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 10 مايو إلى 16 مايو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

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 10th of May to 16th of May. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2026-20182	cisco - multiple products	May 2026: This security advisory provides the details and fix information for a vulnerability that was discovered and fixed after the was disclosed in February 2026. This new advisory is for a new vulnerability in the control connection handshaking. The section of this advisory includes Show Control Connections guidance to help with system checks. A vulnerability in the peering authentication in Cisco Catalyst SD-WAN Controller, formerly SD-WAN vSmart, and Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an unauthenticated, remote attacker to bypass authentication and obtain administrative privileges on an affected system. This vulnerability exists because the peering authentication mechanism in an affected system is not working properly. An attacker could exploit this vulnerability by sending crafted requests to the affected system. A successful exploit could allow the attacker to log in to an affected Cisco Catalyst SD-WAN Controller as an internal, high-privileged, non-root user account. Using this account, the attacker could access NETCONF, which would then allow the attacker to manipulate network configuration for the SD-WAN fabric.	2026-05-14	10
CVE-2026-42823	microsoft - azure_logic_apps	Improper access control in Azure Logic Apps allows an authorized attacker to elevate privileges over a network.	2026-05-12	9.9
CVE-2026-42898	microsoft - dynamics_365	Improper control of generation of code ('code injection') in Microsoft Dynamics 365 (on-premises) allows an authorized attacker to execute code over a network.	2026-05-12	9.9
CVE-2026-40636	dell - multiple products	Dell ECS versions 3.8.1.0 through 3.8.1.7 and Dell ObjectScale versions prior to 4.3.0.0, contains a use of hard-coded credentials vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to filesystem access for attacker.	2026-05-11	9.8
CVE-2026-8401	mozilla - firefox	Sandbox escape in the Profile Backup component. This vulnerability was fixed in Firefox 150.0.3, Firefox ESR 115.36, Firefox ESR 140.11, and Thunderbird 140.11.	2026-05-12	9.8
CVE-2026-41293	apache - multiple products	Improper Input Validation vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.21, from 10.1.0-M1 through 10.1.54, from 9.0.0.M1 through 9.0.117, from 10.0.0-M1 through 10.0.27. Older, end of support versions may also be affected. Users are recommended to upgrade to version [FIXED_VERSION], which fixes the issue.	2026-05-12	9.8
CVE-2026-43512	apache - multiple products	DEPRECATED: Authentication Bypass Issues vulnerability in digest authentication in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.21, from 10.1.0-M1 through 10.1.54, from 9.0.0.M1 through 9.0.117, from 8.5.0 through 8.5.100, from before 7.0.0. Older unsupported versions any also be affect Users are recommended to upgrade to version 11.0.22, 10.1.55 or 9.0.118 which fix the issue.	2026-05-12	9.8
CVE-2026-26083	fortinet - multiple products	A missing authorization vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.1, FortiSandbox 4.4.0 through 4.4.8, FortiSandbox Cloud 5.0.2 through 5.0.5, FortiSandbox PaaS 23.4 all versions, FortiSandbox PaaS 23.3 all versions, FortiSandbox PaaS 23.1 all versions, FortiSandbox PaaS 22.2 all versions, FortiSandbox PaaS 22.1 all versions, FortiSandbox PaaS 21.4 all versions, FortiSandbox PaaS 21.3 all versions, FortiSandbox PaaS 5.0.0 through 5.0.1, FortiSandbox PaaS 4.4.5 through 4.4.8 may allow an unauthenticated attacker to execute unauthorized code or commands via HTTP requests.	2026-05-12	9.8

CVE-2026-41089	microsoft - multiple products	Stack-based buffer overflow in Windows Netlogon allows an unauthorized attacker to execute code over a network.	2026-05-12	9.8
CVE-2026-41096	microsoft - multiple products	Heap-based buffer overflow in Microsoft Windows DNS allows an unauthorized attacker to execute code over a network.	2026-05-12	9.8
CVE-2026-44277	fortinet - multiple products	A improper access control vulnerability in Fortinet FortiAuthenticator 8.0.2, FortiAuthenticator 8.0.0, FortiAuthenticator 6.6.0 through 6.6.8, FortiAuthenticator 6.5.0 through 6.5.6 may allow attacker to execute unauthorized code or commands via <insert attack vector here>	2026-05-12	9.8
CVE-2026-45185	exim - Exim	Exim before 4.99.3, in certain GnuTLS configurations, has a remotely reachable use-after-free in the BDAT body parsing path. It is triggered when a client sends a TLS close_notify mid-body during a CHUNKING transfer, followed by a final cleartext byte on the same TCP connection. This can lead to heap corruption. An unauthenticated network attacker exploiting this vulnerability could execute arbitrary code.	2026-05-12	9.8
CVE-2026-8043	ivanti - xtraction	External control of a file name in Ivanti Xtraction before version 2026.2 allows a remote authenticated attacker to read sensitive files and write arbitrary HTML files to a web directory, leading to information disclosure and possible client-side attacks.	2026-05-12	9.6
CVE-2026-34659	adobe - multiple products	Adobe Connect versions 2025.9.15, 2025.8.157 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	2026-05-12	9.6
CVE-2026-41615	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Microsoft Authenticator allows an unauthorized attacker to disclose information over a network.	2026-05-14	9.6
CVE-2026-8511	google - chrome	Use after free in UI in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-05-14	9.6
CVE-2026-8580	google - chrome	Use after free in Mojo in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	9.6
CVE-2026-6722	php - multiple products	In PHP versions 8.2.* before 8.2.31, 8.3.* before 8.3.31, 8.4.* before 8.4.21, and 8.5.* before 8.5.6, the SOAP extension's object deduplication mechanism stores pointers to PHP objects in a global map without incrementing their reference counts. When an apache:Map node contains duplicate keys, processing the second entry overwrites the first in the temporary result map, freeing the original PHP object while its stale pointer remains in the map. A subsequent href reference to the freed node can copy the dangling pointer into the result. As PHP string allocations can reclaim the freed memory region, an attacker with control over the SOAP request body can exploit this use-after-free to achieve remote code execution.	2026-05-10	9.5
CVE-2026-25786	siemens - multiple products	Affected devices do not properly validate and sanitize PLC/station name rendered on the "communication" parameters page of the web interface. This could allow an authenticated attacker who is authorized to download a TIA project into the product, to inject malicious scripts into the page. If a benign user with appropriate rights accesses the "communication" parameters page, the malicious code would be executed in the scope of their web session.	2026-05-12	9.3
CVE-2026-25787	siemens - multiple products	Affected devices do not properly validate and sanitize Technology Object (TO) name rendered on the "Motion Control Diagnostics" page of the web interface. This could allow an authenticated attacker who is authorized to download a TIA project into the product, to inject malicious scripts into the page. If a benign user with appropriate rights accesses the "Motion Control Diagnostics" parameters page, the malicious code would be executed in the scope of their web session.	2026-05-12	9.3
CVE-2026-41551	siemens - ROS#	A vulnerability has been identified in ROS# (All versions < V2.2.2). Affected versions contain a path traversal vulnerability because user input is not properly sanitized. This could allow a remote attacker to access arbitrary files on the device.	2026-05-12	9.3
CVE-2026-40379	microsoft - entra_id	Exposure of sensitive information to an unauthorized actor in Azure Entra ID allows an unauthorized attacker to perform spoofing over a network.	2026-05-12	9.3
CVE-2026-40402	microsoft - multiple products	Use after free in Windows Hyper-V allows an unauthorized attacker to elevate privileges locally.	2026-05-12	9.3
CVE-2026-34660	adobe - multiple products	Adobe Connect versions 2025.9.15, 2025.8.157 and earlier are affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to inject malicious scripts into a web page, potentially gaining elevated access or control over the victim's account or session. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	2026-05-12	9.3
CVE-2026-42945	f5 - multiple products	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_rewrite_module module. This vulnerability exists when the rewrite directive is followed by a rewrite, if, or set directive and an unnamed Perl-Compatible Regular Expression (PCRE) capture (for example, $1, $2) with a replacement string that includes a question mark (?). An unauthenticated attacker along with conditions beyond its control can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer overflow in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	9.2
CVE-2026-43515	apache - multiple products	Improper Authorization vulnerability when multiple method constraints define an HTTP method for the same extension in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.21, from 10.1.0-M1 through 10.1.54, from 9.0.0.M1 through 9.0.117, from 8.5.0 through 8.5.100, from 7.0.0 through 7.0.109. Users are recommended to upgrade to version 11.0.22, 10.1.55 or 9.0.118 which fix the issue.	2026-05-12	9.1

CVE-2026-33117	microsoft - azure_sdk_for_java	The Java Key Vault Keys library in the Azure SDK for Java contains an issue in the local cryptographic verification path where authentication tag comparison was implemented incorrectly. In affected applications that use the vulnerable local cryptography path, specially crafted encrypted input may bypass integrity verification checks. Operations delegated to the Key Vault service are not affected. The issue is addressed in version 4.10.6.	2026-05-12	9.1
CVE-2026-41103	microsoft - multiple products	Incorrect implementation of authentication algorithm in Microsoft SSO Plugin for Jira & Confluence allows an unauthorized attacker to elevate privileges over a network.	2026-05-12	9.1
CVE-2026-42833	microsoft - dynamics_365	Execution with unnecessary privileges in Microsoft Dynamics 365 (on-premises) allows an authorized attacker to execute code over a network.	2026-05-12	9.1
CVE-2025-40949	siemens - multiple products	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.17.1), RUGGEDCOM ROX MX5000RE (All versions < V2.17.1), RUGGEDCOM ROX RX1400 (All versions < V2.17.1), RUGGEDCOM ROX RX1500 (All versions < V2.17.1), RUGGEDCOM ROX RX1501 (All versions < V2.17.1), RUGGEDCOM ROX RX1510 (All versions < V2.17.1), RUGGEDCOM ROX RX1511 (All versions < V2.17.1), RUGGEDCOM ROX RX1512 (All versions < V2.17.1), RUGGEDCOM ROX RX1524 (All versions < V2.17.1), RUGGEDCOM ROX RX1536 (All versions < V2.17.1), RUGGEDCOM ROX RX5000 (All versions < V2.17.1). Affected devices do not properly sanitize user-supplied input in the Scheduler functionality of the Web UI, allowing commands to be injected into the task scheduling backend. This could allow an authenticated remote attacker to execute arbitrary commands with root privileges on the underlying operating system.	2026-05-12	8.9
CVE-2026-28847	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.5, iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-05-11	8.8
CVE-2026-28923	apple - multiple products	A logging issue was addressed with improved data redaction. This issue is fixed in macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. A malicious app may be able to break out of its sandbox.	2026-05-11	8.8
CVE-2026-28940	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5. Processing a maliciously crafted image may corrupt process memory.	2026-05-11	8.8
CVE-2026-28947	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in Safari 26.5, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2026-05-11	8.8
CVE-2026-28955	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.5, iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-05-11	8.8
CVE-2026-28978	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. A malicious app may be able to break out of its sandbox.	2026-05-11	8.8
CVE-2026-28995	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. A malicious app may be able to break out of its sandbox.	2026-05-11	8.8
CVE-2026-41489	pi-hole - pi-hole	Pi-hole is a DNS sinkhole that protects devices from unwanted content without installing any client-side software. From 6.0 to before Core 6.4.2 and FTL 6.6.1, two shell scripts executed as root by systemd (pihole-FTL-prestart.sh and pihole-FTL-poststop.sh) read the files.pid path from this config without validation and use it in privileged file operations (install and rm -f). By writing an arbitrary path into files.pid, an attacker with pihole privilege can cause root to delete and then recreate any file on the system outside the ProtectSystem=full-restricted directories, gaining write access to it. On a default Pi-hole installation this yields local privilege escalation to root via SSH authorized keys manipulation. If /root/.ssh/authorized_keys does not exist (default on fresh installs), only ExecStartPre is required. If the file exists, ExecStopPost deletes it first, and the same restart triggers both hooks in sequence. This vulnerability is fixed in Core 6.4.2 and FTL 6.6.1.	2026-05-11	8.8
CVE-2026-7256	zyxel - wre6505_firmware	** UNSUPPORTED WHEN ASSIGNED ** A command injection vulnerability in the CGI program of Zyxel WRE6505 v2 firmware version V1.00(ABDV.3)C0 could allow an adjacent attacker on the LAN to execute operating system (OS) commands on a vulnerable device by sending a crafted HTTP request.	2026-05-12	8.8
CVE-2026-22924	siemens - SIMATIC CN 4100	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V5.0). The affected application does not properly restrict unauthenticated connections and is susceptible to resource exhaustion conditions. This could allow an attacker to disrupt normal operations or perform unauthorized actions, potentially impacting system availability and integrity.	2026-05-12	8.8
CVE-2026-8111	ivanti - multiple products	SQL injection in the web console of Ivanti Endpoint Manager before version 2024 SU6 allows a remote authenticated attacker to achieve remote code execution.	2026-05-12	8.8
CVE-2025-43524	apple - multiple products	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.2. An app may be able to break out of its sandbox.	2026-05-12	8.8
CVE-2025-53844	fortinet - multiple products	A out-of-bounds write vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2.0 through 7.2.11 allows attacker to execute unauthorized code or commands via specially crafted packets.	2026-05-12	8.8
CVE-2026-33110	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-05-12	8.8
CVE-2026-33112	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-05-12	8.8
CVE-2026-34329	microsoft - multiple products	Heap-based buffer overflow in Windows Message Queuing allows an unauthorized attacker to execute code over an adjacent network.	2026-05-12	8.8
CVE-2026-35436	microsoft - multiple products	Insufficient granularity of access control in Microsoft Office Click-To-Run allows an authorized attacker to elevate privileges locally.	2026-05-12	8.8

CVE-2026-35439	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-05-12	8.8
CVE-2026-40357	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-05-12	8.8
CVE-2026-40365	microsoft - multiple products	Insufficient granularity of access control in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-05-12	8.8
CVE-2026-40370	microsoft - multiple products	External control of file name or path in SQL Server allows an authorized attacker to execute code over a network.	2026-05-12	8.8
CVE-2026-40403	microsoft - multiple products	Heap-based buffer overflow in Windows Win32K - GRFX allows an authorized attacker to execute code locally.	2026-05-12	8.8
CVE-2026-40420	microsoft - multiple products	Improper access control in Microsoft Office Click-To-Run allows an authorized attacker to elevate privileges locally.	2026-05-12	8.8
CVE-2026-41086	microsoft - windows_admin_center	Improper access control in Windows Admin Center allows an authorized attacker to elevate privileges over a network.	2026-05-12	8.8
CVE-2026-41094	microsoft - data_formulator	Improper control of generation of code ('code injection') in Microsoft Data Formulator allows an unauthorized attacker to execute code over a network.	2026-05-12	8.8
CVE-2026-41109	microsoft - visual_studio_code	Improper neutralization of special elements in output used by a downstream component ('injection') in GitHub Copilot and Visual Studio allows an unauthorized attacker to bypass a security feature over a network.	2026-05-12	8.8
CVE-2026-41613	microsoft - visual_studio_code	Session fixation in Visual Studio Code allows an unauthorized attacker to elevate privileges over a network.	2026-05-12	8.8
CVE-2026-23819	hewlett packard enterprise (hpe) - ArubaOS (AOS)	A vulnerability in the web-based management interface of Access Points running AOS-10 and AOS-8 Instant could allow an unauthenticated remote attacker to execute arbitrary JavaScript code in a victim's browser within the same local network. Successful exploitation could allow an attacker to compromise user data and potentially manipulate device configuration settings.	2026-05-12	8.8
CVE-2026-8509	google - chrome	Heap buffer overflow in WebML in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Critical)	2026-05-14	8.8
CVE-2026-8517	google - chrome	Object lifecycle issue in WebShare in Google Chrome on Mac prior to 148.0.7778.168 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-05-14	8.8
CVE-2026-8518	google - chrome	Use after free in Blink in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Critical)	2026-05-14	8.8
CVE-2026-8519	google - chrome	Integer overflow in ANGLE in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)	2026-05-14	8.8
CVE-2026-8522	google - chrome	Use after free in Downloads in Google Chrome on Mac prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-05-14	8.8
CVE-2026-8524	google - chrome	Out of bounds write in WebAudio in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.8
CVE-2026-8526	google - chrome	Out of bounds write in WebRTC in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.8
CVE-2026-8527	google - chrome	Insufficient validation of untrusted input in Downloads in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.8
CVE-2026-8529	google - chrome	Heap buffer overflow in Codecs in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted video file. (Chromium security severity: High)	2026-05-14	8.8
CVE-2026-8531	google - chrome	Heap buffer overflow in WebML in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.8
CVE-2026-8532	google - chrome	Integer overflow in XML in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.8
CVE-2026-8540	google - chrome	Type Confusion in V8 in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.8
CVE-2026-8544	google - chrome	Use after free in Media in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.8
CVE-2026-8549	google - chrome	Use after free in Media in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.8
CVE-2026-8551	google - chrome	Use after free in Downloads in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.8
CVE-2026-8555	google - chrome	Use after free in GTK in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.8
CVE-2026-8558	google - chrome	Out of bounds write in Fonts in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.8
CVE-2026-8577	google - chrome	Integer overflow in Fonts in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	8.8

CVE-2026-8581	google - chrome	Use after free in GPU in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	8.8
CVE-2026-8587	google - chrome	Use after free in Extensions in Google Chrome on Mac prior to 148.0.7778.168 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-05-14	8.8
CVE-2026-43490	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ksmbd: validate inherited ACE SID length smb_inherit_dacl() walks the parent directory DACL loaded from the security descriptor xattr. It verifies that each ACE contains the fixed SID header before using it, but does not verify that the variable-length SID described by sid.num_subauth is fully contained in the ACE. A malformed inheritable ACE can advertise more subauthorities than are present in the ACE. compare_sids() may then read past the ACE. smb_set_ace() also clamps the copied destination SID, but used the unchecked source SID count to compute the inherited ACE size. That could advance the temporary inherited ACE buffer pointer and nt_size accounting past the allocated buffer. Fix this by validating the parent ACE SID count and SID length before using the SID during inheritance. Compute the inherited ACE size from the copied SID so the size matches the bounded destination SID. Reject the inherited DACL if size accumulation would overflow smb_acl.size or the security descriptor allocation size.	2026-05-15	8.8
CVE-2025-40833	siemens - multiple products	The affected devices contain a null pointer dereference vulnerability while processing specially crafted IPv4 requests. This could allow an attacker to cause denial of service condition. A manual restart is required to recover the system.	2026-05-12	8.7
CVE-2026-22925	siemens - SIMATIC CN 4100	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V5.0). The affected application is susceptible to resource exhaustion when subjected to high volume of TCP SYN packets This could allow an attacker to render the service unavailable and cause denial-of-service conditions by overwhelming system resources.	2026-05-12	8.7
CVE-2026-33893	siemens - multiple products	A vulnerability has been identified in Teamcenter V2312 (All versions < V2312.0014), Teamcenter V2406 (All versions < V2406.0012), Teamcenter V2412 (All versions < V2412.0009), Teamcenter V2506 (All versions < V2506.0005), Teamcenter V2512 (All versions). The affected application contains hardcoded key which is used for obfuscation stored directly into the application. This could allow an attacker to obtain these keys and misuse them to gain unauthorized access.	2026-05-12	8.7
CVE-2026-34653	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in arbitrary file system read and write. An authenticated attacker with administrative privileges could exploit this vulnerability to read or write files outside the restricted directory. Exploitation of this issue does not require user interaction. Scope is changed.	2026-05-12	8.7
CVE-2026-34686	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 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, potentially gaining elevated access or control over the victim's account or session. Scope is changed.	2026-05-12	8.7
CVE-2026-8053	mongodb - multiple products	An issue in MongoDB Server's time-series collection implementation allows an authenticated user with database write privileges to trigger an out-of-bounds memory write in the mongod process. The issue results from an inconsistency in the internal field-name-to-index mapping within the time-series bucket catalog. Under certain conditions this can result in arbitrary code execution. This issue impacts MongoDB Server v5.0 versions prior to 5.0.33, v6.0 versions prior to 6.0.28, v7.0 versions prior to 7.0.34, v8.0 versions prior to 8.0.23, v8.2 versions prior to 8.2.9 and v8.3 versions prior to 8.3.2.	2026-05-13	8.7
CVE-2026-39455	f5 - BIG-IP	When the BIG-IP Configuration utility is configured to use Lightweight Directory Access Protocol (LDAP) authentication, undisclosed traffic can cause the httpd process to exhaust the available file descriptors. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.7
CVE-2026-39458	f5 - BIG-IP	When a BIG-IP DNS profile enabled with DNS cache is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.7
CVE-2026-40060	f5 - BIG-IP	When a BIG-IP Advanced WAF or ASM security policy is configured on a virtual server, undisclosed requests can cause the bd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.7
CVE-2026-40067	f5 - BIG-IP	When a BIG-IP APM access policy is configured on a virtual server, undisclosed traffic can cause the apmd process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.7
CVE-2026-40423	f5 - BIG-IP	When a SIP profile is configured on a virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate.	2026-05-13	8.7

		Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
CVE-2026-40618	f5 - multiple products	When an SSL profile is configured on a virtual server on BIG-IP Virtual Edition (VE) without Intel QuickAssist Technology (QAT) or on BIG-IP hardware platforms with the database variable crypto.hwacceleration set to disabled, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.7
CVE-2026-40629	f5 - multiple products	When SSL profiles are configured on a virtual server, undisclosed traffic can cause the virtual server to stop processing new client connections. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.7
CVE-2026-41218	f5 - BIG-IP	When BIG-IP PEM iRules are configured on a virtual server (iRules using commands starting with CLASSIFICATION::, CLASSIFY::, PEM::, PSC::, and the urlcatquery command), undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.7
CVE-2026-41227	f5 - BIG-IP	On an HTTP/2 virtual server with Layer 7 DoS Protection configured, undisclosed traffic can result in an increase in memory consumption causing the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.7
CVE-2026-41956	f5 - multiple products	When a classification profile is configured on a UDP virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.7
CVE-2026-41957	f5 - multiple products	An authenticated remote code execution vulnerability through undisclosed vectors exists in the BIG-IP and BIG-IQ Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.7
CVE-2026-42409	f5 - multiple products	When an HTTP/2 profile and an iRule containing the HTTP::redirect or HTTP::respond command are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) process to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.7
CVE-2026-42920	f5 - BIG-IP	When a Client SSL profile is configured with Allow Dynamic Record Sizing on a UDP virtual server, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.7
CVE-2026-6281	lenovo - multiple products	A potential vulnerability was reported in some Lenovo Personal Cloud Storage devices that could allow a remote authenticated user on the local network to execute arbitrary commands on the device.	2026-05-13	8.7
CVE-2025-10470	wso2 - identity_server	The Magic Link authentication flow accepts multiple invalid authentication requests without adequate rate limiting or resource control, leading to uncontrolled memory usage growth. This vulnerability can result in a denial-of-service condition, causing service unavailability for deployments that utilize the Magic Link authenticator. The impact is limited to these specific deployments and requires repeated invalid authentication attempts to trigger.	2026-05-11	8.6
CVE-2026-39459	f5 - BIG-IP	A vulnerability exists in iControl REST and the TMOS Shell (tmsh) where a highly privileged, authenticated attacker with at least the Manager role can create configuration objects that allow running arbitrary commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.6
CVE-2026-41225	f5 - BIG-IP	A vulnerability exists in iControl REST where a highly privileged, authenticated attacker with at least the Manager role can create configuration objects that allow running arbitrary commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.6
CVE-2026-6282	lenovo - multiple products	A potential improper file path validation vulnerability was reported in some Lenovo Personal Cloud Storage devices that could allow a remote authenticated user to move or access files belonging to other users on the same device.	2026-05-13	8.6
CVE-2026-20224	cisco - Cisco Catalyst SD-WAN Manager	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an unauthenticated, remote attacker to read arbitrary files that are stored in an affected system. The attacker does not need to have valid user credentials. This vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing an XML file. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to read arbitrary files that are stored in the affected system.	2026-05-14	8.6
CVE-2026-33862	siemens - multiple products	A vulnerability has been identified in Teamcenter V2312 (All versions < V2312.0014), Teamcenter V2406 (All versions < V2406.0012), Teamcenter V2412 (All versions < V2412.0009), Teamcenter V2506 (All versions < V2506.0005), Teamcenter V2512 (All versions). The affected application does not properly encode or filter user-supplied data. This could allow an attacker to inject malicious code that can be executed by other users when they visit the affected page.	2026-05-12	8.5
CVE-2026-20714	intel - quickassist_technology	Out-of-bounds write for some Intel(R) QAT software drivers for Windows before version 1.13 within Ring 3: User Applications may allow a escalation of privilege. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	2026-05-12	8.5
CVE-2026-20767	intel - quickassist_technology	Improper input validation for some Intel(R) QAT software drivers for Windows before version 1.13 within Ring 3: User Applications may allow an escalation of privilege. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable escalation of privilege. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential	2026-05-12	8.5

		vulnerability may impact the confidentiality (high), integrity (high) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.		
CVE-2026-32643	f5 - multiple products	A vulnerability exists in BIG-IP and BIG-IQ systems where a highly privileged, authenticated attacker with at least the Certificate Manager role can modify configuration objects that allow running arbitrary commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.5
CVE-2026-32673	f5 - BIG-IP	A vulnerability exists in BIG-IP scripted monitors that may allow an authenticated attacker with the Resource Administrator or Administrator role to execute arbitrary system commands with higher privileges. In appliance mode deployments, a successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.5
CVE-2026-34176	f5 - BIG-IP	When running in Appliance mode, an authenticated remote command injection vulnerability exists in an undisclosed iControl REST endpoint. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.5
CVE-2026-40061	f5 - BIG-IP	When BIG-IP DNS is provisioned, a vulnerability exists in an undisclosed iControl REST and BIG-IP TMOS Shell (tmsh) command that may allow an authenticated attacker with the Resource Administrator or Administrator role to execute arbitrary system commands with higher privileges. In Appliance mode deployments, a successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.5
CVE-2026-40631	f5 - BIG-IP	An authenticated attacker with the Resource Administrator or Administrator role can modify configuration objects through iControl SOAP resulting in privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.5
CVE-2026-40698	f5 - multiple products	A vulnerability exists in BIG-IP and BIG-IQ systems where a highly privileged, authenticated attacker with at least the Resource Administrator role can create SNMP configuration objects through iControl REST or the TMOS shell (tmsh) resulting in privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.5
CVE-2026-41953	f5 - BIG-IP	A vulnerability exists in BIG-IP systems where a highly privileged, authenticated attacker with at least the Resource Administrator role can modify configuration objects resulting in privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.5
CVE-2026-42406	f5 - multiple products	A vulnerability exists in BIG-IP and BIG-IQ systems where a highly privileged, authenticated attacker with at least the Certificate Manager role can modify configuration objects that allow running arbitrary commands. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.5
CVE-2026-42924	f5 - BIG-IP	An authenticated attacker with the Resource Administrator or Administrator role can create SNMP configuration objects through iControl SOAP resulting in privilege escalation. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.5
CVE-2026-42930	f5 - BIG-IP	When running in Appliance mode, an authenticated attacker assigned the 'Administrator' role may be able to bypass Appliance mode restrictions on a BIG-IP system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.5
CVE-2026-40358	microsoft - multiple products	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-05-12	8.4
CVE-2026-40361	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-05-12	8.4
CVE-2026-40363	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-05-12	8.4
CVE-2026-40364	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-05-12	8.4
CVE-2026-40366	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-05-12	8.4
CVE-2026-40367	microsoft - multiple products	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-05-12	8.4
CVE-2026-41964	huawei - HarmonyOS	Permission control vulnerability in the web. Impact: Successful exploitation of this vulnerability may affect availability.	2026-05-15	8.4
CVE-2026-35438	microsoft - Windows Admin Center	Missing authorization in Windows Admin Center allows an authorized attacker to elevate privileges over a network.	2026-05-12	8.3
CVE-2026-41217	f5 - BIG-IP	A vulnerability exists in an undisclosed BIG-IP TMOS Shell (tmsh) command that may allow an authenticated attacker with resource administrator or administrator role to execute arbitrary system commands with higher privileges. In Appliance mode deployments, a successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.3
CVE-2026-42946	f5 - multiple products	A vulnerability exists in the ngx_http_scgi_module and ngx_http_uwsgi_module modules that may result in excessive memory allocation or an over-read of data. When scgi_pass or uwsgi_pass is configured, an unauthenticated attacker with man-in-the-middle (MITM) ability to control responses from an upstream server may be able to read the memory of the NGINX worker process or restart it. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	8.3
CVE-2026-8512	google - chrome	Use after free in FileSystem in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-05-14	8.3

CVE-2026-8513	google - chrome	Use after free in Input in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-05-14	8.3
CVE-2026-8514	google - chrome	Use after free in Aura in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-05-14	8.3
CVE-2026-8515	google - chrome	Use after free in HID in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-05-14	8.3
CVE-2026-8520	google - chrome	Race in Payments in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-05-14	8.3
CVE-2026-8523	google - chrome	Use after free in Mojo in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.3
CVE-2026-8525	google - chrome	Heap buffer overflow in ANGLE in Google Chrome on Mac prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.3
CVE-2026-8530	google - chrome	Use after free in Network in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.3
CVE-2026-8533	google - chrome	Use after free in Accessibility in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.3
CVE-2026-8534	google - chrome	Integer overflow in GPU in Google Chrome on Linux and ChromeOS prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.3
CVE-2026-8542	google - chrome	Use after free in Core in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.3
CVE-2026-8548	google - chrome	Out of bounds write in Media in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-05-14	8.3
CVE-2026-8569	google - chrome	Out of bounds write in Codecs in Google Chrome on Mac prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: Medium)	2026-05-14	8.3
CVE-2026-8571	google - chrome	Insufficient policy enforcement in GPU in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	8.3
CVE-2026-8573	google - chrome	Integer overflow in Codecs in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: Medium)	2026-05-14	8.3
CVE-2026-8574	google - chrome	Use after free in Core in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	8.3
CVE-2026-8575	google - chrome	Use after free in UI in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	8.3
CVE-2026-41713	vmware - multiple products	A malicious user could craft input that is stored in conversation memory and later interpreted by the model in an unintended way. Applications using the affected advisor with user-controlled input may be susceptible to manipulation of model behavior across conversation turns.	2026-05-12	8.2
CVE-2026-35071	dell - insightiq	Dell PowerScale InsightIQ, versions 6.0.0 through 6.2.0, contains 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.	2026-05-12	8.2
CVE-2026-33833	microsoft - Azure Machine Learning	Improper neutralization of special elements in output used by a downstream component ('injection') in Azure Machine Learning allows an unauthorized attacker to perform spoofing over a network.	2026-05-12	8.2
CVE-2026-28907	apple - multiple products	The issue was addressed with improved input validation. This issue is fixed in Safari 26.5, iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.	2026-05-11	8.1
CVE-2026-40415	microsoft - multiple products	Use after free in Windows TCP/IP allows an unauthorized attacker to execute code over a network.	2026-05-12	8.1
CVE-2026-42897	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	2026-05-14	8.1
CVE-2026-35194	apache - multiple products	Code injection in SQL code generation in Apache Flink 1.15.0 through 1.20.x and 2.0.0 through 2.x allows authenticated users with query submission privileges to execute arbitrary code on TaskManagers via maliciously crafted SQL queries. The vulnerability affects JSON functions (1.15.0+) and LIKE expressions with ESCAPE clauses (1.17.0+). User-controlled strings are interpolated into generated Java code without proper escaping, allowing attackers to break out of string literals and inject arbitrary expressions. Users are recommended to upgrade to either version 1.20.4, 2.0.2, 2.1.2 or 2.2.1, which fixes this issue.	2026-05-15	8.1
CVE-2026-32658	dell - automation_platform	Dell Automation Platform versions prior to 2.0.0.0, contains a missing authorization vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-05-11	8

CVE-2026-4802	red hat - multiple products	A flaw was found in Cockpit. This vulnerability allows a remote attacker to achieve arbitrary command execution on the host by exploiting unsanitized user-controlled parameters within crafted links in the system logs user interface (UI). An attacker can inject shell metacharacters and command substitutions into these parameters, leading to the execution of arbitrary shell commands on the affected system. This could result in a complete system compromise.	2026-05-11	8
CVE-2026-34332	microsoft - windows_server_2025	Use after free in Windows Kernel-Mode Drivers allows an authorized attacker to execute code over a network.	2026-05-12	8
CVE-2026-40368	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-05-12	8
CVE-2026-43500	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: rxrpc: Also unshare DATA/RESPONSE packets when paged frags are present The DATA-packet handler in rxrpc_input_call_event() and the RESPONSE handler in rxrpc_verify_response() copy the skb to a linear one before calling into the security ops only when skb_cloned() is true. An skb that is not cloned but still carries externally-owned paged fragments (e.g. SKBFL_SHARED_FRAG set by splice() into a UDP socket via __ip_append_data, or a chained skb_has_frag_list()) falls through to the in-place decryption path, which binds the frag pages directly into the AEAD/skcipher SGL via skb_to_sgvec(). Extend the gate to also unshare when skb_has_frag_list() or skb_has_shared_frag() is true. This catches the splice-loopback vector and other externally-shared frag sources while preserving the zero-copy fast path for skbs whose frags are kernel-private (e.g. NIC page_pool RX, GRO). The OOM/trace handling already in place is reused.	2026-05-11	7.8
CVE-2026-28840	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.4. An app may be able to gain root privileges.	2026-05-11	7.8
CVE-2026-28915	apple - multiple products	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. An app may be able to gain root privileges.	2026-05-11	7.8
CVE-2026-28919	apple - multiple products	A consistency issue was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. An app may be able to gain root privileges.	2026-05-11	7.8
CVE-2026-28951	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. An app may be able to gain root privileges.	2026-05-11	7.8
CVE-2026-7432	ivanti - multiple products	A race condition in Ivanti Secure Access Client before 22.8R6 allows a locally authenticated user to escalate privileges to SYSTEM	2026-05-12	7.8
CVE-2026-8110	ivanti - multiple products	Incorrect permissions assignment in the agent of Ivanti Endpoint Manager before version 2024 SU6 allows a local authenticated attacker to escalate their privileges.	2026-05-12	7.8
CVE-2026-32204	microsoft - Azure Monitor	External control of file name or path in Azure Monitor Agent allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-33834	microsoft - multiple products	Improper access control in Windows Event Logging Service allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-33835	microsoft - multiple products	Use after free in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-33837	microsoft - multiple products	Heap-based buffer overflow in Windows TCP/IP allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-33838	microsoft - multiple products	Double free in Windows Message Queuing allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-33840	microsoft - multiple products	Use after free in Windows Win32K - ICOMP allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-33841	microsoft - multiple products	Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-34330	microsoft - multiple products	Integer overflow or wraparound in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-34333	microsoft - multiple products	Use after free in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-34334	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows TCP/IP allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-34336	microsoft - multiple products	Buffer over-read in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-34337	microsoft - multiple products	Use after free in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-34338	microsoft - multiple products	Use after free in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-34343	microsoft - multiple products	Heap-based buffer overflow in Windows Application Identity (AppID) Subsystem allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-34344	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-34351	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows TCP/IP allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-34636	adobe - multiple products	Premiere Pro versions 26.0.2, 25.6.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8

CVE-2026-34637	adobe - multiple products	Premiere Pro versions 26.0.2, 25.6.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34638	adobe - multiple products	Premiere Pro versions 26.0.2, 25.6.4 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34639	adobe - multiple products	Media Encoder versions 26.0.2, 25.6.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34640	adobe - multiple products	Media Encoder versions 26.0.2, 25.6.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34642	adobe - multiple products	After Effects versions 26.0, 25.6.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34643	adobe - multiple products	After Effects versions 26.0, 25.6.4 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34644	adobe - multiple products	After Effects versions 26.0, 25.6.4 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34661	adobe - multiple products	Illustrator versions 29.8.6, 30.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34675	adobe - substance_3d_painter	Substance3D - Painter versions 12.0.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34676	adobe - substance_3d_painter	Substance3D - Painter versions 12.0.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34687	adobe - multiple products	Illustrator versions 29.8.6, 30.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-35415	microsoft - multiple products	Integer overflow or wraparound in Windows Storage Spaces Controller allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-35417	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Win32K - ICOMP allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-35418	microsoft - multiple products	Use after free in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-35420	microsoft - multiple products	Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-35421	microsoft - multiple products	Heap-based buffer overflow in Windows GDI allows an unauthorized attacker to execute code locally.	2026-05-12	7.8
CVE-2026-40359	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-05-12	7.8
CVE-2026-40360	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-05-12	7.8
CVE-2026-40362	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-05-12	7.8
CVE-2026-40369	microsoft - multiple products	Untrusted pointer dereference in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-40377	microsoft - multiple products	Heap-based buffer overflow in Windows Cryptographic Services allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-40381	microsoft - azure_connected_machine_agent	Improper access control in Azure Connected Machine Agent allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-40382	microsoft - multiple products	Use after free in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-40397	microsoft - multiple products	Integer underflow (wrap or wraparound) in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-40398	microsoft - multiple products	Heap-based buffer overflow in Windows Remote Desktop allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-40399	microsoft - multiple products	Stack-based buffer overflow in Windows TCP/IP allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-40407	microsoft - multiple products	Heap-based buffer overflow in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-40408	microsoft - multiple products	Use after free in Windows Kernel-Mode Drivers allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-40417	microsoft - multiple products	Weak authentication in Dynamics Business Central allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-40418	microsoft - multiple products	Use after free in Microsoft Office Click-To-Run allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-40419	microsoft - multiple products	Use after free in Microsoft Office allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-41088	microsoft - multiple products	External control of file name or path in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-41095	microsoft - multiple products	Use after free in Data Deduplication allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8

CVE-2026-41611	microsoft - visual_studio_code	Improper neutralization of script-related html tags in a web page (basic xss) in Visual Studio Code allows an unauthorized attacker to execute code locally.	2026-05-12	7.8
CVE-2026-42831	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-05-12	7.8
CVE-2026-42896	microsoft - multiple products	Integer overflow or wraparound in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-05-12	7.8
CVE-2026-34681	adobe - substance_3d_designer	Substance3D - Designer versions 15.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34682	adobe - substance_3d_designer	Substance3D - Designer versions 15.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34683	adobe - substance_3d_designer	Substance3D - Designer versions 15.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34684	adobe - substance_3d_designer	Substance3D - Designer versions 15.1.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-34690	adobe - multiple products	After Effects versions 26.0, 25.6.4 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	7.8
CVE-2026-43476	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: iio: chemical: sps30_i2c: fix buffer size in sps30_i2c_read_meas() sizeof(num) evaluates to sizeof(size_t) (8 bytes on 64-bit) instead of the intended __be32 element size (4 bytes). Use sizeof(*meas) to correctly match the buffer element type.	2026-05-13	7.8
CVE-2026-43481	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net-shapers: don't free reply skb after genlmsg_reply() genlmsg_reply() hands the reply skb to netlink, and netlink_unicast() consumes it on all return paths, whether the skb is queued successfully or freed on an error path. net_shaper_nl_get_doit() and net_shaper_nl_cap_get_doit() currently jump to free_msg after genlmsg_reply() fails and call nlmsg_free(msg), which can hit the same skb twice. Return the genlmsg_reply() error directly and keep free_msg only for pre-reply failures.	2026-05-13	7.8
CVE-2026-41702	vmware - fusion	VMware Fusion contains a TOCTOU (Time-of-check Time-of-use) vulnerability that occurs during an operation performed by a SETUID binary. A malicious actor with local non-administrative user privileges may exploit this vulnerability to escalate privileges to root on the system where Fusion is installed.	2026-05-15	7.8
CVE-2025-40947	siemens - multiple products	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.17.1), RUGGEDCOM ROX MX5000RE (All versions < V2.17.1), RUGGEDCOM ROX RX1400 (All versions < V2.17.1), RUGGEDCOM ROX RX1500 (All versions < V2.17.1), RUGGEDCOM ROX RX1501 (All versions < V2.17.1), RUGGEDCOM ROX RX1510 (All versions < V2.17.1), RUGGEDCOM ROX RX1511 (All versions < V2.17.1), RUGGEDCOM ROX RX1512 (All versions < V2.17.1), RUGGEDCOM ROX RX1524 (All versions < V2.17.1), RUGGEDCOM ROX RX1536 (All versions < V2.17.1), RUGGEDCOM ROX RX5000 (All versions < V2.17.1). Affected devices do not properly sanitize user-supplied input during the feature key installation process. This could allow an authenticated remote attacker to inject arbitrary commands, resulting in remote code execution with root privileges on the underlying operating system.	2026-05-12	7.7
CVE-2026-33821	microsoft - dynamics_365_customer_insights	Improper privilege management in Microsoft Dynamics 365 Customer Insights allows an authorized attacker to elevate privileges over a network.	2026-05-12	7.7
CVE-2026-42832	microsoft - multiple products	Improper access control in Microsoft Office allows an unauthorized attacker to perform spoofing locally.	2026-05-12	7.7
CVE-2026-8336	mongodb - multiple products	After invoking $_internalJsEmit, which is not intended to be directly accessible, or mapreduce command's map function in a certain way, an authenticated user can subsequently crash mongod when the server-side JavaScript engine (through $where, $function, mapreduce reduce stage, etc.) is used also in a specific way, resulting in a post-authentication denial-of-service. This issue impacts MongoDB Server v8.2 versions prior to 8.2.9 and v8.3 versions prior to 8.3.2.	2026-05-13	7.7
CVE-2026-28846	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. A remote attacker may be able to cause unexpected app termination.	2026-05-11	7.5
CVE-2026-28848	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.7, macOS Tahoe 26.5. A remote attacker may be able to cause unexpected system termination.	2026-05-11	7.5
CVE-2026-28860	apple - multiple products	The issue was addressed with improved input validation. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4, macOS Sequoia 15.7.5, macOS Sonoma 14.8.5, macOS Tahoe 26.4,	2026-05-11	7.5

		tvOS 26.4, visionOS 26.4, watchOS 26.4. A local attacker may be able to modify the state of the Keychain.		
CVE-2026-28872	apple - multiple products	A resource exhaustion issue was addressed with improved input validation. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.4 and iPadOS 26.4. A remote attacker may be able to cause a denial-of-service.	2026-05-11	7.5
CVE-2026-28873	apple - multiple products	This issue was addressed with additional entitlement checks. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.4 and iPadOS 26.4. An app may be able to circumvent App Privacy Report logging.	2026-05-11	7.5
CVE-2026-28883	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in Safari 26.5, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-05-11	7.5
CVE-2026-28904	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.5, iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-05-11	7.5
CVE-2026-28905	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.5, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-05-11	7.5
CVE-2026-28906	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, visionOS 26.5. An attacker may be able to track users through their IP address.	2026-05-11	7.5
CVE-2026-28908	apple - multiple products	A denial of service issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. An app may be able to modify protected parts of the file system.	2026-05-11	7.5
CVE-2026-28913	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.5, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, watchOS 26.5. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-05-11	7.5
CVE-2026-28924	apple - multiple products	A race condition was addressed with improved handling of symbolic links. This issue is fixed in macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. An app may be able to access Contacts without user consent.	2026-05-11	7.5
CVE-2026-28925	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. An app may be able to cause unexpected system termination or write kernel memory.	2026-05-11	7.5
CVE-2026-28929	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. Replying to an email could display remote images in Mail in Lockdown Mode.	2026-05-11	7.5
CVE-2026-28930	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26.5. An app may be able to access protected user data.	2026-05-11	7.5
CVE-2026-28936	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sonoma 14.8.7, macOS Tahoe 26.5, visionOS 26.5. Processing a maliciously crafted file may lead to unexpected app termination.	2026-05-11	7.5
CVE-2026-28943	apple - multiple products	A logging issue was addressed with improved data redaction. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, watchOS 26.5. An app may be able to determine kernel memory layout.	2026-05-11	7.5
CVE-2026-28944	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.5, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, visionOS 26.5. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-05-11	7.5
CVE-2026-28952	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. An app may be able to cause unexpected system termination.	2026-05-11	7.5
CVE-2026-28953	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.5, iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-05-11	7.5
CVE-2026-28954	apple - multiple products	A file quarantine bypass was addressed with additional checks. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. A maliciously crafted disk image may bypass Gatekeeper checks.	2026-05-11	7.5
CVE-2026-28959	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. An app may be able to cause unexpected system termination.	2026-05-11	7.5
CVE-2026-28962	apple - multiple products	This issue was addressed with improved access restrictions. This issue is fixed in Safari 26.5, iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, visionOS 26.5. Processing maliciously crafted web content may disclose sensitive user information.	2026-05-11	7.5
CVE-2026-28964	apple - multiple products	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 26.5 and iPadOS 26.5, visionOS 26.5. An app may be able to access sensitive user data.	2026-05-11	7.5
CVE-2026-28965	apple - multiple products	A privacy issue was addressed with improved checks. This issue is fixed in iOS 26.5 and iPadOS 26.5. A user may be able to view restricted content from the lock screen.	2026-05-11	7.5
CVE-2026-28969	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. An app may be able to cause unexpected system termination.	2026-05-11	7.5
CVE-2026-28974	apple - multiple products	This issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. An app may be able to cause a denial-of-service.	2026-05-11	7.5
CVE-2026-28976	apple - macos	An information leakage was addressed with additional validation. This issue is fixed in macOS Tahoe 26.5. An app may be able to gain root privileges.	2026-05-11	7.5

CVE-2026-28983	apple - multiple products	A type confusion issue was addressed with improved checks. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. A remote attacker may be able to cause a denial of service.	2026-05-11	7.5
CVE-2026-28986	apple - multiple products	A race condition was addressed with additional validation. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, watchOS 26.5. An app may be able to cause unexpected system termination.	2026-05-11	7.5
CVE-2026-28987	apple - multiple products	A logging issue was addressed with improved data redaction. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, watchOS 26.5. An app may be able to leak sensitive kernel state.	2026-05-11	7.5
CVE-2026-28990	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing a maliciously crafted image may corrupt process memory.	2026-05-11	7.5
CVE-2026-28991	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. An app may be able to cause a denial-of-service.	2026-05-11	7.5
CVE-2026-39870	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. Processing a maliciously crafted image may corrupt process memory.	2026-05-11	7.5
CVE-2026-39871	apple - multiple products	A path handling issue was addressed with improved logic. This issue is fixed in macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. An app may be able to observe unprotected user data.	2026-05-11	7.5
CVE-2026-43652	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26.5. An app may be able to access protected user data.	2026-05-11	7.5
CVE-2026-43654	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. An app may be able to disclose kernel memory.	2026-05-11	7.5
CVE-2026-43658	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.5, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2026-05-11	7.5
CVE-2026-43660	apple - multiple products	A validation issue was addressed with improved logic. This issue is fixed in Safari 26.5, iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.	2026-05-11	7.5
CVE-2026-43661	apple - multiple products	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, watchOS 26.5. Processing a maliciously crafted image may corrupt process memory.	2026-05-11	7.5
CVE-2026-43668	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory.	2026-05-11	7.5
CVE-2026-7287	zyxel - nwa1100-n_firmware	** UNSUPPORTED WHEN ASSIGNED ** A buffer overflow vulnerability in the formWep(), formWlAc(), formPasswordSetup(), formUpgradeCert(), and formDelcert() functions of the “webs” binary in Zyxel NWA1100-N customized firmware version 1.00(AACE.1)C0 could allow an attacker to trigger a denial-of-service (DoS) condition by sending a crafted HTTP request to a vulnerable device.	2026-05-12	7.5
CVE-2026-41712	vmware - multiple products	Spring AI's chat memory component contained a problematic default that, when not explicitly overridden, could result in unintended data exposure between users.	2026-05-12	7.5
CVE-2026-41284	apache - multiple products	Allocation of Resources Without Limits or Throttling vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.21, from 10.1.0-M1 through 10.1.54, from 9.0.0.M1 through 9.0.117. Older, unsupported versions may also be affected. Users are recommended to upgrade to version [FIXED_VERSION], which fixes the issue.	2026-05-12	7.5
CVE-2026-43513	apache - multiple products	Improper Handling of Case Sensitivity vulnerability in LockOutRealm in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.21, from 10.1.0-M1 through 10.1.54, from 9.0.0.M1 through 9.0.117, from 8.5.0 through 8.5.100, from 7.0.0 through 7.0.109. Older unsupported versions may also be affected. Users are recommended to upgrade to version 11.0.22, 10.1.55 or 9.0.118 which fix the issue.	2026-05-12	7.5
CVE-2025-46311	apple - multiple products	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 18.7.3 and iPadOS 18.7.3, iOS 26.2 and iPadOS 26.2. An app may be able to access sensitive user data.	2026-05-12	7.5
CVE-2026-32161	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Native WiFi Miniport Driver allows an unauthorized attacker to execute code over an adjacent network.	2026-05-12	7.5
CVE-2026-35424	microsoft - multiple products	Missing release of memory after effective lifetime in Windows Internet Key Exchange (IKE) Protocol allows an unauthorized attacker to deny service over a network.	2026-05-12	7.5
CVE-2026-40405	microsoft - multiple products	Null pointer dereference in Windows TCP/IP allows an unauthorized attacker to deny service over a network.	2026-05-12	7.5
CVE-2026-40406	microsoft - multiple products	Use after free in Windows TCP/IP allows an unauthorized attacker to disclose information over a network.	2026-05-12	7.5
CVE-2026-42899	microsoft - multiple products	Loop with unreachable exit condition ('infinite loop') in ASP.NET Core allows an unauthorized attacker to deny service over a network.	2026-05-12	7.5
CVE-2026-23824	arubanetworks - multiple products	Vulnerabilities exist in a protocol-handling component of AOS-8 and AOS-10 Operating Systems. An unauthenticated attacker could exploit these vulnerabilities by sending specially crafted network messages to the affected service. Due to insufficient input validation, successful exploitation may terminate a critical system process, resulting in a denial-of-service condition.	2026-05-12	7.5

CVE-2026-23825	arubanetworks - multiple products	Vulnerabilities exist in a protocol-handling component of AOS-8 and AOS-10 Operating Systems. An unauthenticated attacker could exploit these vulnerabilities by sending specially crafted network messages to the affected service. Due to insufficient input validation, successful exploitation may terminate a critical system process, resulting in a denial-of-service condition.	2026-05-12	7.5
CVE-2026-23826	arubanetworks - multiple products	A vulnerability in a network management service of AOS-8 Operating System could allow an unauthenticated remote attacker to exploit this vulnerability by sending specially crafted network packets to the affected device, potentially resulting in a denial-of-service condition. Successful exploitation could cause the affected service process to terminate unexpectedly, disrupting normal device operations.	2026-05-12	7.5
CVE-2026-23827	arubanetworks - multiple products	A heap-based buffer overflow vulnerability exists in a Network management service of AOS-8 and AOS-10 that could allow an unauthenticated remote attacker to achieve remote code execution. Successful exploitation could allow an unauthenticated attacker to execute arbitrary code as a privileged user on the underlying operating system, potentially leading to a system compromise. Exploitation may also result in a denial-of-service (DoS) condition affecting the impacted system process.	2026-05-12	7.5
CVE-2026-34645	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier are affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue does not require user interaction.	2026-05-12	7.5
CVE-2026-34646	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier are affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue does not require user interaction.	2026-05-12	7.5
CVE-2026-34648	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	7.5
CVE-2026-34649	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	7.5
CVE-2026-34650	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	7.5
CVE-2026-34651	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	7.5
CVE-2026-34652	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier are affected by a Dependency on Vulnerable Third-Party Component vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	7.5
CVE-2026-34665	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	7.5
CVE-2026-8510	google - chrome	Integer overflow in Skia in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Critical)	2026-05-14	7.5
CVE-2026-8521	google - chrome	Use after free in Tab Groups in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: Critical)	2026-05-14	7.5
CVE-2026-8547	google - chrome	Insufficient policy enforcement in Passwords in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: High)	2026-05-14	7.5
CVE-2026-8557	google - chrome	Use after free in Accessibility in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: High)	2026-05-14	7.5
CVE-2026-8585	google - chrome	Inappropriate implementation in Media in Google Chrome on iOS prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	7.5
CVE-2025-14179	php - multiple products	In PHP versions 8.2.* before 8.2.31, 8.3.* before 8.3.31, 8.4.* before 8.4.21, and 8.5.* before 8.5.6, the PDO Firebird driver improperly handles NUL bytes when preparing SQL queries. During token-by-token query construction, a string token containing a NUL byte is copied via strncat(), which stops at the NUL byte, dropping the closing quote and causing subsequent SQL tokens to be interpreted as part of the string. This allows SQL injection when attacker-controlled values are quoted via PDO::quote() and embedded in SQL statements.	2026-05-10	7.4
CVE-2026-40413	microsoft - multiple products	Null pointer dereference in Windows TCP/IP allows an unauthorized attacker to deny service over an adjacent network.	2026-05-12	7.4
CVE-2026-40414	microsoft - multiple products	Null pointer dereference in Windows TCP/IP allows an unauthorized attacker to deny service over an adjacent network.	2026-05-12	7.4
CVE-2026-41107	microsoft - edge_chromium	External control of file name or path in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	2026-05-12	7.4

CVE-2026-42893	microsoft - outlook	Improper neutralization of special elements used in a command ('command injection') in M365 Copilot allows an unauthorized attacker to perform tampering over a network.	2026-05-12	7.4
CVE-2026-34647	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	2026-05-12	7.4
CVE-2026-33376	grafana - Grafana OSS	When using an IPv6 allow-list for the Auth Proxy feature, it defaults to /32 addresses. Addresses specifying a mask explicitly are not affected; to mitigate easily, add the desired mask (usually /128) to the addresses. Only auth proxy is affected; Okta, SAML, LDAP, etc are unaffected here.	2026-05-13	7.4
CVE-2026-45539	microsoft - apm	Microsoft APM is an open-source, community-driven dependency manager for AI agents. From 0.5.4 to 0.12.4, two primitive integrators in apm-cli enumerate package files with bare Path.glob() / Path.rglob() calls and read each match with Path.read_text(), transparently following symbolic links. A symlink committed inside a remote APM dependency under .apm/prompts/<x>.prompt.md or .apm/agents/<x>.agent.md is preserved verbatim into apm_modules/ on clone and then dereferenced during integration, with the resolved content written as a regular file into the project's deploy directories. The package content_hash, the pre-deploy SecurityGate scan, and apm audit do not flag this. The deploy roots are not added to the auto-generated .gitignore, so the resulting files are staged by git add by default. This vulnerability is fixed in 0.13.0.	2026-05-15	7.4
CVE-2026-6735	php - multiple products	In PHP versions 8.2.* before 8.2.31, 8.3.* before 8.3.31, 8.4.* before 8.4.21, 8.5.* before 8.5.6, due to improper sanitation of user data, it allows an attacker to compose an URL, which will cause the target to execute arbitrary JavaScript code (XSS) on the target's machine when the target is viewing the PHP-FPM status page.	2026-05-10	7.3
CVE-2025-10908	wso2 - multiple products	Due to a lack of user account state validation during authentication, locked user accounts can be successfully authenticated using Magic Link or Pass Key methods. This bypasses the intended security control that should prevent access to accounts that have been locked. This vulnerability may allow unauthorized access to applications and sensitive data associated with accounts that should have been restricted via the account lock mechanism. It also undermines the effectiveness of the account lock mechanism intended to prevent further login attempts.	2026-05-11	7.3
CVE-2026-43655	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, watchOS 26.5. An app may be able to cause unexpected system termination or read kernel memory.	2026-05-11	7.3
CVE-2026-43656	apple - multiple products	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. Parsing a maliciously crafted file may lead to an unexpected app termination.	2026-05-11	7.3
CVE-2026-44411	siemens - Solid Edge SE2026	A vulnerability has been identified in Solid Edge SE2026 (All versions < V226.0 Update 5). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted PAR files. An attacker could leverage this vulnerability to execute code in the context of the current process.	2026-05-12	7.3
CVE-2026-44412	siemens - Solid Edge SE2026	A vulnerability has been identified in Solid Edge SE2026 (All versions < V226.0 Update 5). The affected applications contain a stack based overflow vulnerability while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process.	2026-05-12	7.3
CVE-2025-12659	siemens - Simcenter Femap	The affected applications contains a memory corruption vulnerability while parsing specially crafted IPT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-27349, ZDI-CAN-27389)	2026-05-12	7.3
CVE-2026-8389	mozilla - firefox	JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability was fixed in Firefox 150.0.3.	2026-05-12	7.3
CVE-2026-8390	mozilla - firefox	Use-after-free in the JavaScript: WebAssembly component. This vulnerability was fixed in Firefox 150.0.3.	2026-05-12	7.3
CVE-2026-42498	apache - multiple products	Exposure of HTTP Authentication Header to unexpected hosts during WebSocket authentication vulnerability in Apache Tomcat. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.21, from 10.1.0-M1 through 10.1.54, from 9.0.2 through 9.0.117, from 8.5.24 through 8.5.100, from 7.0.83 through 7.0.109. Users are recommended to upgrade to version 11.0.22, 10.1.55 or 9.0.118, which fix the issue.	2026-05-12	7.3
CVE-2026-32177	microsoft - multiple products	Heap-based buffer overflow in .NET allows an unauthorized attacker to elevate privileges locally.	2026-05-12	7.3
CVE-2026-35433	microsoft - multiple products	Improper input validation in .NET allows an unauthorized attacker to elevate privileges locally.	2026-05-12	7.3
CVE-2025-40946	siemens - multiple products	A vulnerability has been identified in blueplanet 100 NX3 M8 (All versions), blueplanet 100 TL3 GEN2 (All versions < V6.1.4.9), blueplanet 105 TL3 (All versions), blueplanet 105 TL3 GEN2 (All versions < V6.1.4.9), blueplanet 110 TL3 (All versions), blueplanet 125 NX3 M11 (All versions), blueplanet 125 TL3 (All versions), blueplanet 125 TL3 GEN2 (All versions < V6.1.4.9), blueplanet 137 TL3 (All versions), blueplanet 150 TL3 (All versions), blueplanet 150 TL3 GEN2 (All versions < V6.1.4.9), blueplanet 155 TL3 (All versions), blueplanet 155 TL3 GEN2 (All versions < V6.1.4.9), blueplanet 165 TL3 (All versions), blueplanet 165 TL3 GEN2 (All versions < V6.1.4.9), blueplanet 25.0 NX3-33.0 NX3 (All versions), blueplanet 3.0 NX3-20.0 NX3 (All versions), blueplanet 3.0 TL3-60.0 TL3 (All versions), blueplanet 3.0-5.0 NX1 (All versions), blueplanet 360 NX3 M6 (All versions), blueplanet 50.0 NX3-60.0 NX3 (All versions), blueplanet 87.0 TL3 (All versions), blueplanet 87.0 TL3 GEN2 (All versions < V6.1.4.9), blueplanet 92.0 TL3 (All versions), blueplanet 92.0 TL3 GEN2 (All versions < V6.1.4.9), blueplanet gridsafe 110 TL3-S (All versions < V3.91), blueplanet gridsafe 137 TL3-S (All versions < V3.91), blueplanet gridsafe 92.0 TL3-S (All versions < V3.91), blueplanet hybrid 10.0 TL3 (All versions), blueplanet hybrid 6.0 NH3-12.0 NH3 (All versions). A CRC16-based algorithm	2026-05-12	7.2

		for generating Technical Service credentials could allow an attacker to derive the credentials from the devices serial number and misuse them to gain unauthorized access.		
CVE-2026-25789	siemens - multiple products	Affected devices do not properly validate and sanitize filenames on the Firmware Update page. This could allow a remote attacker to social engineer the user into selecting the modified firmware file to be uploaded. This would result in malitcious JavaScript execution in the context of the authenticated user's session without requiring the file to be uploaded, potentially leading to session hijacking or credential theft.	2026-05-12	7.2
CVE-2026-8051	ivanti - multiple products	OS command injection in Ivanti Virtual Traffic Manager before version 22.9r4 allows a remote authenticated attacker with admin privileges to achieve remote code execution.	2026-05-12	7.2
CVE-2025-53681	fortinet - multiple products	An improper neutralization of special elements used in an SQL Command ("SQL Injection&") vulnerability [CWE-89] vulnerability in Fortinet FortiMail 7.6.0 through 7.6.3, FortiMail 7.4.0 through 7.4.5, FortiMail 7.2.0 through 7.2.8 allows an authenticated privileged attacker to execute unauthorized code or commands via specifically crafted HTTP or HTTPS requests.	2026-05-12	7.2
CVE-2026-23820	hewlett packard enterprise (hpe) - ArubaOS (AOS)	A vulnerability in the command line interface of Access Points running AOS-10 and AOS-8 Instant could allow an authenticated remote attacker to execute system commands in a restricted shell environment. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system.	2026-05-12	7.2
CVE-2026-23821	hewlett packard enterprise (hpe) - ArubaOS (AOS)	A vulnerability in the configuration processing logic of Access Points running AOS-10 could allow an authenticated remote attacker to execute system commands under certain pre-existing conditions. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system. Note: Access Points running AOS-8 Instant software are not affected by this vulnerability.	2026-05-12	7.2
CVE-2026-23823	hewlett packard enterprise (hpe) - ArubaOS (AOS)	A vulnerability in the command line interface of Access Points running AOS-10 could allow an authenticated remote attacker to perform command injection. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system. NOTE: This vulnerability only impacts Access Points running AOS-10.7.x.x and above. AOS-10.4 AP and AOS-8 Instant software branches are not affected by this vulnerability.	2026-05-12	7.2
CVE-2026-44852	arubanetworks - multiple products	An authenticated remote code execution vulnerability exists in the AOS-8 and AOS-10 web-based management interface. A vulnerability in the certificate download functionality could allow an authenticated remote attacker to overwrite arbitrary files on the underlying operating system by exploiting improper input validation in the file path parameter. Successful exploitation could allow the attacker to execute arbitrary commands on the underlying operating system as a privileged user.	2026-05-12	7.2
CVE-2026-44853	arubanetworks - multiple products	Command injection vulnerabilities exist in the web-based management interface of AOS-8 and AOS-10 Operating Systems. Successful exploitation could allow an authenticated remote attacker to upload arbitrary files to the underlying operating system, potentially leading to remote code execution as a privileged user.	2026-05-12	7.2
CVE-2026-44854	arubanetworks - multiple products	Command injection vulnerabilities exist in the web-based management interface of AOS-8 and AOS-10 Operating Systems. Successful exploitation could allow an authenticated remote attacker to upload arbitrary files to the underlying operating system, potentially leading to remote code execution as a privileged user.	2026-05-12	7.2
CVE-2026-44855	arubanetworks - multiple products	Stack-based buffer overflow vulnerabilities exist in several underlying management service components accessed through the command-line interface of the AOS-8 and AOS-10 Operating Systems. An authenticated attacker with administrative privileges could exploit these vulnerabilities by sending specially crafted requests to the affected services. Successful exploitation could allow the attacker to execute arbitrary code with elevated privileges on the underlying operating system.	2026-05-12	7.2
CVE-2026-44856	arubanetworks - multiple products	Stack-based buffer overflow vulnerabilities exist in several underlying management service components accessed through the command-line interface of the AOS-8 and AOS-10 Operating Systems. An authenticated attacker with administrative privileges could exploit these vulnerabilities by sending specially crafted requests to the affected services. Successful exploitation could allow the attacker to execute arbitrary code with elevated privileges on the underlying operating system.	2026-05-12	7.2
CVE-2026-44857	arubanetworks - multiple products	Stack-based buffer overflow vulnerabilities exist in several underlying management service components accessed through the command-line interface of the AOS-8 and AOS-10 Operating Systems. An authenticated attacker with administrative privileges could exploit these vulnerabilities by sending specially crafted requests to the affected services. Successful exploitation could allow the attacker to execute arbitrary code with elevated privileges on the underlying operating system.	2026-05-12	7.2
CVE-2026-44858	arubanetworks - multiple products	Stack-based buffer overflow vulnerabilities exist in several underlying management service components accessed through the command-line interface of the AOS-8 and AOS-10 Operating Systems. An authenticated attacker with administrative privileges could exploit these vulnerabilities by sending specially crafted requests to the affected services. Successful exploitation could allow the attacker to execute arbitrary code with elevated privileges on the underlying operating system.	2026-05-12	7.2
CVE-2026-44859	arubanetworks - multiple products	Stack-based buffer overflow vulnerabilities exist in several underlying management service components accessed through the command-line interface of the AOS-8 and AOS-10 Operating Systems. An authenticated attacker with administrative privileges could exploit these vulnerabilities by sending specially crafted requests to the affected services. Successful exploitation could allow the attacker to execute arbitrary code with elevated privileges on the underlying operating system.	2026-05-12	7.2
CVE-2026-44860	arubanetworks - multiple products	SQL injection vulnerabilities exist in several underlying service components accessible through the AOS-8 and AOS-10 command-line interface and management protocol. An authenticated attacker with administrative privileges could exploit these vulnerabilities by injecting crafted input into parameters that are passed unsanitized to backend database queries. Successful exploitation could allow the attacker to execute arbitrary commands on the underlying operating system.	2026-05-12	7.2
CVE-2026-44861	arubanetworks - multiple products	SQL injection vulnerabilities exist in several underlying service components accessible through the AOS-8 and AOS-10 command-line interface and management protocol. An authenticated attacker with administrative privileges could exploit these vulnerabilities by injecting crafted input into parameters that are passed unsanitized to backend database queries. Successful exploitation could allow the attacker to execute arbitrary commands on the underlying operating system.	2026-05-12	7.2

CVE-2026-44862	arubanetworks - multiple products	SQL injection vulnerabilities exist in several underlying service components accessible through the AOS-8 and AOS-10 command-line interface and management protocol. An authenticated attacker with administrative privileges could exploit these vulnerabilities by injecting crafted input into parameters that are passed unsanitized to backend database queries. Successful exploitation could allow the attacker to execute arbitrary commands on the underlying operating system.	2026-05-12	7.2
CVE-2026-44863	arubanetworks - multiple products	SQL injection vulnerabilities exist in several underlying service components accessible through the AOS-8 and AOS-10 command-line interface and management protocol. An authenticated attacker with administrative privileges could exploit these vulnerabilities by injecting crafted input into parameters that are passed unsanitized to backend database queries. Successful exploitation could allow the attacker to execute arbitrary commands on the underlying operating system.	2026-05-12	7.2
CVE-2026-44864	arubanetworks - multiple products	SQL injection vulnerabilities exist in several underlying service components accessible through the AOS-8 and AOS-10 command-line interface and management protocol. An authenticated attacker with administrative privileges could exploit these vulnerabilities by injecting crafted input into parameters that are passed unsanitized to backend database queries. Successful exploitation could allow the attacker to execute arbitrary commands on the underlying operating system.	2026-05-12	7.2
CVE-2026-44865	arubanetworks - multiple products	Command injection vulnerabilities exist in the web-based management interface of AOS-8 and AOS-10 Operating Systems. Successful exploitation of these vulnerabilities could allow an authenticated remote attacker to execute arbitrary commands on the underlying operating system.	2026-05-12	7.2
CVE-2026-44866	arubanetworks - multiple products	Command injection vulnerabilities exist in the web-based management interface of AOS-8 and AOS-10 Operating Systems. Successful exploitation of these vulnerabilities could allow an authenticated remote attacker to execute arbitrary commands on the underlying operating system.	2026-05-12	7.2
CVE-2026-44867	arubanetworks - multiple products	Command injection vulnerabilities exist in the web-based management interface of AOS-8 and AOS-10 Operating Systems. Successful exploitation of these vulnerabilities could allow an authenticated remote attacker to execute arbitrary commands on the underlying operating system.	2026-05-12	7.2
CVE-2026-44868	arubanetworks - multiple products	Command injection vulnerabilities exist in the web-based management interface of AOS-8 and AOS-10 Operating Systems. Successful exploitation of these vulnerabilities could allow an authenticated remote attacker to execute arbitrary commands on the underlying operating system.	2026-05-12	7.2
CVE-2026-44869	arubanetworks - multiple products	Command injection vulnerabilities exist in the web-based management interface of AOS-8 and AOS-10 Operating Systems. Successful exploitation of these vulnerabilities could allow an authenticated remote attacker to execute arbitrary commands on the underlying operating system.	2026-05-12	7.2
CVE-2026-44870	arubanetworks - multiple products	Command injection vulnerabilities exist in the command line interface (CLI) service accessed by the PAPI protocol of AOS-8 and AOS-10 Operating Systems. Successful exploitation of these vulnerabilities could allow an authenticated remote attacker to execute arbitrary commands on the underlying operating system.	2026-05-12	7.2
CVE-2026-44872	arubanetworks - multiple products	A command injection vulnerability exists in the web-based management interface of AOS-8 and AOS-10 Operating Systems. Successful exploitation could allow an authenticated remote attacker to place arbitrary files on the underlying filesystem of the affected device.	2026-05-12	7.2
CVE-2026-44871	arubanetworks - multiple products	Command injection vulnerabilities exist in the command line interface (CLI) service accessed by the PAPI protocol of AOS-8 and AOS-10 Operating Systems. Successful exploitation of these vulnerabilities could allow an authenticated remote attacker to execute arbitrary commands on the underlying operating system.	2026-05-12	7.2
CVE-2026-20916	f5 - BIG-IQ	An authenticated iControl REST user with low privileges can create or modify arbitrary files through an undisclosed iControl REST endpoint on the BIG-IQ system. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	7.2
CVE-2026-28941	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, macOS Sequoia 15.7.7, macOS Tahoe 26.5. Processing a maliciously crafted file may lead to a denial-of-service or potentially disclose memory contents.	2026-05-11	7.1
CVE-2026-40401	microsoft - multiple products	Null pointer dereference in Windows TCP/IP allows an unauthorized attacker to deny service locally.	2026-05-12	7.1
CVE-2026-41101	microsoft - word	Improper access control in Microsoft Office Word allows an authorized attacker to perform spoofing locally.	2026-05-12	7.1
CVE-2026-41102	microsoft - powerpoint	Improper access control in Microsoft Office PowerPoint allows an authorized attacker to perform spoofing locally.	2026-05-12	7.1
CVE-2026-8199	mongodb - multiple products	An authenticated user can cause excess memory usage via bitwise match expression AST processing of $bitsAllSet, $bitsAnySet, $bitsAllClear, and $bitsAnyClear. This contributes to memory pressure and may lead to availability loss by OOM. This issue impacts MongoDB Server v7.0 versions prior to 7.0.34, v8.0 versions prior to 8.0.23, v8.2 versions prior to 8.2.9 and v8.3 versions prior to 8.3.2.	2026-05-13	7.1
CVE-2026-35062	f5 - BIG-IP	An authenticated iControl SOAP user may be able to obtain information of other accounts. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	7.1
CVE-2026-40462	f5 - BIG-IP	Incorrect permission assignment vulnerabilities exist in iControl REST and TMOS shell (tmsh) undisclosed command which may allow an authenticated attacker to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	7.1
CVE-2026-40699	f5 - BIG-IP	A vulnerability exists in the undisclosed pages in the Configuration utility that may allow a low-privileged authenticated attacker to access to undisclosed sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	7.1
CVE-2026-41219	f5 - multiple products	An improper sanitization vulnerability exists in the BIG-IP QKView utility that allows a low-privileged attacker to read sensitive information from a QKView file. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2026-05-13	7.1
CVE-2026-41959	f5 - multiple products	Incorrect permission assignment vulnerabilities exist in BIG-IP and BIG-IQ TMOS Shell (tmsh) network diagnostics commands and in BIG-IP iControl REST. These vulnerabilities may allow an authenticated attacker to view the network status of destination systems. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	7.1

CVE-2026-42781	f5 - BIG-IP	When embedded Packet Velocity Acceleration (ePVA) acceleration is configured, undisclosed local ethernet traffic can cause an increase in ePVA and Traffic Management Microkernel (TMM) resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	7.1
CVE-2026-42919	f5 - BIG-IP	A vulnerability exists in BIG-IP systems that may allow an authenticated attacker with administrative access to escalate their privileges. A successful exploit may allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	7.1
CVE-2026-42937	f5 - multiple products	Incorrect permission assignment vulnerabilities exist in BIG-IP and BIG-IQ TMOS Shell (tmsh) arp and ndp commands, and in BIG-IP iControl REST. These vulnerabilities may allow an authenticated attacker to view adjacent network information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	7.1
CVE-2026-33377	grafana - Grafana OSS	An Editor can overwrite a dashboard not owned by them to acquire admin on that specific dashboard. The user must have write access to the dashboard to escalate privilege.	2026-05-13	7.1
CVE-2026-46333	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ptrace: slightly saner 'get_dumpable()' logic The 'dumpability' of a task is fundamentally about the memory image of the task - the concept comes from whether it can core dump or not - and makes no sense when you don't have an associated mm. And almost all users do in fact use it only for the case where the task has a mm pointer. But we have one odd special case: ptrace_may_access() uses 'dumpable' to check various other things entirely independently of the MM (typically explicitly using flags like PTRACE_MODE_READ_FSCREDS). Including for threads that no longer have a VM (and maybe never did, like most kernel threads). It's not what this flag was designed for, but it is what it is. The ptrace code does check that the uid/gid matches, so you do have to be uid-0 to see kernel thread details, but this means that the traditional "drop capabilities" model doesn't make any difference for this all. Make it all make a *bit* more sense by saying that if you don't have a MM pointer, we'll use a cached "last dumpability" flag if the thread ever had a MM (it will be zero for kernel threads since it is never set), and require a proper CAP_SYS_PTRACE capability to override.	2026-05-15	7.1
CVE-2026-44641	microsoft - apm	Microsoft APM is an open-source, community-driven dependency manager for AI agents. Prior to 0.8.12, Microsoft APM normalizes marketplace plugins by copying plugin components referenced in plugin.json into .apm/. The manifest fields agents, skills, commands, and hooks are attacker-controlled, but the implementation does not enforce that those paths remain inside the plugin directory. A malicious plugin can therefore use absolute paths or ../ traversal paths to copy arbitrary readable host files or directories from the installer's machine during apm install. This vulnerability is fixed in 0.8.12.	2026-05-15	7.1
CVE-2026-27662	siemens - multiple products	Affected devices do not properly restrict access to the web browser via the Control Panel when no corresponding security mechanisms are in place. This could allow an unauthenticated attacker to gain unauthorized access to the web browser, potentially enabling the discovery of backdoors, performing unauthorized actions, or exploiting misconfigurations that may lead to further system compromise.	2026-05-12	7
CVE-2026-33839	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally.	2026-05-12	7
CVE-2026-34331	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally.	2026-05-12	7
CVE-2026-34340	microsoft - multiple products	Use after free in Windows Projected File System allows an authorized attacker to elevate privileges locally.	2026-05-12	7
CVE-2026-34341	microsoft - multiple products	Double free in Windows Link-Layer Discovery Protocol (LLDP) allows an authorized attacker to elevate privileges locally.	2026-05-12	7
CVE-2026-34342	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Print Spooler Components allows an authorized attacker to elevate privileges locally.	2026-05-12	7
CVE-2026-34345	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-05-12	7
CVE-2026-34347	microsoft - multiple products	Use after free in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally.	2026-05-12	7
CVE-2026-35416	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-05-12	7
CVE-2026-40410	microsoft - multiple products	Use after free in Windows SMB Client allows an authorized attacker to elevate privileges locally.	2026-05-12	7
CVE-2026-42825	microsoft - multiple products	Use after free in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-05-12	7

CVE-2026-44503	microsoft - multiple products	The RedirectHandler middleware in microsoft/kiota-java (com.microsoft.kiota:microsoft-kiota-http-okHttp v1.9.0) and other Kiota libraries fails to strip sensitive HTTP headers when following 3xx redirects to a different host or scheme. Only the Authorization header is removed; Cookie, Proxy-Authorization, and all custom headers are forwarded to the redirect target.	2026-05-14	7
CVE-2024-54017	siemens - multiple products	A vulnerability has been identified in SIPROTEC 5 6MD84 (CP300) (All versions < V11.0), SIPROTEC 5 6MD85 (CP200) (All versions), SIPROTEC 5 6MD85 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 6MD86 (CP200) (All versions), SIPROTEC 5 6MD86 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 6MD89 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 6MU85 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7KE85 (CP200) (All versions), SIPROTEC 5 7KE85 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7SA82 (CP100) (All versions >= V7.80), SIPROTEC 5 7SA82 (CP150) (All versions < V11.0), SIPROTEC 5 7SA84 (CP200) (All versions), SIPROTEC 5 7SA86 (CP200) (All versions), SIPROTEC 5 7SA86 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7SA87 (CP200) (All versions), SIPROTEC 5 7SA87 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7SD82 (CP100) (All versions >= V7.80), SIPROTEC 5 7SD82 (CP150) (All versions < V11.0), SIPROTEC 5 7SD84 (CP200) (All versions), SIPROTEC 5 7SD86 (CP200) (All versions), SIPROTEC 5 7SD86 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7SD87 (CP200) (All versions), SIPROTEC 5 7SD87 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7SJ81 (CP100) (All versions >= V7.80), SIPROTEC 5 7SJ81 (CP150) (All versions < V11.0), SIPROTEC 5 7SJ82 (CP100) (All versions >= V7.80), SIPROTEC 5 7SJ82 (CP150) (All versions < V11.0), SIPROTEC 5 7SJ85 (CP200) (All versions), SIPROTEC 5 7SJ85 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7SJ86 (CP200) (All versions), SIPROTEC 5 7SJ86 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7SK82 (CP100) (All versions >= V7.80), SIPROTEC 5 7SK82 (CP150) (All versions < V11.0), SIPROTEC 5 7SK85 (CP200) (All versions), SIPROTEC 5 7SK85 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7SL82 (CP100) (All versions >= V7.80), SIPROTEC 5 7SL82 (CP150) (All versions < V11.0), SIPROTEC 5 7SL86 (CP200) (All versions), SIPROTEC 5 7SL86 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7SL87 (CP200) (All versions), SIPROTEC 5 7SL87 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7SS85 (CP200) (All versions), SIPROTEC 5 7SS85 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7ST85 (CP200) (All versions), SIPROTEC 5 7ST85 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7ST86 (CP300) (All versions < V11.0), SIPROTEC 5 7SX82 (CP150) (All versions < V11.0), SIPROTEC 5 7SX85 (CP300) (All versions < V11.0), SIPROTEC 5 7SY82 (CP150) (All versions < V11.0), SIPROTEC 5 7UM85 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7UT82 (CP100) (All versions >= V7.80), SIPROTEC 5 7UT82 (CP150) (All versions < V11.0), SIPROTEC 5 7UT85 (CP200) (All versions), SIPROTEC 5 7UT85 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7UT86 (CP200) (All versions), SIPROTEC 5 7UT86 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7UT87 (CP200) (All versions), SIPROTEC 5 7UT87 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7VE85 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7VK87 (CP200) (All versions), SIPROTEC 5 7VK87 (CP300) (All versions >= V7.80 < V11.0), SIPROTEC 5 7VU85 (CP300) (All versions < V11.0), SIPROTEC 5 Compact 7SX800 (CP050) (All versions < V11.0). Affected devices do not use sufficiently random values to create session identifiers. This could allow an unauthenticated remote attacker to brute force a session identifier and gain read access to limited information from the web server without authorization.	2026-05-12	6.9
CVE-2026-20717	intel - quickassist_technology	Improper input validation for some Intel(R) QAT software drivers for Windows before version 1.13 within Ring 3: User Applications may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (low), integrity (low) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	2026-05-12	6.9
CVE-2026-20771	intel - quickassist_technology	Null pointer dereference for some Intel(R) QAT software drivers for Windows before version 1.13 within Ring 3: User Applications may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (low), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	2026-05-12	6.9
CVE-2026-20782	intel - quickassist_technology	Buffer overflow for some Intel(R) QAT software drivers for Windows before version 1.13 within Ring 3: User Applications may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (low), integrity (low) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	2026-05-12	6.9
CVE-2026-20905	intel - quickassist_technology	Improper input validation for some Intel(R) QAT software drivers for Windows before version 2.6 within Ring 3: User Applications may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (low), integrity (low) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	2026-05-12	6.9
CVE-2026-21022	samsung - multiple products	Improper handling of insufficient permissions in Routines prior to SMR May-2026 Release 1 allows local attackers to access sensitive information.	2026-05-13	6.9
CVE-2026-24464	f5 - BIG-IP	When running in Appliance mode, a directory traversal vulnerability exists in an undisclosed iControl REST endpoint that may allow an authenticated attacker with administrator role privileges to cross a security boundary and delete files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	6.9
CVE-2026-40435	f5 - BIG-IP	When configured, IP-based access restrictions for httpd do not cover all endpoints, which may allow connections from blocked addresses. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	6.9
CVE-2026-40460	f5 - multiple products	When NGINX Plus or NGINX Open Source are configured to use the HTTP/3 QUIC module, an attacker may be able to spoof their source IP address allowing for bypass of authorization or bypass	2026-05-13	6.9

		of rate limiting. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
CVE-2026-41954	f5 - multiple products	Sensitive information disclosure vulnerability exists in the undisclosed iControl REST endpoint and TMOS Shell (tmsh) command which may allow an authenticated attacker with resource administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	6.9
CVE-2026-42063	f5 - BIG-IP	A vulnerability exists in iControl SOAP where an authenticated attacker with the Resource Administrator or Administrator role can download sensitive files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	6.9
CVE-2026-42780	f5 - multiple products	A directory traversal vulnerability exists in BIG-IP SSL Orchestrator that allows an authenticated attacker with high privilege to overwrite, delete or corrupt arbitrary local files. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	6.9
CVE-2026-20881	intel - quickassist_technology	Divide by zero for some Intel(R) QAT software drivers for Windows before version 1.13 within Ring 3: User Applications may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	2026-05-12	6.8
CVE-2026-20914	intel - quickassist_technology	Null pointer dereference for some Intel(R) QAT software drivers for Windows before version 2.6.0 within Ring 3: User Applications may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (high) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	2026-05-12	6.8
CVE-2026-21015	samsung - multiple products	Incorrect default permissions in FactoryCamera prior to SMR May-2026 Release 1 allows local attacker to access unique identifier.	2026-05-13	6.8
CVE-2026-21018	samsung - multiple products	Out-of-bounds write in SveService prior to SMR May-2026 Release 1 allows local privileged attackers to execute arbitrary code.	2026-05-13	6.8
CVE-2026-6332	schneider-electric - ecostruxure_machine_expert_hvac	CWE-312: Cleartext Storage of Sensitive Information vulnerability exists that could cause the disclosure of a sensitive information which could result in revealing protected source code and loss of confidentiality, When an authorized attacker accesses the source code for editing or compiling it.	2026-05-14	6.8
CVE-2026-41970	huawei - multiple products	Out-of-bounds write vulnerability in the distributed file system module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-05-15	6.8
CVE-2026-26946	dell - multiple products	Dell ECS versions 3.8.1.0 through 3.8.1.7 and Dell ObjectScale versions prior to 4.3.0.0, contains an improper privilege management vulnerability in the OS. A high privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.	2026-05-11	6.7
CVE-2026-40638	dell - insightiq	Dell PowerScale InsightIQ, versions 5.0.0 through 6.2.0, contains an execution with unnecessary privileges vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to elevation of privileges.	2026-05-12	6.7
CVE-2025-53680	fortinet - multiple products	An improper neutralization of special elements used in an OS command ("OS Command Injection") vulnerability [CWE-78] vulnerability in Fortinet FortiAP 7.6.0 through 7.6.2, FortiAP 7.4.0 through 7.4.5, FortiAP 7.2 all versions, FortiAP 7.0 all versions, FortiAP 6.4 all versions, FortiAP-U 7.0.0 through 7.0.5, FortiAP-U 6.2 all versions, FortiAP-W2 7.4.0 through 7.4.4, FortiAP-W2 7.2 all versions, FortiAP-W2 7.0 all versions allows an authenticated privileged attacker to execute unauthorized code or commands via crafted CLI requests.	2026-05-12	6.7
CVE-2025-53870	fortinet - multiple products	An improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiAP 7.6.0 through 7.6.2, FortiAP 7.4.0 through 7.4.5, FortiAP 7.2 all versions, FortiAP 7.0 all versions, FortiAP 6.4 all versions, FortiAP-W2 7.4.0 through 7.4.4, FortiAP-W2 7.2 all versions, FortiAP-W2 7.0 all versions may allow an authenticated attacker to execute unauthorized code or commands via a specifically crafted cli command.	2026-05-12	6.7
CVE-2026-21530	microsoft - multiple products	Double free in Windows Rich Text Edit allows an authorized attacker to elevate privileges locally.	2026-05-12	6.7
CVE-2026-32170	microsoft - multiple products	Double free in Windows Rich Text Edit Control allows an authorized attacker to elevate privileges locally.	2026-05-12	6.7
CVE-2026-41097	microsoft - multiple products	Reliance on a component that is not updateable in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-05-12	6.7
CVE-2026-28758	f5 - BIG-IP	When BIG-IP DNS is provisioned, a vulnerability exists in the gtm_add and bigip_add iControl REST commands that return the ssh-password parameter in cleartext in the iControl REST response and is also logged in the audit log. This may allow a highly privileged, authenticated attacker with access to the audit log to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	2026-05-13	6.7
CVE-2026-42408	f5 - BIG-IP	When BIG-IP DNS is provisioned, a vulnerability exists in an undisclosed TMOS Shell (tmsh) command that may allow a highly privileged authenticated attacker to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	6.7
CVE-2026-41018	apache - apache-airflow-providers-elasticsearch	The Elasticsearch logging provider, when configured with a `host` URL that embeds credentials (for example `https://user:password@server.example.com:9200`), wrote the full host URL — including the embedded credentials — into task logs. Any user with task-log read permission could harvest the backend credentials. Users are advised to upgrade to `apache-airflow-providers-elasticsearch` 6.5.3 or later and, as a defense-in-depth measure, configure the backend credentials via a secret backend rather than embedding them in the `[elasticsearch] host` URL.	2026-05-11	6.5
CVE-2026-43826	apache - apache-airflow-providers-opensearch	The OpenSearch logging provider, when configured with a `host` URL that embeds credentials (for example `https://user:password@server.example.com:9200`), wrote the full host URL — including the embedded credentials — into task logs. Any user with task-log read permission could harvest the backend credentials. Users are advised to upgrade to `apache-airflow-providers-opensearch`	2026-05-11	6.5

		1.9.1 or later and, as a defense-in-depth measure, configure the backend credentials via a secret backend rather than embedding them in the `[opensearch] host` URL.		
CVE-2026-28902	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.5, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-05-11	6.5
CVE-2026-28903	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.5, iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-05-11	6.5
CVE-2026-28918	apple - multiple products	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Parsing a maliciously crafted file may lead to an unexpected app termination.	2026-05-11	6.5
CVE-2026-28920	apple - multiple products	An information leakage was addressed with additional validation. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Visiting a maliciously crafted website may leak sensitive data.	2026-05-11	6.5
CVE-2026-28922	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. An app may be able to access private information.	2026-05-11	6.5
CVE-2026-28942	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in Safari 26.5, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2026-05-11	6.5
CVE-2026-28946	apple - macos	A use-after-free issue was addressed with improved memory management. This issue is fixed in Safari 26.5, macOS Tahoe 26.5. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2026-05-11	6.5
CVE-2026-28956	apple - multiple products	A memory corruption issue was addressed with improved input validation. This issue is fixed in iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing a maliciously crafted media file may lead to unexpected app termination or corrupt process memory.	2026-05-11	6.5
CVE-2026-28972	apple - multiple products	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. An app may be able to cause unexpected system termination or write kernel memory.	2026-05-11	6.5
CVE-2026-7255	zyxel - wre6505_firmware	** UNSUPPORTED WHEN ASSIGNED ** An improper restriction of excessive authentication attempts vulnerability in the web management interface of Zyxel WRE6505 v2 firmware version V1.00(ABDV.3)C0 could allow an adjacent attacker on the LAN to brute-force the password and bypass authentication.	2026-05-12	6.5
CVE-2026-8388	mozilla - firefox	Incorrect boundary conditions in the JavaScript Engine: JIT component. This vulnerability was fixed in Firefox 150.0.3, Firefox ESR 115.36, Firefox ESR 140.11, and Thunderbird 140.11.	2026-05-12	6.5
CVE-2026-8109	ivanti - multiple products	An exposed dangerous method on the Core Server of Ivanti Endpoint Manager before version 2024 SU6 allows a remote authenticated attacker to leak access credentials.	2026-05-12	6.5
CVE-2026-34350	microsoft - windows_server_2025	Null pointer dereference in Windows Storport Miniport Driver allows an unauthorized attacker to deny service over a network.	2026-05-12	6.5
CVE-2026-35422	microsoft - multiple products	Authentication bypass using an alternate path or channel in Windows TCP/IP allows an authorized attacker to bypass a security feature over a network.	2026-05-12	6.5
CVE-2026-40374	microsoft - power_automate_for_desktop	Exposure of sensitive information to an unauthorized actor in Power Automate allows an authorized attacker to disclose information over a network.	2026-05-12	6.5
CVE-2026-42830	microsoft - azure_monitor_agent	Untrusted search path in Azure Monitor Agent allows an authorized attacker to elevate privileges locally.	2026-05-12	6.5
CVE-2026-42891	microsoft - edge_chromium	User interface (ui) misrepresentation of critical information in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-05-12	6.5
CVE-2026-28376	grafana - multiple products	The Grafana Live push endpoint can be exploited to cause unbounded memory allocation by sending a large or streaming request body, potentially leading to out-of-memory conditions. An authenticated user with access to the Grafana Live API can trigger this issue.	2026-05-13	6.5
CVE-2026-28379	grafana - Grafana OSS	A race condition in Grafana Live allows authenticated users with Viewer role to trigger a server crash by sending concurrent requests that cause a fatal map access error. This results in complete service unavailability requiring restart of the Grafana server.	2026-05-13	6.5
CVE-2026-28380	grafana - Grafana OSS	Any Editor could delete any snapshot, even if they have no access to read or write them.	2026-05-13	6.5
CVE-2026-28383	grafana - Grafana OSS	A request to the Grafana plugin resources endpoint can cause unbounded memory allocation by reading the entire request body into memory. An authenticated user can exploit this to trigger an out-of-memory condition, potentially causing a denial of service.	2026-05-13	6.5
CVE-2026-33378	grafana - Grafana OSS	Using the $__timeGroup macro, one can achieve an OOM by overloading the server. This requires a SQL datasource. If the server is set up to auto-restart, the impact is minimal or non-existent, as the attack can take upwards of half an hour to crash the server.	2026-05-13	6.5
CVE-2026-8550	google - chrome	Use after free in Google Lens in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-05-14	6.5
CVE-2026-8570	google - chrome	Type Confusion in V8 in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	6.5
CVE-2025-9973	wso2 - identity_server	Due to not validating the organization context when executing adaptive authentication flows, the WSO2 Identity Server allows adaptive authentication logic to be triggered on unintended organizations. A malicious actor with privileges to configure adaptive authentication within one organization can leverage this functionality to execute authentication logic on other organizations and sub-organizations.	2026-05-11	6.4

		This flaw allows bypassing authorization boundaries between organizations, leading to unauthorized access to critical operations and user accounts in other organizations. When adaptive authentication is enabled in a multi-organization deployment, a malicious actor with privileges to configure adaptive authentication in one organization could exploit this feature to perform critical operations in other organizations without authorization. This may result in privilege escalation, unauthorized access to resources, and potential account takeover across organizations.		
CVE-2026-7258	php - multiple products	In PHP versions 8.2.* before 8.2.31, 8.3.* before 8.3.31, 8.4.* before 8.4.21, and 8.5.* before 8.5.6, some functions, including urldecode(), pass signed char to ctype functions (like isxdigit()). On the systems with default signed char and optimized table-lookup ctype functions - such as NetBSD - this can lead to accessing array with negative offset, which can trigger a denial of service.	2026-05-10	6.3
CVE-2026-7261	php - multiple products	In PHP versions 8.2.* before 8.2.31, 8.3.* before 8.3.31, 8.4.* before 8.4.21, and 8.5.* before 8.5.6, when SoapServer is configured with SOAP_PERSISTENCE_SESSION, the handler object is persisted across requests via session storage. However, in the case SOAP requests results in an error, the persistance is handled incorrectly, resulting in freeing the object while keeping a pointer to it, which may lead to use-after-free. This may lead to memory corruption, information disclosure, or process crashes, with confidentiality, integrity, and availability impact on the vulnerable system.	2026-05-10	6.3
CVE-2026-7568	php - multiple products	In PHP versions 8.2.* before 8.2.31, 8.3.* before 8.3.31, 8.4.* before 8.4.21, and 8.5.* before 8.5.6, the metaphone() function in ext/standard/metaphone.c uses a signed int variable to track the current position within the input string. If a string longer than 2,147,483,647 bytes is passed, a signed integer overflow occurs, resulting in undefined behavior. This can lead to an out-of-bounds read, causing a segmentation fault or access to unrelated memory, and may affect the availability of the PHP process.	2026-05-10	6.3
CVE-2026-6104	php - multiple products	In PHP versions 8.4.* before 8.4.21 and 8.5.* before 8.5.6, when an encoding name containing an embedded NUL byte is passed to mb_convert_encoding() or related mbstring functions, the code incorrectly assumes that when strncasecmp() returns 0 it means the strings have the same length. This can lead to out-of-bounds read of global memory, potentially causing a crash or information disclosure or crash. Affected functions include mb_convert_encoding(), mb_detect_encoding(), mb_convert_variables(), and mb_detect_order(), as well as the mbstring.detect_order and mbstring.http_output INI settings.	2026-05-10	6.3
CVE-2026-7263	php - multiple products	In PHP versions 8.4.* before 8.4.21 and 8.5.* before 8.5.6, DOMNode::C14N() method may process the XML data incorrectly, causing a circular linked list in the data structure representing the XML document. This may cause subsequent processing of the XML document to enter infinite loop, causing denial of service in the processing application.	2026-05-10	6.3
CVE-2025-8325	wso2 - api_control_plane	The software fails to enforce role-based access controls for certain Gateway API invocations. Users with the 'Internal/Everyone' role can invoke these APIs, bypassing intended permission checks. This same vulnerability also affects Internal Service APIs, potentially exposing them in WSO2 APIM 3.x versions. A malicious actor with a valid user account on a vulnerable deployment can perform sensitive operations against the Gateway REST API regardless of their actual roles or privileges. This could lead to unintended behavior or misuse, particularly in production environments.	2026-05-11	6.3
CVE-2026-41610	microsoft - visual_studio_code	Improper neutralization of input during web page generation ('cross-site scripting') in Visual Studio Code allows an unauthorized attacker to bypass a security feature locally.	2026-05-12	6.3
CVE-2026-34664	adobe - substance_3d_designer	Substance3D - Designer versions 15.1.0 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-05-12	6.3
CVE-2026-34019	f5 - BIG-IP	When Bidirectional Forwarding Detection (BFD) is configured in Static and Dynamic routing protocols, undisclosed traffic can cause the Traffic Management Microkernel (TMM) to stop processing BFD packets and cause the configured routing protocol to fail over. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	6.3
CVE-2026-40701	f5 - multiple products	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_ssl_module module when the ssl_verify_client directive is set to "on" or "optional," and the ssl_ocsp directive is set to "on" or the leaf parameters are configured with a resolver. With this configuration, an unauthenticated attacker can send requests along with conditions beyond its control that may cause a heap-use-after-free error in the NGINX worker process. This vulnerability may result in limited modification of data or the NGINX worker process restarting. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	6.3
CVE-2026-42926	f5 - NGINX Open Source	When NGINX Open Source is configured to proxy HTTP/2 traffic by setting proxy_http_version to 2, and also uses proxy_set_body, an attacker may be able to inject frame headers and payload bytes to the upstream peer. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	6.3
CVE-2026-42934	f5 - multiple products	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_charset_module module. When charset, source_charset, and charset_map and proxy_pass with disabled buffering ("off") directives are configured, unauthenticated attackers can send requests that with conditions beyond the attackers' control to cause a heap buffer over-read in the NGINX worker process, leading to limited disclosure of memory or a restart. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	6.3
CVE-2026-2695	teamviewer - DEX (On-Premises)	A command injection vulnerability was discovered in TeamViewer DEX Platform On-Premises	2026-05-13	6.3

		(former 1E DEX Platform On-Premises) prior to version 9.2. Improper input validation allows authenticated users with at least questioner privileges to inject commands in specific instructions. Exploitation could lead to execution of elevated commands on devices connected to the platform.		
CVE-2026-33380	grafana - Grafana OSS	A vulnerability in SQL Expressions allows an authenticated attacker to read arbitrary files from the Grafana server's filesystem. Only instances with the sqlExpressions feature toggle enabled are vulnerable.	2026-05-13	6.3
CVE-2026-28897	apple - multiple products	A buffer overflow was addressed with improved input validation. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. A local user may be able to cause unexpected system termination or read kernel memory.	2026-05-11	6.2
CVE-2026-28977	apple - multiple products	The issue was addressed with improved bounds checks. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing a maliciously crafted file may lead to unexpected app termination.	2026-05-11	6.2
CVE-2026-28985	apple - multiple products	A null pointer dereference was addressed with improved input validation. This issue is fixed in iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5. An attacker on the local network may be able to cause a denial-of-service.	2026-05-11	6.2
CVE-2026-43653	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5. An attacker on the local network may be able to cause a denial-of-service.	2026-05-11	6.2
CVE-2026-43666	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. An attacker on the local network may be able to cause a denial-of-service.	2026-05-11	6.2
CVE-2026-40380	microsoft - multiple products	Heap-based buffer overflow in Volume Manager Extension Driver allows an authorized attacker to execute code with a physical attack.	2026-05-12	6.2
CVE-2026-41614	microsoft - 365_copilot	Improper access control in M365 Copilot for Desktop allows an unauthorized attacker to perform spoofing locally.	2026-05-12	6.2
CVE-2026-34666	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Improper Input Validation vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	6.2
CVE-2026-34667	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	6.2
CVE-2026-34668	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Improper Input Validation vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	6.2
CVE-2026-34669	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Improper Input Validation vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	6.2
CVE-2026-34670	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Improper Input Validation vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	6.2
CVE-2026-34671	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	6.2
CVE-2026-34672	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Integer Underflow (Wrap or Wraparound) vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	6.2
CVE-2026-34673	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	6.2
CVE-2026-34677	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	6.2
CVE-2026-34678	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	6.2
CVE-2026-34679	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Improper Input Validation vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	6.2
CVE-2026-34680	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	6.2
CVE-2026-34688	adobe - multiple products	CAI Content Credentials versions 0.78.2, 0.7.0 and earlier are affected by an Improper Input Validation vulnerability that could result in an application denial-of-service. An attacker could	2026-05-12	6.2

		exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.		
CVE-2026-41969	huawei - multiple products	Permission control vulnerability in the projection module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-05-15	6.2
CVE-2025-40948	siemens - multiple products	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.17.1), RUGGEDCOM ROX MX5000RE (All versions < V2.17.1), RUGGEDCOM ROX RX1400 (All versions < V2.17.1), RUGGEDCOM ROX RX1500 (All versions < V2.17.1), RUGGEDCOM ROX RX1501 (All versions < V2.17.1), RUGGEDCOM ROX RX1510 (All versions < V2.17.1), RUGGEDCOM ROX RX1511 (All versions < V2.17.1), RUGGEDCOM ROX RX1512 (All versions < V2.17.1), RUGGEDCOM ROX RX1524 (All versions < V2.17.1), RUGGEDCOM ROX RX1536 (All versions < V2.17.1), RUGGEDCOM ROX RX5000 (All versions < V2.17.1). Affected devices do not properly validate input in the web server's JSON-RPC interface. This could allow an authenticated remote attacker to read arbitrary files from the underlying operating system's filesystem with root privileges.	2026-05-12	6.1
CVE-2026-8201	mongodb - multiple products	A use-after-free vulnerability exists in MongoDB's Field-Level Encryption (FLE) query analysis component, affecting client-side uses of mongocryptd and crypt_shared. Triggering this vulnerability requires control over the structure of a client's FLE-related query. This issue impacts MongoDB Server’s mongocryptd component v7.0 versions prior to 7.0.34, v8.0 versions prior to 8.0.23, v8.2 versions prior to 8.2.9 and v8.3 versions prior to 8.3.2.	2026-05-13	6.1
CVE-2026-41125	siemens - multiple products	A vulnerability has been identified in blueplanet 100 NX3 M8 (All versions), blueplanet 100 TL3 GEN2 (All versions), blueplanet 105 TL3 (All versions), blueplanet 105 TL3 GEN2 (All versions), blueplanet 110 TL3 (All versions), blueplanet 125 NX3 M11 (All versions), blueplanet 125 TL3 (All versions), blueplanet 125 TL3 GEN2 (All versions), blueplanet 137 TL3 (All versions), blueplanet 150 TL3 (All versions), blueplanet 150 TL3 GEN2 (All versions), blueplanet 155 TL3 (All versions), blueplanet 155 TL3 GEN2 (All versions), blueplanet 165 TL3 (All versions), blueplanet 165 TL3 GEN2 (All versions), blueplanet 25.0 NX3-33.0 NX3 (All versions), blueplanet 3.0 NX3-20.0 NX3 (All versions), blueplanet 3.0-5.0 NX1 (All versions), blueplanet 360 NX3 M6 (All versions), blueplanet 50.0 NX3-60.0 NX3 (All versions), blueplanet 87.0 TL3 (All versions), blueplanet 87.0 TL3 GEN2 (All versions), blueplanet 92.0 TL3 (All versions), blueplanet 92.0 TL3 GEN2 (All versions), blueplanet gridsafe 110 TL3-S (All versions), blueplanet gridsafe 137 TL3-S (All versions), blueplanet gridsafe 92.0 TL3-S (All versions), blueplanet hybrid 10.0 TL3 (All versions), blueplanet hybrid 6.0 NH3-12.0 NH3 (All versions). Improper neutralization of special elements used in an sql command ('sql injection') in KACO Meteor server allows an authorized attacker to elevate privileges over a local network.	2026-05-12	5.9
CVE-2026-33381	grafana - Grafana OSS	When a user's access to mint tokens for a service account is revoked, it is sometimes still possible to do so for a few seconds after the event. The user will eventually lose access to do this.	2026-05-13	5.9
CVE-2026-41961	huawei - HarmonyOS	Permission control vulnerability in contacts. Impact: Successful exploitation of this vulnerability may affect availability.	2026-05-15	5.9
CVE-2026-41967	huawei - HarmonyOS	Permission control vulnerability in the manufacturability design module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-05-15	5.9
CVE-2026-41968	huawei - HarmonyOS	Permission control vulnerability in the manufacturability design module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-05-15	5.9
CVE-2026-35157	dell - multiple products	Dell ECS versions 3.8.1.0 through 3.8.1.7 and Dell ObjectScale versions prior to 4.3.0.0, contains an improper neutralization of formula elements in a CSV File vulnerability in the UI. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to remote execution.	2026-05-11	5.8
CVE-2026-41960	huawei - multiple products	Permission control vulnerability in calls. Impact: Successful exploitation of this vulnerability may affect availability.	2026-05-15	5.8
CVE-2025-43992	dell - multiple products	Dell ECS versions 3.8.1.0 through 3.8.1.7 and Dell ObjectScale versions prior to 4.3.0.0, contains an authentication bypass by assumed-immutable data vulnerability in Geo replication. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access to data in transit.	2026-05-11	5.6
CVE-2026-41965	huawei - HarmonyOS	Use-After-Free (UAF) vulnerability in the web. Impact: Successful exploitation of this vulnerability may affect availability.	2026-05-15	5.6
CVE-2026-41966	huawei - HarmonyOS	Permission control vulnerability in the smart sensing service. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-05-15	5.6
CVE-2026-20696	apple - macos	An authorization issue was addressed with improved state management. This issue is fixed in macOS Tahoe 26.4. An app may be able to access sensitive user data.	2026-05-11	5.5
CVE-2026-28914	apple - macos	A logic issue was addressed with improved file handling. This issue is fixed in macOS Tahoe 26.5. A maliciously crafted ZIP archive may bypass Gatekeeper checks.	2026-05-11	5.5
CVE-2026-28958	apple - multiple products	This issue was addressed with improved data protection. This issue is fixed in Safari 26.5, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, visionOS 26.5. An app may be able to access sensitive user data.	2026-05-11	5.5
CVE-2026-28988	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, visionOS 26.5, watchOS 26.5. An app may be able to bypass certain Privacy preferences.	2026-05-11	5.5
CVE-2026-28993	apple - multiple products	This issue was addressed by adding an additional prompt for user consent. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, visionOS 26.5. An app may be able to access user-sensitive data.	2026-05-11	5.5
CVE-2026-28996	apple - multiple products	A race condition was addressed with additional validation. This issue is fixed in iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. An app may be able to access sensitive user data.	2026-05-11	5.5
CVE-2026-32185	microsoft - teams	Files or directories accessible to external parties in Microsoft Teams allows an unauthorized attacker to perform spoofing locally.	2026-05-12	5.5
CVE-2026-34339	microsoft - multiple products	Null pointer dereference in Windows LDAP - Lightweight Directory Access Protocol allows an authorized attacker to deny service locally.	2026-05-12	5.5

CVE-2026-34662	adobe - multiple products	Illustrator versions 29.8.6, 30.3 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	5.5
CVE-2026-34663	adobe - multiple products	Illustrator versions 29.8.6, 30.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-05-12	5.5
CVE-2026-35419	microsoft - multiple products	Out-of-bounds read in Windows DWM Core Library allows an authorized attacker to disclose information locally.	2026-05-12	5.5
CVE-2026-35440	microsoft - multiple products	Files or directories accessible to external parties in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-05-12	5.5
CVE-2026-41612	microsoft - live_preview	Relative path traversal in Visual Studio Code allows an unauthorized attacker to disclose information locally.	2026-05-12	5.5
CVE-2026-44279	fortinet - multiple products	A improper export of android application components vulnerability in Fortinet FortiTokenAndroid 6.2 all versions, FortiTokenAndroid 6.1 all versions, FortiTokenAndroid 5.2 all versions may allow attacker to improper access control via <insert attack vector here>	2026-05-12	5.5
CVE-2026-8586	google - chrome	Inappropriate implementation in Chromoting in Google Chrome prior to 148.0.7778.168 allowed a local attacker to bypass discretionary access control via a malicious file. (Chromium security severity: Medium)	2026-05-14	5.5
CVE-2026-41971	huawei - HarmonyOS	Permission control vulnerability in the security control module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-05-15	5.5
CVE-2026-46383	microsoft - apm	Microsoft APM is an open-source, community-driven dependency manager for AI agents. Prior to 0.13.0, Microsoft APM contains a Windows-specific archive extraction boundary failure in the legacy-bundle probe used by apm install <bundle> on supported Python 3.10 and 3.11 runtimes. When apm install is given a local .tar.gz that is not recognized as a plugin-format bundle, APM probes whether it is a legacy --format apm bundle. On Python versions earlier than 3.12, that probe extracts untrusted tar members with raw tar.extractall() without rejecting Windows absolute member names such as D:/.... This vulnerability is fixed in 0.13.0.	2026-05-15	5.5
CVE-2026-28819	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5. An app may be able to execute arbitrary code with kernel privileges.	2026-05-11	5.4
CVE-2026-25088	fortinet - multiple products	An improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiNDR 7.6.0 through 7.6.2, FortiNDR 7.4.0 through 7.4.9, FortiNDR 7.2 all versions, FortiNDR 7.1 all versions, FortiNDR 7.0 all versions may allow an authenticated attacker to execute unauthorized code or commands via specifically crafted HTTP requests.	2026-05-12	5.4
CVE-2026-35423	microsoft - multiple products	Out-of-bounds read in Telnet Client allows an unauthorized attacker to disclose information over a network.	2026-05-12	5.4
CVE-2026-42838	microsoft - edge_chromium	Improper neutralization of special elements in output used by a downstream component ('injection') in Microsoft Edge (Chromium-based) allows an unauthorized attacker to elevate privileges over a network.	2026-05-12	5.4
CVE-2026-44873	arubanetworks - multiple products	A session management vulnerability in AOS-8 allows previously authenticated users to retain network access after their accounts are administratively disabled. Existing sessions are not invalidated when credentials are revoked, enabling continued access until session expiration. An attacker with compromised credentials could exploit this behavior to maintain unauthorized access even after the account has been disabled.	2026-05-12	5.4
CVE-2026-20209	cisco - Cisco Catalyst SD-WAN Manager	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an authenticated, remote attacker with read-only permissions to elevate their privileges from low to high and perform actions as a high-privileged user. This vulnerability exists because sensitive session information is recorded in audit logs. An attacker could exploit this vulnerability by elevating their read-only permissions in Cisco Catalyst SD-WAN Manager to those of a high-privileged user. A successful exploit could allow the attacker to perform actions as a high-privileged user.	2026-05-14	5.4
CVE-2026-20210	cisco - Cisco Catalyst SD-WAN Manager	A vulnerability in the web UI of Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, could allow an authenticated, remote attacker with read-only permissions to modify configurations and perform unauthorized actions on an affected system. This vulnerability exists because of a failure to redact sensitive information within device configurations and templates. An attacker could exploit this vulnerability by elevating their read-only permissions to those of a high-privileged user. A successful exploit could allow the attacker to access or modify configuration settings within Cisco Catalyst SD-WAN Manager as a high-privileged user.	2026-05-14	5.4
CVE-2026-8539	google - chrome	Script injection in SanitizerAPI in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: High)	2026-05-14	5.4
CVE-2026-8561	google - chrome	Incorrect security UI in Fullscreen in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	5.4
CVE-2024-0391	wso2 - multiple products	The check user account lock states feature within the email OTP flow fails to validate user input, allowing an attacker to infer the existence of registered user accounts. The discovery of valid usernames can increase the risk of brute-force and social engineering attacks. Attackers can leverage this information to craft targeted phishing campaigns or other malicious activities aimed at tricking users into divulging sensitive data, potentially damaging the organization's reputation and leading to regulatory non-compliance and financial consequences.	2026-05-11	5.3
CVE-2025-8154	wso2 - api_control_plane	In Webhook API invocations, the component accepts user-supplied input for HTTP request headers without sufficient validation or sanitization, allowing these headers to be injected into HTTP responses.	2026-05-11	5.3

		By exploiting this vulnerability, a malicious actor can inject or overwrite arbitrary HTTP response headers. This can lead to various adverse effects, including the manipulation of browser caching, alteration of security-related headers, and the injection of sensitive information such as cookie values, potentially enabling session hijacking or other malicious activities.		
CVE-2026-28994	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, watchOS 26.5. An attacker in a privileged network position may be able to perform denial-of-service attack using crafted Wi-Fi packets.	2026-05-11	5.3
CVE-2026-8391	mozilla - firefox	Other issue in the JavaScript Engine component. This vulnerability was fixed in Firefox 150.0.3, Firefox ESR 115.36, Firefox ESR 140.11, and Thunderbird 140.11.	2026-05-12	5.3
CVE-2025-67604	fortinet - multiple products	A use of potentially dangerous function vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.4, FortiAnalyzer 7.4.0 through 7.4.8, FortiAnalyzer 7.2 all versions, FortiAnalyzer 7.0 all versions, FortiAnalyzer 6.4 all versions, FortiManager 7.6.0 through 7.6.4, FortiManager 7.4.0 through 7.4.8, FortiManager 7.2 all versions, FortiManager 7.0 all versions, FortiManager 6.4 all versions may allow an authenticated attacker to cause a system hang via multiple specially crafted HTTP requests causing crashes. This happens if internal locks are aligned, which is out of control of the attacker.	2026-05-12	5.3
CVE-2026-42177	siemens - linux-entra-sso	linux-entra-sso is a browser plugin for Linux to SSO on Microsoft Entra ID. Prior to 1.8.1, platform/chrome/js/platform-chrome.js:69-88 registers a single declarativeNetRequest rule whose urlFilter is Platform.SSO_URL + "/*", i.e. "https://login.microsoftonline.com/*". Chrome's urlFilter without a | or || anchor is substring-matched against the full request URL. The same applied rule action is modifyHeaders that attaches the Entra ID Primary Refresh Token cookie. The Firefox adapter in platform/firefox/js/platform-firefox.js:53 performs a belt-and-braces startsWith(Platform.SSO_URL) check before injecting the header; the Chrome adapter does not. When the extension holds broad host permissions through the optional_host_permissions: ["https://*/*"] declared in platform/chrome/manifest.json:34, a main-frame navigation to a URL whose path embeds https://login.microsoftonline.com/ causes Chrome to attach the PRT cookie to the request to the attacker-controlled host. This vulnerability is fixed in 1.8.1.	2026-05-12	5.3
CVE-2026-23822	hewlett packard enterprise (hpe) - ArubaOS (AOS)	A vulnerability in the XML handling component of AOS-8 DHCP services could allow an unauthenticated remote attacker to trigger a denial-of-service condition. Successful exploitation could allow an attacker to cause excessive resource consumption upon user interaction, leading to service disruption or reduced availability of the affected system. NOTE: This vulnerability only impacts Access Points running AOS Instant 8.x.x.x	2026-05-12	5.3
CVE-2026-34654	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier are affected by a Dependency on Vulnerable Third-Party Component vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-05-12	5.3
CVE-2026-8202	mongodb - multiple products	Using a densely populated chars mask and a large input string in the MongoDB aggregation operators $trim, $ltrim, and $rtrim, an authenticated user with aggregation permissions can pin CPU utilization at 100% for an extended period of time. This issue impacts MongoDB Server v7.0 versions prior to 7.0.34, v8.0 versions prior to 8.0.23, v8.2 versions prior to 8.2.9 and v8.3 versions prior to 8.3.2.	2026-05-13	5.3
CVE-2026-40703	f5 - BIG-IP	A cross-site request forgery (CSRF) vulnerability exists in the dashboard of the BIG-IP Configuration utility. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	5.3
CVE-2026-42058	f5 - BIG-IP	An authenticated attacker's undisclosed requests to BIG-IP iControl REST can lead to an information leak of BIG-IP local user account names. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-05-13	5.3
CVE-2026-45205	apache - commons_configuration	Uncontrolled Recursion vulnerability in Apache Commons. When processing an untrusted configuration file, Commons Configuration will throw a StackOverflowError for YAML input with cycles. This issue affects Apache Commons: from 2.2 before 2.15.0. Users are recommended to upgrade to version 2.15.0, which fixes the issue.	2026-05-14	5.3
CVE-2026-8516	google - chrome	Insufficient validation of untrusted input in DataTransfer in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who convinced a user to engage in specific UI gestures to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Critical)	2026-05-14	5.3
CVE-2026-8535	google - chrome	Out of bounds read in Media in Google Chrome on Linux and ChromeOS prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted JPEG file. (Chromium security severity: High)	2026-05-14	5.3
CVE-2026-8538	google - chrome	Insufficient validation of untrusted input in GPU in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform a denial of service via a crafted HTML page. (Chromium security severity: High)	2026-05-14	5.3
CVE-2026-8541	google - chrome	Out of bounds read in UI in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-05-14	5.3

CVE-2026-8543	google - chrome	Out of bounds read in FileSystem in Google Chrome on Mac prior to 148.0.7778.168 allowed a remote attacker who convinced a user to engage in specific UI gestures to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-05-14	5.3
CVE-2026-8546	google - chrome	Out of bounds read in GPU in Google Chrome on Mac and Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-05-14	5.3
CVE-2026-8582	google - chrome	Object lifecycle issue in Dawn in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	5.3
CVE-2026-8583	google - chrome	Insufficient policy enforcement in WebXR in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	5.3
CVE-2026-21016	samsung - multiple products	Incorrect privilege assignment in LocationManager prior to SMR May-2026 Release 1 allows local attackers to access sensitive information.	2026-05-13	5.1
CVE-2026-21020	samsung - multiple products	Improper export of android application components in OmaCP prior to SMR May-2026 Release 1 allows local attackers to trigger privileged functions.	2026-05-13	5.1
CVE-2026-21021	samsung - multiple products	Improper input validation in Routines prior to SMR May-2026 Release 1 allows physical attackers to launch privileged activity.	2026-05-13	5.1
CVE-2020-37233	wordpress - Buddypress	WordPress Plugin Buddypress 6.2.0 contains a persistent cross-site scripting vulnerability that allows authenticated attackers with moderator privileges to inject malicious script code through the figure parameter in wp:html blocks. Attackers can inject iframe elements with event handlers like onload that execute when administrators or privileged users preview or view the affected page content, enabling session hijacking and persistent phishing attacks.	2026-05-16	5.1
CVE-2026-28967	apple - multiple products	A denial-of-service issue was addressed with improved input validation. This issue is fixed in iOS 18.7.7 and iPadOS 18.7.7, iOS 26.4 and iPadOS 26.4. An attacker in a privileged network position may be able to cause a denial-of-service.	2026-05-11	4.9
CVE-2026-44874	arubanetworks - multiple products	A vulnerability exists in the web-based management interface of an AOS-10 Gateway that could allow an authenticated remote attacker to access sensitive files on the underlying operating system. Successful exploitation of this vulnerability could result in the disclosure of confidential system information, potentially enabling further attacks against the affected device.	2026-05-12	4.9
CVE-2026-20793	intel - quickassist_technology	Unchecked return value for some Intel(R) QAT software drivers for Windows before version 1.13 within Ring 3: User Applications may allow a denial of service. Unprivileged software adversary with an authenticated user combined with a low complexity attack may enable denial of service. This result may potentially occur via local access when attack requirements are not present without special internal knowledge and requires no user interaction. The potential vulnerability may impact the confidentiality (none), integrity (none) and availability (low) of the vulnerable system, resulting in subsequent system confidentiality (none), integrity (none) and availability (none) impacts.	2026-05-12	4.8
CVE-2026-34655	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-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. Scope is changed.	2026-05-12	4.8
CVE-2026-34658	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-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. Scope is changed.	2026-05-12	4.8
CVE-2026-8200	mongodb - multiple products	When schema validation is enabled on a collection and an update or insert would violate the collection's schema, the local server log message generated may not have all user data redacted. This issue impacts MongoDB Server v7.0 versions prior to 7.0.34, v8.0 versions prior to 8.0.23, v8.2 versions prior to 8.2.9 and v8.3 versions prior to 8.3.2.	2026-05-13	4.8
CVE-2026-28830	apple - macos	A race condition was addressed with additional validation. This issue is fixed in macOS Tahoe 26.4. An app may be able to access sensitive user data.	2026-05-11	4.7
CVE-2026-28992	apple - multiple products	A memory corruption vulnerability was addressed with improved locking. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. An attacker may be able to cause unexpected app termination.	2026-05-11	4.7
CVE-2026-43659	apple - multiple products	A race condition was addressed with additional validation. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, visionOS 26.5. An app may be able to access sensitive user data.	2026-05-11	4.7
CVE-2026-8565	google - chrome	Inappropriate implementation in Downloads in Google Chrome on Mac prior to 148.0.7778.168 allowed an attacker who convinced a user to install a malicious extension to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-05-14	4.7
CVE-2026-28961	apple - macos	This issue was addressed with improved checks. This issue is fixed in macOS Tahoe 26.5. An attacker with physical access to a locked device may be able to view sensitive user information.	2026-05-11	4.6
CVE-2026-28963	apple - multiple products	A privacy issue was addressed by removing the vulnerable code. This issue is fixed in iOS 26.5 and iPadOS 26.5. An attacker with physical access may be able to use Visual Intelligence to access sensitive user data during iPhone Mirroring.	2026-05-11	4.6
CVE-2026-7257	zyxel - wre6505_firmware	** UNSUPPORTED WHEN ASSIGNED ** An insecure storage of sensitive information vulnerability in the configuration file of Zyxel WRE6505 v2 firmware version V1.00(ABDV.3)C0 could allow a local attacker with administrator privileges to download and decrypt a backup configuration file.	2026-05-12	4.4
CVE-2026-7431	ivanti - multiple products	An incorrect permission assignment for critical resource of Ivanti Secure Access Client before 22.8R6 allows a local authenticated user to read or modify sensitive log data via write access to a shared memory section.	2026-05-12	4.4

CVE-2026-32209	microsoft - multiple products	Improper access control in Windows Filtering Platform (WFP) allows an authorized attacker to bypass a security feature locally.	2026-05-12	4.4
CVE-2026-41100	microsoft - 365_copilot	Improper access control in M365 Copilot allows an authorized attacker to perform spoofing locally.	2026-05-12	4.4
CVE-2026-28901	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in Safari 26.5, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-05-11	4.3
CVE-2026-28917	apple - multiple products	The issue was addressed with improved input validation. This issue is fixed in Safari 26.5, iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing maliciously crafted web content may lead to an unexpected process crash.	2026-05-11	4.3
CVE-2026-28971	apple - multiple products	The issue was addressed with improved UI handling. This issue is fixed in Safari 26.5, iOS 26.5 and iPadOS 26.5, macOS Tahoe 26.5, visionOS 26.5. A malicious iframe may use another website’s download settings.	2026-05-11	4.3
CVE-2026-39869	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, macOS Sequoia 15.7.7, macOS Sonoma 14.8.7, macOS Tahoe 26.5, tvOS 26.5, visionOS 26.5, watchOS 26.5. Processing an audio stream in a maliciously crafted media file may terminate the process.	2026-05-11	4.3
CVE-2026-25690	fortinet - multiple products	An improper neutralization of argument delimiters in a command ('argument injection') vulnerability in Fortinet FortiDeceptor 6.0.0 through 6.0.2, FortiDeceptor 5.3.0 through 5.3.3, FortiDeceptor 5.2.0 through 5.2.1, FortiDeceptor 5.1 all versions, FortiDeceptor 5.0 all versions may allow an authenticated attacker with at least read-only admin permission to read log files via HTTP crafted requests.	2026-05-12	4.3
CVE-2026-32175	microsoft - multiple products	A tampering vulnerability exists when .NET Core improperly handles specially crafted files. An attacker who successfully exploited this vulnerability could write arbitrary files and directories to certain locations on a vulnerable system. However, an attacker would have limited control over the destination of the files and directories. To exploit the vulnerability, an attacker must send a specially crafted file to a vulnerable system. The security update fixes the vulnerability by ensuring .NET Core properly handles files.	2026-05-12	4.3
CVE-2026-35429	microsoft - edge	User interface (ui) misrepresentation of critical information in Microsoft Edge for Android allows an unauthorized attacker to perform spoofing over a network.	2026-05-12	4.3
CVE-2026-40416	microsoft - edge_chromium	User interface (ui) misrepresentation of critical information in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-05-12	4.3
CVE-2026-40421	microsoft - multiple products	External control of file name or path in Microsoft Office Word allows an unauthorized attacker to disclose information over a network.	2026-05-12	4.3
CVE-2026-34656	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier are affected by an Improper Authorization vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page.	2026-05-12	4.3
CVE-2026-28374	grafana - Grafana OSS	Editors could delete any annotation, even those they do not have read access to. The editor user cannot create or read the annotations.	2026-05-13	4.3
CVE-2026-8528	google - chrome	Insufficient validation of untrusted input in SiteIsolation in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to bypass Site Isolation via a crafted HTML page. (Chromium security severity: High)	2026-05-14	4.3
CVE-2026-8537	google - chrome	Insufficient policy enforcement in ViewTransitions in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-05-14	4.3
CVE-2026-8552	google - chrome	Heap buffer overflow in GPU in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	2026-05-14	4.3
CVE-2026-8559	google - chrome	Integer overflow in Internationalization in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	2026-05-14	4.3
CVE-2026-8560	google - chrome	Heap buffer overflow in SwiftShader in Google Chrome on Mac and iOS prior to 148.0.7778.168 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	4.3
CVE-2026-8562	google - chrome	Side-channel information leakage in Navigation in Google Chrome prior to 148.0.7778.168 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	4.3
CVE-2026-8563	google - chrome	Insufficient policy enforcement in IFrame Sandbox in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	4.3
CVE-2026-8566	google - chrome	Insufficient policy enforcement in Payments in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	4.3
CVE-2026-8567	google - chrome	Integer overflow in ANGLE in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	4.3
CVE-2026-8576	google - chrome	Inappropriate implementation in CORS in Google Chrome on Linux and ChromeOS prior to 148.0.7778.168 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	4.3
CVE-2026-8564	google - chrome	Incorrect security UI in Downloads in Google Chrome on Android and Mac prior to 148.0.7778.168 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	4.2
CVE-2026-8584	google - chrome	Inappropriate implementation in Views in Google Chrome on iOS prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	4.2
CVE-2026-43514	apache - multiple products	Observable Timing Discrepancy vulnerability when comparing AJP secret in Apache Tomcat.	2026-05-12	3.7

		This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.21, from 10.1.0-M1 through 10.1.54, from 9.0.0.M1 through 9.0.117, from 8.5.0 through 8.5.100, from 7.0.0 through 7.0.109. Older unsupported versions may also be affected. Users are recommended to upgrade to version 11.0.22, 10.1.55 or 9.0.118 which fix the issue.		
CVE-2026-41962	huawei - HarmonyOS	Permission control vulnerability in the app management and control module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-05-15	3.6
CVE-2026-34685	adobe - multiple products	Adobe Commerce versions 2.4.9-beta1, 2.4.8-p4, 2.4.7-p9, 2.4.6-p14, 2.4.5-p16, 2.4.4-p17 and earlier [NEEDS REVIEW: impact mismatch — ticket says 'Arbitrary file system write', CIA triad derives 'Security Feature Bypass'. Verify CVSS vector before publishing.] are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A high-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	2026-05-12	3.4
CVE-2026-28910	apple - macos	This issue was addressed with improved permissions checking. This issue is fixed in macOS Tahoe 26.4. A malicious app may be able to access arbitrary files.	2026-05-11	3.3
CVE-2026-28957	apple - multiple products	An issue with app access to camera metadata was addressed with improved logic. This issue is fixed in iOS 18.7.9 and iPadOS 18.7.9, iOS 26.5 and iPadOS 26.5, visionOS 26.5. An app may be able to capture a user's screen.	2026-05-11	3.3
CVE-2026-8536	google - chrome	Insufficient validation of untrusted input in ReadingMode in Google Chrome on Mac prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to bypass site Isolation via a crafted HTML page. (Chromium security severity: High)	2026-05-14	3.1
CVE-2026-8545	google - chrome	Object corruption in Compositing in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-05-14	3.1
CVE-2026-8553	google - chrome	Use after free in GPU in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	2026-05-14	3.1
CVE-2026-8554	google - chrome	Type Confusion in ANGLE in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page. (Chromium security severity: High)	2026-05-14	3.1
CVE-2026-8556	google - chrome	Inappropriate implementation in ANGLE in Google Chrome on Windows prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-05-14	3.1
CVE-2026-8568	google - chrome	Insufficient policy enforcement in AI in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to bypass Site Isolation via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	3.1
CVE-2026-8572	google - chrome	Insufficient policy enforcement in Network in Google Chrome on Android prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	3.1
CVE-2026-8578	google - chrome	Out of bounds read in GPU in Google Chrome on Linux prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-05-14	3.1
CVE-2026-8579	google - chrome	Insufficient validation of untrusted input in Skia in Google Chrome prior to 148.0.7778.168 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted print file. (Chromium security severity: Medium)	2026-05-14	3.1
CVE-2026-7262	php - multiple products	In PHP versions 8.2.* before 8.2.31, 8.3.* before 8.3.31, 8.4.* before 8.4.21, and 8.5.* before 8.5.6, when a SOAP server has a typemap configured, the decoding process contains a mistake which checks the wrong variable in case of missing value element. This leads to dereferences a NULL pointer, causing a segmentation fault. This allows a remote unauthenticated attacker to crash the PHP SOAP server process, resulting in denial of service.	2026-05-10	2.9
CVE-2026-32684	hikvision - Hik-Connect APP	The application does not impose strict enough restrictions on directory access permissions, posing a risk that other malicious applications could obtain sensitive information.	2026-05-12	2.9
CVE-2026-41963	huawei - HarmonyOS	Stack overflow vulnerability in the media platform. Impact: Successful exploitation of this vulnerability may affect availability.	2026-05-15	2.8
CVE-2026-44278	fortinet - forticlient	A use of hard-coded cryptographic key vulnerability in Fortinet FortiClientWindows 7.4.0 through 7.4.2, FortiClientWindows 7.2 all versions may allow attacker to information disclosure via <insert attack vector here>	2026-05-12	2.3
CVE-2026-7259	php - multiple products	In PHP versions 8.2.* before 8.2.31, 8.3.* before 8.3.31, 8.4.* before 8.4.21, and 8.5.* before 8.5.6, a mismatch between encoding lists in Oniguruma and mbfl leads to a NULL pointer dereference, resulting in a segmentation fault and denial of service. The vulnerability is exploitable when user-controlled input can influence the encoding passed to mb_regex_encoding().	2026-05-10	2.1

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.