operation, leading to kernel memory exhaustion.	2026-02-03	5.5
CVE-2025-58348	samsung - exynos_980_firmware	An issue was discovered in the Wi-Fi driver in Samsung Mobile Processor and Wearable Processor Exynos 980, 850, 1080, 1280, 1330, 1380, 1480, 1580, W920, W930 and W1000. There is unbounded memory allocation via a large buffer in a /proc/driver/unifi0/confg_tspec write operation, leading to kernel memory exhaustion.	2026-02-03	5.5
CVE-2026-24927	huawei - multiple products	Out-of-bounds access vulnerability in the frequency modulation module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-02-06	5.5
CVE-2026-2054	d-link - multiple products	A security flaw has been discovered in D-Link DIR-605L and DIR-619L 2.06B01/2.13B01. Impacted is an unknown function of the component Wifi Setting Handler. Performing a manipulation results in information disclosure. The attack may be initiated remotely. The exploit has been released to the public and may be used for attacks. This vulnerability only affects products that are no longer supported by the maintainer.	2026-02-06	5.5
CVE-2026-2055	d-link - multiple products	A weakness has been identified in D-Link DIR-605L and DIR-619L 2.06B01/2.13B01. The affected element is an unknown function of the component DHCP Client Information Handler. Executing a manipulation can lead to information disclosure. The attack may be launched remotely. The exploit has been made available to the public and could be used for attacks. This vulnerability only affects products that are no longer supported by the maintainer.	2026-02-06	5.5
CVE-2026-2056	d-link - multiple products	A security vulnerability has been detected in D-Link DIR-605L and DIR-619L 2.06B01/2.13B01. The impacted element is an unknown function of the file /wan_connection_status.asp of the component DHCP Connection Status Handler. The manipulation leads to information disclosure. Remote exploitation of the attack is possible. The exploit has been disclosed publicly and may be used. This vulnerability only affects products that are no longer supported by the maintainer.	2026-02-06	5.5
CVE-2025-36033	ibm - Engineering Lifecycle Management - Global Configuration Management	IBM Engineering Lifecycle Management - Global Configuration Management 7.0.3 through 7.0.3 Interim Fix 017, and 7.1.0 through 7.1.0 Interim Fix 004 IBM Global Configuration Management is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-02-03	5.4
CVE-2025-36094	ibm - Cloud Pak for Business Automation	IBM Cloud Pak for Business Automation 25.0.0 through 25.0.0 Interim Fix 002, 24.0.1 through 24.0.1 Interim Fix 005, and 24.0.0 through 24.0.0 Interim Fix 007 could allow an authenticated user to cause a denial of service or corrupt existing data due to the improper validation of input length.	2026-02-03	5.4
CVE-2026-20981	samsung - multiple products	Improper input validation in FacAtFunction prior to SMR Feb-2026 Release 1 allows privileged physical attacker to execute arbitrary command with system privilege.	2026-02-04	5.4
CVE-2026-0945	drupal - Role Delegation	Privilege Defined With Unsafe Actions vulnerability in Drupal Role Delegation allows Privilege Escalation.This issue affects Role Delegation: from 1.3.0 before 1.5.0.	2026-02-04	5.4
CVE-2026-20417	google - multiple products	In pcie, 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: ALPS10314946 / ALPS10340155; Issue ID: MSV-5154.	2026-02-02	5.3
CVE-2026-1760	red hat - multiple products	A flaw was found in SoupServer. This HTTP request smuggling vulnerability occurs because SoupServer improperly handles requests that combine Transfer-Encoding: chunked and Connection: keep-alive headers. A remote, unauthenticated client can exploit this by sending specially crafted requests, causing SoupServer to fail to close the connection as required by RFC 9112. This allows the attacker to smuggle additional requests over the persistent connection, leading to unintended request processing and potential denial-of-service (DoS) conditions.	2026-02-02	5.3
CVE-2026-1801	red hat - multiple products	A flaw was found in libsoup, an HTTP client/server library. This HTTP Request Smuggling vulnerability arises from non-RFC-compliant parsing in the soup_filter_input_stream_read_line() logic, where libsoup accepts malformed chunk headers, such as lone line feed (LF) characters instead of the required carriage return and line feed (CRLF). A remote attacker can exploit this without authentication or user interaction by sending specially crafted chunked requests. This allows libsoup to parse and process multiple HTTP requests from a single network message, potentially leading to information disclosure.	2026-02-03	5.3
CVE-2023-38010	ibm - multiple products	IBM Cloud Pak System displays sensitive information in user messages that could aid in further attacks against the system.	2026-02-04	5.3
CVE-2023-38017	ibm - multiple products	IBM Cloud Pak System is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-02-04	5.3
CVE-2023-38281	ibm - multiple products	IBM Cloud Pak System does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic.	2026-02-04	5.3
CVE-2024-39724	ibm - Db2 Big SQL on Cloud Pak for Data	IBM Db2 Big SQL on Cloud Pak for Data versions 7.6 (on CP4D 4.8), 7.7 (on CP4D 5.0), and 7.8 (on CP4D 5.1) do not properly limit the allocation of system resources. An authenticated user with internal knowledge of the environment could exploit this weakness to cause a denial of service.	2026-02-04	5.3
CVE-2025-13491	ibm - multiple products	IBM App Connect Enterprise Certified Container up to 12.19.0 (Continuous Delivery) and 12.0 LTS (Long Term Support) could allow an attacker to access sensitive files or modify configurations due to an untrusted search path.	2026-02-05	5.1
CVE-2026-23795	apache - multiple products	Improper Restriction of XML External Entity Reference vulnerability in Apache Syncope Console. An administrator with adequate entitlements to create or edit Keymaster parameters via Console can construct malicious XML text to launch an XXE attack, thereby causing sensitive data leakage occurs.	2026-02-03	4.9

		This issue affects Apache Syncope: from 3.0 through 3.0.15, from 4.0 through 4.0.3. Users are recommended to upgrade to version 3.0.16 / 4.0.4, which fix this issue.		
CVE-2026-20111	cisco - Cisco Prime Infrastructure	A vulnerability in the web-based management interface of Cisco Prime Infrastructure could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against users of the interface of an affected system._x000D_ _x000D_ This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by inserting malicious code into specific data fields in 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, an attacker must have valid administrative credentials.	2026-02-04	4.8
CVE-2026-24921	huawei - harmonyos	Address read vulnerability in the HDC module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	2026-02-06	4.8
CVE-2025-15395	ibm - multiple products	IBM Jazz Foundation 7.0.3 through 7.0.3 iFix019 and 7.1.0 through 7.1.0 iFix005 is vulnerable to access control violations that allows the users to view or access/perform actions beyond their expected capability.	2026-02-02	4.3
CVE-2026-20123	cisco - multiple products	A vulnerability in the web-based management interface of Cisco Evolved Programmable Network Manager (EPNM) and Cisco Prime Infrastructure could allow an unauthenticated, remote attacker to redirect a user to a malicious web page._x000D_ _x000D_ This vulnerability is due to improper input validation of the parameters in the HTTP request. An attacker could exploit this vulnerability by intercepting and modifying an HTTP request from a user. A successful exploit could allow the attacker to redirect the user to a malicious web page.	2026-02-04	4.3
CVE-2024-40685	ibm - Operations Analytics - Log Analysis	IBM Operations Analytics – Log Analysis versions 1.3.5.0 through 1.3.8.3 and IBM SmartCloud Analytics – Log Analysis are vulnerable to a cross-site request forgery (CSRF) vulnerability that could allow an attacker to trick a trusted user into performing unauthorized actions.	2026-02-04	4.3
CVE-2026-0598	red hat - multiple products	A security flaw was identified in the Ansible Lightspeed API conversation endpoints that handle AI chat interactions. The APIs do not properly verify whether a conversation identifier belongs to the authenticated user making the request. As a result, an attacker with valid credentials could access or influence conversations owned by other users. This exposes sensitive conversation data and allows unauthorized manipulation of AI-generated outputs.	2026-02-06	4.2
CVE-2026-20056	cisco - Cisco Secure Web Appliance	A vulnerability in the Dynamic Vectoring and Streaming (DVS) Engine implementation of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass the anti-malware scanner, allowing malicious archive files to be downloaded._x000D_ _x000D_ This vulnerability is due to improper handling of certain archive files. An attacker could exploit this vulnerability by sending a crafted archive file, which should be blocked, through an affected device. A successful exploit could allow the attacker to bypass the anti-malware scanner and download malware onto an end user workstation. The downloaded malware will not automatically execute unless the end user extracts and launches the malicious file.	2026-02-04	4
CVE-2026-24914	huawei - harmonyos	Type confusion vulnerability in the camera module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-02-06	4
CVE-2025-1823	ibm - multiple products	IBM Jazz Reporting Service could allow an authenticated user on the host network to cause a denial of service using specially crafted SQL query that consumes excess memory resources.	2026-02-04	3.5
CVE-2025-27550	ibm - Jazz Reporting Service	IBM Jazz Reporting Service could allow an authenticated user on the host network to obtain sensitive information about other projects that reside on the server.	2026-02-04	3.5
CVE-2025-2134	ibm - Jazz Reporting Service	IBM Jazz Reporting Service could allow an authenticated user on the network to affect the system's performance using complicated queries due to insufficient resource pooling.	2026-02-04	3.5
CVE-2025-33081	ibm - concert	IBM Concert 1.0.0 through 2.1.0 stores potentially sensitive information in log files that could be read by a local user.	2026-02-03	3.3
CVE-2026-25815	fortinet - FortiOS	Fortinet FortiOS through 7.6.6 allows attackers to decrypt LDAP credentials stored in device configuration files, as exploited in the wild from 2025-12-16 through 2026 (by default, the encryption key is the same across all customers' installations). NOTE: the Supplier's position is that the instance of CWE-1394 is not a vulnerability because customers "are supposed to enable" a non-default option that eliminates the weakness. However, that non-default option can disrupt functionality as shown in the "Managing FortiGates with private data encryption" document, and is therefore intentionally not a default option.	2026-02-05	3.2
CVE-2025-36194	ibm - PowerVM Hypervisor	IBM PowerVM Hypervisor FW1110.00 through FW1110.03, FW1060.00 through FW1060.51, and FW950.00 through FW950.F0 may expose a limited amount of data to a peer partition in specific shared processor configurations during certain operations.	2026-02-02	2.8
CVE-2025-13881	red hat - multiple products	A flaw was found in Keycloak Admin API. This vulnerability allows an administrator with limited privileges to retrieve sensitive custom attributes via the /unmanagedAttributes endpoint, bypassing User Profile visibility settings.	2026-02-02	2.7
CVE-2026-1518	red hat - multiple products	A flaw was found in Keycloak’s CIBA feature where insufficient validation of client-configured backchannel notification endpoints could allow blind server-side requests to internal services.	2026-02-02	2.7
CVE-2026-20732	f5 - multiple products	A vulnerability exists in an undisclosed BIG-IP Configuration utility page that may allow an attacker to spoof error messages. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-02-04	2.3
CVE-2026-20730	f5 - multiple products	A vulnerability exists in BIG-IP Edge Client and browser VPN clients on Windows that may allow attackers to gain access to sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2026-02-04	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.