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 12 يوليو إلى 18 يوليو. 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 12th of July to 18th of July. 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-2026-56451	siemens - Opcenter X	A vulnerability has been identified in Opcenter X (All versions < V2604). Affected applications do not properly validate the algorithm specified in the JSON Web Token (JWT) header._x000D_ This could allow an unauthenticated remote attacker to forge arbitrary JWT, bypass authentication mechanisms and impersonate any user including administrative accounts, potentially gaining full unauthorized access to the application.	2026-07-14	10
CVE-2026-15409	sonicwall - multiple products	A Server-side request forgery (SSRF) vulnerability has been identified in the SMA1000 Appliance Work Place interface. A remote unauthenticated attacker could potentially cause the appliance to make requests to unintended location.	2026-07-14	10
CVE-2026-57092	microsoft - multiple products	Use after free in Windows VMSwitch allows an authorized attacker to elevate privileges over a network.	2026-07-14	9.9
CVE-2026-48318	adobe - multiple products	ColdFusion is 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 does not require user interaction. Scope is changed.	2026-07-14	9.9
CVE-2026-62390	apache - kylin	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Apache Kylin. A backend API refreshing table catalog may cause the injection to the generated SQL. This issue affects Apache Kylin: from 4 through 5.0.3. Users are recommended to upgrade to version 5.0.4, which fixes the issue.	2026-07-14	9.8
CVE-2026-62392	apache - kylin	Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability in Apache Kylin. A backend API may bring job config parameters to OS command line. This issue affects Apache Kylin: from 4 through 5.0.3. Users are recommended to upgrade to version 5.0.4, which fixes the issue.	2026-07-14	9.8
CVE-2026-42990	microsoft - multiple products	Heap-based buffer overflow in SQL Server ODBC driver allows an unauthorized attacker to execute code over a network.	2026-07-14	9.8
CVE-2026-49172	microsoft - multiple products	Heap-based buffer overflow in Windows FTP Service allows an unauthorized attacker to execute code over a network.	2026-07-14	9.8
CVE-2026-50522	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office SharePoint allows an unauthorized attacker to execute code over a network.	2026-07-14	9.8
CVE-2026-54990	microsoft - multiple products	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-07-14	9.8
CVE-2026-58644	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office SharePoint allows an unauthorized attacker to execute code over a network.	2026-07-14	9.8

CVE-2026-50447	microsoft - multiple products	Heap-based buffer overflow in Windows Message Queuing allows an unauthorized attacker to execute code over a network.	2026-07-14	9.8
CVE-2026-50518	microsoft - multiple products	Heap-based buffer overflow in Windows DHCP Server allows an unauthorized attacker to execute code over a network.	2026-07-14	9.8
CVE-2026-55010	microsoft - minecraft_bedrock_dedicated_server	Heap-based buffer overflow in Minecraft Bedrock Dedicated Server allows an unauthorized attacker to execute code over a network.	2026-07-14	9.8
CVE-2026-55944	microsoft - dynamics_nav	Deserialization of untrusted data in Microsoft Dynamics NAV allows an unauthorized attacker to execute code over a network.	2026-07-14	9.8
CVE-2026-56159	microsoft - multiple products	Heap-based buffer overflow in Windows DHCP Server allows an unauthorized attacker to execute code over a network.	2026-07-14	9.8
CVE-2026-56188	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Server Network driver allows an unauthorized attacker to execute code over a network.	2026-07-14	9.8
CVE-2026-56190	microsoft - multiple products	Use of uninitialized resource in Windows RDP allows an unauthorized attacker to execute code over a network.	2026-07-14	9.8
CVE-2026-48561	microsoft - multiple products	Improper neutralization of special elements used in a command ('command injection') in Microsoft Copilot allows an unauthorized attacker to execute code over a network.	2026-07-14	9.6
CVE-2026-55008	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.	2026-07-14	9.6
CVE-2026-50380	microsoft - multiple products	Heap-based buffer overflow in Windows GDI+ allows an unauthorized attacker to execute code over a network.	2026-07-14	9.6
CVE-2026-48259	adobe - multiple products	Adobe Experience Manager is affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in arbitrary code execution in the context of the current user. A low-privileged attacker could leverage this vulnerability to issue unauthorized server-side requests, potentially gaining elevated access or control over the victim's account or session. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	9.6
CVE-2026-48359	adobe - multiple products	Adobe Experience Manager is affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could result in arbitrary code execution in the context of the current user. A low-privileged attacker could exploit this vulnerability to read sensitive files, potentially gaining elevated access or control over the victim's account or session. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	9.6
CVE-2026-15773	google - chrome	Use after free in Core in Google Chrome on Windows prior to 150.0.7871.125 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-14	9.6
CVE-2026-48284	adobe - multiple products	ColdFusion is affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	9.6
CVE-2026-48322	adobe - multiple products	ColdFusion is affected by an Improper Control of Generation of Code ('Code Injection') vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	9.6
CVE-2026-49798	microsoft - multiple products	Use after free in Windows Kernel allows an unauthorized attacker to elevate privileges locally.	2026-07-14	9.3
CVE-2026-48356	adobe - multiple products	Adobe Commerce is affected by an Unrestricted Upload of File with Dangerous Type vulnerability that could result in arbitrary code execution in the context of the current user, 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.	2026-07-14	9.3
CVE-2026-48321	adobe - multiple products	ColdFusion is affected by an Incorrect Authorization vulnerability that could result in privilege escalation. An attacker could leverage this vulnerability to gain unauthorized read and write access. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	9.3
CVE-2026-48325	adobe - multiple products	ColdFusion is affected by a Missing Authentication for Critical Function vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	9.3
CVE-2026-48334	adobe - multiple products	Illustrator is affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user, 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 open a malicious file. Scope is changed.	2026-07-14	9.3
CVE-2026-54733	microsoft - o365-moodle	The Microsoft 365 and Microsoft Entra ID Plugins for Moodle provide Office 365 and Azure Active Directory integration for Moodle. Prior to 4.5.6, 5.0.5, and 5.1.1, the Microsoft Office 365 Integration plugin local_o365 Teams SSO endpoint sso_login.php base64-decodes a JWT payload and authenticates users from the upn claim without verifying the JWT signature, allowing an unauthenticated attacker to forge a token and obtain a Moodle session as an O365-authenticated user. This issue is fixed in versions 4.5.6, 5.0.5, and 5.1.1.	2026-07-16	9.3
CVE-2026-59864	microsoft - kiota	Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.32.5, `kiota plugin add` and `kiota plugin generate` (with `-t APIPlugin`) emitted attacker-controlled static_template.file values from x-ai-adaptive-card and x-ai-capabilities into generated Microsoft 365 Copilot and Teams plugin manifests without path validation, allowing ../, absolute, rooted, UNC, Windows drive, or URI paths in response_semantics.static_template.file to cause path traversal or out-of-package file inclusion when the generated plugin was deployed. This issue is fixed in version 1.32.5.	2026-07-16	9.3

CVE-2026-59865	microsoft - kiota	Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.32.5, `kiota info` read x-ms-kiota-info.languagesInformation.<language>.dependencyInstallCommand plus dependency name and version values from an OpenAPI description and presented the spec-supplied command as Kiota's recommended install command, allowing an attacker-controlled or compromised description to cause command injection when the suggested command was run manually or through the Kiota VS Code extension's kiota info --json dependency-install flow. This issue is fixed in version 1.32.5.	2026-07-16	9.3
CVE-2026-59866	microsoft - kiota	Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.32.5, Kiota emitted x-ms-kiota-info clientClassName and clientNamespaceName values without identifier or path sanitization as both generated client class or namespace names and generated output path components when `kiota generate` ran without -c/--class-name, allowing an attacker-controlled or compromised OpenAPI description to write generated source outside the -o output directory and inject arbitrary text into generated class or namespace declarations. This issue is fixed in version 1.32.5 by GenerationConfiguration.SanitizeClientClassName and SanitizeClientNamespaceName.	2026-07-16	9.3
CVE-2026-42533	f5 - multiple products	A vulnerability exists in NGINX Plus and NGINX Open Source when a map directive uses regex matching and a string expression references the map's regex capture variables before referencing the map output variable. Alternatively, the same result could be achieved by using a non-cacheable variable in a string expression under certain conditions. An unauthenticated attacker along with conditions beyond their 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. Impact: This vulnerability may allow remote attackers to cause a denial-of-service (DoS) on the NGINX system or to possibly trigger a code execution. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-07-15	9.2
CVE-2026-41041	apache - gravitino	URL path injection via unencoded user-supplied identifiers vulnerability in Apache Gravitino. This issue affects Apache Gravitino: from 1.0.0 before 1.2.1. Users are recommended to upgrade to version 1.2.1, which fixes the issue.	2026-07-13	9.1
CVE-2026-59083	apache - multiple products	Improper Handling of URL Encoding (Hex Encoding) vulnerability in Apache Tomcat's rewrite valve allowed security constraint bypass for some configurations. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.23, from 10.1.0-M1 through 10.1.56, from 9.0.0.M1 through 9.0.119, from 8.5.0 through 8.5.100. Other versions that have reached end of support may also be affected. Users are recommended to upgrade to version 11.0.24, 10.1.57 or 9.0.120, which fix the issue.	2026-07-14	9.1
CVE-2026-59084	apache - multiple products	Insufficient Technical Documentation vulnerability in Apache Tomcat since the requirements to securely configure the EncryptInterceptor were not clearly documented. This issue affects Apache Tomcat: from 11.0.0-M1 through 11.0.23, from 10.1.0-M1 through 10.1.56, from 9.0.13 through 9.0.119, from 8.5.38 through 8.5.100, from 7.0.100 through 7.0.109. Other versions that have reached end of support may also be affected. Users are recommended to upgrade to version 11.0.24, 10.1.57 or 9.0.120 which fix the issue.	2026-07-14	9.1
CVE-2026-58319	apache - doris	Certain Apache Doris FE HTTP REST administrative APIs were accessible without proper authentication. An unauthenticated attacker with network access to the FE HTTP service could perform unauthorized administrative operations, potentially affecting cluster integrity and availability and leading to cluster instability or denial of service. This issue affects Apache Doris versions prior to 3.1.0. Users are advised to upgrade to Apache Doris 3.1.0 or later.	2026-07-14	9.1
CVE-2026-55040	microsoft - multiple products	Weak authentication in Microsoft Office SharePoint allows an unauthorized attacker to bypass a security feature over a network.	2026-07-14	9.1
CVE-2026-48358	adobe - multiple products	Adobe Commerce is affected by an Improper Encoding or Escaping of Output vulnerability that could result in arbitrary code execution in the context of the current user. An attacker with high privileges could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	9.1
CVE-2026-48319	adobe - multiple products	ColdFusion is affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in arbitrary code execution in the context of the current user. An attacker with high privileges could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	9.1
CVE-2026-48324	adobe - multiple products	ColdFusion is affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could result in arbitrary code execution in the context of the current user. An attacker with high privileges could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	9.1
CVE-2026-48327	adobe - multiple products	ColdFusion is affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	9

CVE-2026-47632	microsoft - multiple products	Improper certificate validation in Azure Monitor Agent allows an unauthorized attacker to elevate privileges over an adjacent network.	2026-07-14	8.8
CVE-2026-48564	microsoft - multiple products	Heap-based buffer overflow in Windows DHCP Server allows an authorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-49178	microsoft - multiple products	Heap-based buffer overflow in Active Directory Domain Services allows an authorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-49795	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	8.8
CVE-2026-50342	microsoft - multiple products	Improper access control in Windows MIDI Service Module allows an authorized attacker to elevate privileges locally.	2026-07-14	8.8
CVE-2026-50663	microsoft - age_of_empires_ii	Relative path traversal in Age of Empires II: Definitive Edition Game allows an unauthorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-54107	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-07-14	8.8
CVE-2026-54117	microsoft - multiple products	Deserialization of untrusted data in SQL Server allows an authorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-54118	microsoft - multiple products	Deserialization of untrusted data in SQL Server allows an authorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-54982	microsoft - multiple products	Integer underflow (wrap or wraparound) in Reliable Multicast Transport Driver (RMCAST) allows an unauthorized attacker to execute code over an adjacent network.	2026-07-14	8.8
CVE-2026-54999	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows TCP/IP allows an unauthorized attacker to execute code over an adjacent network.	2026-07-14	8.8
CVE-2026-55005	microsoft - multiple products	Heap-based buffer overflow in Microsoft Exchange Server allows an authorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-57969	microsoft - azure_cyclecloud	Missing authentication for critical function in Azure CycleCloud allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-58608	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Print Spooler Components allows an authorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-47295	microsoft - multiple products	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-50360	microsoft - multiple products	Incorrect implementation of authentication algorithm in Windows SMB Server allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-50369	microsoft - multiple products	Use after free in Windows Remote Desktop Services allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-50370	microsoft - multiple products	Heap-based buffer overflow in Windows DHCP Server allows an unauthorized attacker to execute code over an adjacent network.	2026-07-14	8.8
CVE-2026-50382	microsoft - multiple products	Untrusted pointer dereference in Windows DirectX allows an authorized attacker to execute code locally.	2026-07-14	8.8
CVE-2026-50385	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	8.8
CVE-2026-50398	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-50413	microsoft - multiple products	Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	8.8
CVE-2026-50438	microsoft - pc_manager	Improper link resolution before file access ('link following') in Microsoft PC Manager allows an authorized attacker to elevate privileges locally.	2026-07-14	8.8
CVE-2026-50444	microsoft - multiple products	Missing authentication for critical function in Windows Server Update Service allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-50474	microsoft - multiple products	Use after free in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-50477	microsoft - multiple products	Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	8.8
CVE-2026-50489	microsoft - multiple products	Heap-based buffer overflow in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-07-14	8.8

CVE-2026-50666	microsoft - multiple products	Use after free in Windows Remote Access Connection Manager allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-50670	microsoft - multiple products	Out-of-bounds read in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	8.8
CVE-2026-50687	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	8.8
CVE-2026-50692	microsoft - multiple products	Heap-based buffer overflow in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	2026-07-14	8.8
CVE-2026-54121	microsoft - multiple products	Improper authorization in Active Directory Certificate Services (AD CS) allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-55052	microsoft - multiple products	Missing authorization in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-56194	microsoft - multiple products	Heap-based buffer overflow in Windows Network File System allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-56196	microsoft - windows_admin_center	Relative path traversal in Windows Admin Center allows an authorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-56197	microsoft - windows_admin_center	Improper neutralization of special elements used in a command ('command injection') in Windows Admin Center allows an authorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-56642	microsoft - fabric_data_warehouse	Stack-based buffer overflow in Microsoft Fabric Data Warehouse allows an authorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-56647	microsoft - multiple products	Integer overflow or wraparound in Windows Remote Access Service Infrastructure allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-57087	microsoft - multiple products	Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-57090	microsoft - multiple products	Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-57094	microsoft - multiple products	Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-57102	microsoft - visual_studio_code	Inclusion of functionality from untrusted control sphere in Visual Studio Code allows an unauthorized attacker to bypass a security feature over a network.	2026-07-14	8.8
CVE-2026-58277	microsoft - multiple products	Improper authorization in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-58534	microsoft - multiple products	Heap-based buffer overflow in Microsoft Input Method Editor (IME) allows an authorized attacker to elevate privileges locally.	2026-07-14	8.8
CVE-2026-58594	microsoft - multiple products	Integer overflow or wraparound in Windows RDP allows an unauthorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-58626	microsoft - multiple products	Use after free in Windows Remote Desktop Services allows an authorized attacker to execute code over a network.	2026-07-14	8.8
CVE-2026-47300	microsoft - multiple products	Incorrect implementation of authentication algorithm in ASP.NET Core allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-47301	microsoft - multiple products	Improper access control in Microsoft Configuration Manager allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-47303	microsoft - multiple products	Authentication bypass by assumed-immutable data in ASP.NET Core allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.8
CVE-2026-15767	google - chrome	Heap buffer overflow in libyuv in Google Chrome on Windows prior to 150.0.7871.125 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted video file. (Chromium security severity: High)	2026-07-14	8.8
CVE-2026-15776	google - chrome	Inappropriate implementation in V8 in Google Chrome prior to 150.0.7871.125 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-14	8.8
CVE-2026-50130	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 6.4.2, a user with code execution as the unprivileged pihole user can escalate to root by replacing /etc/pihole/logrotate. The replacement is laundered to root:root ownership by pihole-FTL-prestart.sh and then parsed as root by the daily pihole flush cron, executing firstaction shell as uid 0. This issue is fixed in version 6.4.3.	2026-07-14	8.8
CVE-2026-35152	apache - fineract	A SQL Injection vulnerability exists in Apache Fineract's Report Execution API (runreports endpoint) in versions up to and including 1.14.0. Report parameter values are incorporated into the generated SQL query without sufficient validation, allowing an authenticated user with	2026-07-15	8.8

		permission to run reports to inject arbitrary SQL via crafted parameter values. This can be leveraged to perform unauthorized access to data beyond what the report was designed to expose. Users are recommended to upgrade to a version containing the fix.		
CVE-2026-60005	f5 - multiple products	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_slice_module module. When the slice directive and unnamed regex captures are configured or when a background cache update happens, unauthenticated attackers can send requests that may cause uninitialized memory access in the NGINX worker process, leading to limited disclosure of memory or a restart. Impact: This vulnerability may allow remote, unauthenticated attackers to have limited control to disclose memory contents or restart the NGINX worker process. There is no control plane exposure; this is a data plane issue only. Note: The ngx_http_slice_module module is not enabled by default; it's enabled with the --with-http_slice_module configuration parameter. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-07-15	8.8
CVE-2026-20150	cisco - Cisco RoomOS Software	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco RoomOS engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities._x000D_ _x000D_ The vulnerabilities tracked by CVE-2026-20150 are related to improper access control that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-284.	2026-07-15	8.8
CVE-2026-5674	red hat - multiple products	A flaw was found in PipeWire, a multimedia server. This vulnerability allows an attacker to escape sandboxed applications, such as Flatpak, by exploiting PipeWire's PulseAudio compatibility layer. An attacker with minimal permissions within a sandboxed environment can load a malicious library, leading to arbitrary code execution outside the sandbox and potential compromise of the user's system.	2026-07-16	8.8
CVE-2026-14371	lenovo - XClarity Integrator for Microsoft Windows Admin Center	The Lenovo XClarity Integrator for Windows Admin Center plugin version 5.1.1 and below running on the WAC Gateway is vulnerable to Powershell Command Injection when establishing remote PowerShell commands.	2026-07-16	8.8
CVE-2026-15483	trendnet - TEW-821DAP	A security vulnerability has been detected in TRENDnet TEW-821DAP 1.12B01. Impacted is the function sub_41EC14 of the file /goform/tools_nslookup of the component ssi. The manipulation of the argument nslookup_target leads to buffer overflow. It is possible to initiate the attack remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer.	2026-07-12	8.7
CVE-2026-15484	trendnet - TEW-821DAP	A vulnerability was detected in TRENDnet TEW-821DAP 1.12B01. The affected element is the function sub_41EC14 of the file /goform/tools_nslookup of the component ssi. The manipulation results in buffer overflow. It is possible to launch the attack remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer.	2026-07-12	8.7
CVE-2026-47994	adobe - multiple products	Adobe Commerce is 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.	2026-07-14	8.7
CVE-2026-55723	f5 - multiple products	When NGINX Ingress Controller is configured with Custom Resource Definitions (CRDs) or Ingress annotations, an injection vulnerability exists in the configuration generator of NGINX Ingress Controller. Multiple user-controllable fields are written into the generated NGINX configuration without sanitization. An authenticated attacker with permission to create or modify these CRDs or annotations may craft values that inject arbitrary NGINX configuration directives. Impact: An authenticated attacker granted write access to NGINX Ingress Controller CRDs or Ingress annotations through the Kubernetes API may be able to inject arbitrary NGINX configuration directives, create or delete files, or disable services. There is no data plane exposure; this is a control plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-07-15	8.7
CVE-2026-59762	f5 - multiple products	When an HTTP/2 profile is configured on a virtual server, undisclosed requests can cause an increase in memory resource utilization. Impact: System performance can degrade until the TMM process is either forced to restart or is	2026-07-15	8.7

		manually restarted. This vulnerability allows a remote, unauthenticated attacker to cause a degradation of service that can lead to a denial-of-service (DoS) on the BIG-IP system. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.		
CVE-2026-59859	microsoft - kiota	Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.32.4, Kiota's PHP generator embedded OpenAPI description, default fields, property names, and other schema-derived strings into PHP double-quoted literals through SanitizeDoubleQuote() in Writers/StringExtensions.cs without escaping $, allowing attacker-controlled ${...}, $var, or {$obj->prop} interpolation constructs to inject arbitrary PHP code into generated model and request-builder classes. This issue is fixed in version 1.32.4.	2026-07-16	8.7
CVE-2026-59860	microsoft - kiota	Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.32.3, Kiota is affected by a code-generation injection vulnerability in the C# XML documentation-comment sink (the description, externalDocs label, and externalDocs link fields emitted as /// ... comments). When text from an OpenAPI description is written into single-line XML doc comments without stripping newline and Unicode line-terminator characters, an attacker can break out of the /// comment line and inject additional code into generated C# clients. This issue is fixed in version 1.32.3.	2026-07-16	8.7
CVE-2026-53597	microsoft - prompty	Prompty is a markdown file format (.prompty) for LLM prompts. From 2.0.0-alpha.1 until 2.0.0-beta.3, the @prompty/core TypeScript loader in runtime/typescript/packages/core/src/core/loader.ts used gray-matter without overriding executable js and javascript frontmatter engines, allowing an attacker-controlled .prompty file with ---js frontmatter to execute arbitrary JavaScript during prompt loading. This issue is fixed in version 2.0.0-beta.3.	2026-07-16	8.7
CVE-2026-59835	fortinet - multiple products	A exposure of resource to wrong sphere vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.2, FortiSandbox 4.4.3 through 4.4.8 may allow an unauthenticated attacker to access the VNC server of VMs performing scanning via network requests.	2026-07-14	8.6
CVE-2026-47988	adobe - multiple products	Adobe Commerce is 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 read and write access. Exploitation of this issue does not require user interaction.	2026-07-14	8.6
CVE-2026-48252	adobe - multiple products	Adobe Experience Manager is affected by a Missing Authentication for Critical Function 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. Scope is changed.	2026-07-14	8.6
CVE-2026-48310	adobe - multiple products	Adobe Experience Manager is 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 does not require user interaction. Scope is changed.	2026-07-14	8.6
CVE-2026-48350	adobe - multiple products	Animate is affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to access sensitive files or directories outside the intended restrictions. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-07-14	8.6
CVE-2026-48275	adobe - multiple products	Illustrator is affected by an Untrusted Search Path 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. Scope is changed.	2026-07-14	8.6
CVE-2026-15583	grafana - Grafana MCP Server	A confused-deputy flaw in Grafana MCP Server allows an unauthenticated remote attacker to exfiltrate the server's environment-configured Grafana service-account token by supplying a crafted X-Grafana-URL request header. This also enables SSRF against arbitrary internal services, including cloud metadata endpoints.	2026-07-15	8.6
CVE-2026-57206	microsoft - simplechat	SimpleChat is a secure AI conversation application with personal and group workspaces for document-grounded interactions. Prior to 0.241.206, several plugin validation routes in application/single_app/plugin_validation_endpoint.py, including `POST /api/admin/plugins/test-instantiation`, `GET /api/admin/plugins/health-check/<plugin_name>`, `POST /api/admin/plugins/repair/<plugin_name>`, and `POST /api/plugins/validate`, relied on @swagger_route(security=get_auth_security()) documentation without enforcing @login_required, @user_required, or @admin_required at runtime, allowing unauthenticated or unauthorized clients to invoke plugin validation, health, and repair behavior. This issue is fixed in version 0.241.206.	2026-07-16	8.6
CVE-2025-40945	siemens - multiple products	A vulnerability has been identified in COMOS V10.4.5 (All versions < V10.4.5.0.2), COMOS V10.6 (All versions < V10.6.1), Designcenter NX (All versions < V2512.7000), Simcenter 3D (All versions < V2512.7000), Simcenter Femap V2506 (All versions < V2506.0003), Simcenter Femap V2512 (All versions < V2512.0002), Simcenter Nastran (All versions < V2606), Simcenter STAR-CCM+ (All versions < V2606), Solid Edge SE2025 (All versions < V225.0 Update 13), Solid Edge SE2026 (All versions < V226.0 Update 04), Teamcenter Visualization V2412 (All versions < V2412.0012), Teamcenter Visualization V2506 (All versions < V2506.0009), Teamcenter Visualization V2512 (All versions < V2512.2605), Tecnomatix Plant Simulation V2404 (All versions < V2404.0022), Tecnomatix Plant Simulation V2504 (All versions < V2504.0010), Tecnomatix Process Simulate (All versions < V2606). Untrusted search path in IAM Client SDK may allow an authenticated user to potentially enable escalation of privilege via local access.	2026-07-14	8.5
CVE-2026-53565	citrix - multiple products	Improper Privilege Management vulnerability in Citrix Secure Access Client for Windows, Citrix Citrix Endpoint Analysis Client for Windows.	2026-07-14	8.5

		This issue affects Secure Access Client for Windows: before 26.6.1.20; Citrix Endpoint Analysis Client for Windows: before 26. 5.1.7.		
CVE-2026-50340	microsoft - multiple products	Use after free in Windows Runtime allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.5
CVE-2026-48320	adobe - multiple products	ColdFusion is affected by a reflected Cross-Site Scripting (XSS) vulnerability. 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 open a malicious file. Scope is changed.	2026-07-14	8.5
CVE-2026-49184	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.	2026-07-14	8.4
CVE-2026-50520	microsoft - visual_studio_code	Improper neutralization of special elements used in a command ('command injection') in Visual Studio Code allows an unauthorized attacker to execute code locally.	2026-07-14	8.4
CVE-2026-54122	microsoft - multiple products	Heap-based buffer overflow in Windows GDI+ allows an unauthorized attacker to execute code locally.	2026-07-14	8.4
CVE-2026-54992	microsoft - multiple products	Heap-based buffer overflow in Windows Message Queuing Queue Manager allows an unauthorized attacker to execute code locally.	2026-07-14	8.4
CVE-2026-54128	microsoft - multiple products	Use after free in Windows DHCP Client allows an unauthorized attacker to execute code locally.	2026-07-14	8.4
CVE-2026-55045	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-07-14	8.4
CVE-2026-58596	microsoft - edge_chromium	Untrusted pointer dereference in Microsoft Edge (Chromium-based) allows an unauthorized attacker to elevate privileges over a network.	2026-07-12	8.3
CVE-2026-56181	microsoft - multiple products	Origin validation error in Windows Network Address Translation (NAT) allows an unauthorized attacker to perform spoofing over an adjacent network.	2026-07-14	8.3
CVE-2026-15769	google - chrome	Insufficient validation of untrusted input in Linux Toolkit Theming in Google Chrome on Linux prior to 150.0.7871.125 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)	2026-07-14	8.3
CVE-2026-15772	google - chrome	Use after free in GPU in Google Chrome on Android prior to 150.0.7871.125 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)	2026-07-14	8.3
CVE-2026-15774	google - chrome	Use after free in Skia in Google Chrome prior to 150.0.7871.125 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)	2026-07-14	8.3
CVE-2026-56434	f5 - multiple products	NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_ssi_module module. This vulnerability may exist when the Server-Side Includes (SSI), proxy_pass, and proxy_buffering off directives are configured. With this configuration, an unauthenticated attacker with man-in-the-middle (MITM) ability to control responses from an upstream server may be able to cause a use-after-free in the NGINX worker process. This issue may lead to limited modification of memory or a restart of the NGINX worker process. Impact: This vulnerability may allow remote attackers to have limited control to modify memory contents or restart the NGINX worker process. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-07-15	8.3
CVE-2026-48363	adobe - multiple products	ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Uncontrolled Search Path Element 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. Scope is changed.	2026-07-13	8.2
CVE-2026-48364	adobe - multiple products	ColdFusion versions 2025.9, 2023.20 and earlier are affected by an Uncontrolled Search Path Element 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. Scope is changed.	2026-07-13	8.2
CVE-2026-50338	microsoft - azure_spring_cloud	Improper authentication in Azure Spring Apps allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.2
CVE-2026-50429	microsoft - multiple products	Out-of-bounds read in Windows Kernel allows an unauthorized attacker to disclose information over a network.	2026-07-14	8.2
CVE-2026-50680	microsoft - multiple products	Heap-based buffer overflow in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	2026-07-14	8.2
CVE-2026-47984	adobe - multiple products	Adobe Commerce is 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 read and write access. Exploitation of this issue does not require user interaction.	2026-07-14	8.2
CVE-2026-48345	adobe - multiple products	Animate is affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could result in arbitrary code execution	2026-07-14	8.2

		in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.		
CVE-2026-50528	microsoft - multiple products	Incorrect authorization in .NET allows an unauthorized attacker to bypass a security feature over a network.	2026-07-14	8.2
CVE-2026-48290	adobe - multiple products	CAI Content Credentials is affected by a Server-Side Request Forgery (SSRF) 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.	2026-07-14	8.2
CVE-2026-12382	red hat - multiple products	A flaw was found in the AAP Gateway Envoy proxy configuration. The non-mTLS route to EDA event streams does not remove the Subject HTTP header from client requests, despite the source code defining requestHeadersToRemove for this header. An unauthenticated remote attacker can inject a spoofed Subject header matching a legitimate client certificate DN to bypass mTLS authentication and inject arbitrary events into protected EDA event streams.	2026-07-15	8.2
CVE-2026-58065	apache - apache-airflow-providers-git	The Apache Airflow Git provider runs its git-over-SSH operations with `StrictHostKeyChecking=no` by default, disabling SSH host-key verification. An attacker who can intercept the network path between an Airflow worker and the Git server can impersonate the server (man-in-the-middle), capturing the SSH deploy key or injecting malicious repository content. Deployments that use the Git DAG bundle or Git provider to clone over SSH with a deploy key are affected. The fix changes the default to verify host keys; upgrade to apache-airflow-providers-git `0.4.1` or later and configure a `known_hosts` file.	2026-07-13	8.1
CVE-2026-59245	apache - apache-airflow-providers-fab	In the Apache Airflow FAB auth manager, a DAG whose `dag_id` is `DAGs` collided with the global all-DAGs permission resource name produced by `resource_name()`, so a user granted per-DAG `access_control` on that one DAG was silently granted the global all-DAGs permission (privilege escalation). The escalation triggers when a DAG named `DAGs` exists and a lower-privileged user is given per-DAG access to it, granting that user read/edit access to every DAG. Users are advised to upgrade to `apache-airflow-providers-fab` 3.7.2 or later, which disambiguates the resource-name collision.	2026-07-13	8.1
CVE-2026-42900	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows App Store allows an unauthorized attacker to elevate privileges over a network.	2026-07-14	8.1
CVE-2026-49164	microsoft - multiple products	Heap-based buffer overflow in Active Directory Domain Services allows an unauthorized attacker to execute code over a network.	2026-07-14	8.1
CVE-2026-50694	microsoft - multiple products	Use after free in Windows Secure Socket Tunneling Protocol (SSTP) allows an unauthorized attacker to execute code over a network.	2026-07-14	8.1
CVE-2026-54995	microsoft - multiple products	Use after free in Reliable Multicast Transport Driver (RMCAST) allows an unauthorized attacker to execute code over a network.	2026-07-14	8.1
CVE-2026-56169	microsoft - windows_admin_center	Improper authentication in Windows Admin Center allows an authorized attacker to elevate privileges over a network.	2026-07-14	8.1
CVE-2026-58595	microsoft - bing_search	Improper restriction of rendered ui layers or frames in Microsoft Bing App for IOS allows an unauthorized attacker to perform spoofing over a network.	2026-07-14	8.1
CVE-2026-50439	microsoft - multiple products	Use after free in Microsoft Message Queuing Queue Manager allows an unauthorized attacker to execute code over a network.	2026-07-14	8.1
CVE-2026-50460	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an unauthorized attacker to elevate privileges over a network.	2026-07-14	8.1
CVE-2026-50487	microsoft - multiple products	Use after free in Microsoft Windows DNS allows an unauthorized attacker to elevate privileges over a network.	2026-07-14	8.1
CVE-2026-50686	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows OLE allows an unauthorized attacker to execute code over a network.	2026-07-14	8.1
CVE-2026-56186	microsoft - multiple products	Out-of-bounds read in Windows Schannel allows an authorized attacker to disclose information over a network.	2026-07-14	8.1
CVE-2026-58617	microsoft - 365_copilot	Improper access control in Microsoft 365 Copilot for iOS allows an unauthorized attacker to elevate privileges over a network.	2026-07-14	8.1
CVE-2026-47304	microsoft - .net_framework	Improper verification of cryptographic signature in .NET allows an unauthorized attacker to bypass a security feature over a network.	2026-07-14	8.1
CVE-2026-47995	adobe - multiple products	Adobe Commerce is 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, potentially gaining elevated access or control over the victim's account or session. Scope is changed.	2026-07-14	8.1
CVE-2026-48349	adobe - multiple products	Animate is affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	8.1
CVE-2026-56287	apache - fineract	A boolean-based SQL Injection vulnerability exists in Apache Fineract's Client Search API (GET /api/v1/clients) in versions up to and including 1.14.0. The orderBy and sortOrder request parameters are concatenated into a SQL query without sufficient validation, allowing an authenticated user with permission to view clients to inject arbitrary SQL via a crafted orderBy value. This can be leveraged to perform blind boolean-based data extraction and, on	2026-07-15	8.1

		MySQL/MariaDB, to disclose arbitrary files readable by the database process via the LOAD_FILE() function. Users are recommended to upgrade to a version containing the fix		
CVE-2026-57821	apache - fineract	A SQL Injection vulnerability exists in Apache Fineract's Office Search API (GET /api/v1/offices) in versions up to and including 1.14.0. The orderBy request parameter is concatenated into a SQL query without sufficient validation, allowing an authenticated user with permission to view offices to inject arbitrary SQL via a crafted orderBy value. This is a bypass of the ColumnValidator fix introduced for CVE-2024-32838, which does not detect bare subqueries in the ORDER BY position. This can be leveraged to perform time-based blind SQL injection for data exfiltration. Because the injected query blocks the database connection for its full duration, concurrent exploitation can exhaust the application's database connection pool, resulting in denial of service for other users. Users are recommended to upgrade to a version containing the fix.	2026-07-15	8.1
CVE-2026-20156	cisco - Cisco RoomOS Software	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco RoomOS engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities._x000D_ _x000D_ The vulnerabilities tracked by CVE-2026-20156 are related to improper restriction of operations within the bounds of a memory buffer that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-119.	2026-07-15	8.1
CVE-2026-40400	microsoft - multiple products	Relative path traversal in Windows PowerShell allows an authorized attacker to execute code over a network.	2026-07-14	8
CVE-2026-42975	microsoft - multiple products	Heap-based buffer overflow in Windows Bluetooth Port Driver allows an unauthorized attacker to execute code over an adjacent network.	2026-07-14	8
CVE-2026-49169	microsoft - windows_server_2025	Use after free in DNS Server allows an authorized attacker to execute code over a network.	2026-07-14	8
CVE-2026-58647	microsoft - power_bi_report_server	Improper neutralization of input during web page generation ('cross-site scripting') in Power BI allows an authorized attacker to perform spoofing over a network.	2026-07-14	8
CVE-2026-50365	microsoft - multiple products	Improper authentication in Windows RPC API allows an unauthorized attacker to elevate privileges over an adjacent network.	2026-07-14	8
CVE-2026-50502	microsoft - multiple products	Insufficient granularity of access control in Windows Event Logging Service allows an authorized attacker to execute code over a network.	2026-07-14	8
CVE-2026-50683	microsoft - multiple products	Heap-based buffer overflow in Windows DHCP Server allows an authorized attacker to elevate privileges over an adjacent network.	2026-07-14	8
CVE-2026-48346	adobe - multiple products	Animate is affected by an Untrusted Search Path 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. Scope is changed.	2026-07-14	7.9
CVE-2026-42982	microsoft - multiple products	Improper validation of consistency within input in Windows Secure Kernel Mode allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-44800	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-47296	microsoft - multiple products	Improper neutralization of special elements used in an sql command ('sql injection') in SQL Server allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-48581	microsoft - surface_go_2_1901_firmware	Insufficient granularity of access control in Microsoft Surface allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-49166	microsoft - multiple products	Use after free in Microsoft Printer Drivers allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-49170	microsoft - multiple products	Insufficient granularity of access control in Windows StateRepository API allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-49173	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-49175	microsoft - multiple products	Heap-based buffer overflow in Windows DNS allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-49176	microsoft - multiple products	Improper privilege management in Windows WalletService allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-49783	microsoft - multiple products	Improperly implemented security check for standard in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-07-14	7.8
CVE-2026-49792	microsoft - multiple products	Numeric truncation error in Windows Resilient File System (ReFS) allows an authorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-49793	microsoft - multiple products	Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an authorized attacker to execute code locally.	2026-07-14	7.8

CVE-2026-49796	microsoft - multiple products	Heap-based buffer overflow in Windows GDI+ allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-49797	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-49800	microsoft - multiple products	Integer overflow or wraparound in Windows Web Proxy Auto-Discovery Protocol (WPAD) allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-49808	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50293	microsoft - multiple products	Use after free in Windows Internal Task Bar allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50308	microsoft - multiple products	Integer underflow (wrap or wraparound) in Windows NTFS allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50311	microsoft - multiple products	Improper access control in Windows Server allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50318	microsoft - multiple products	Stack-based buffer overflow in Windows Resilient File System (ReFS) allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50333	microsoft - multiple products	Missing authentication for critical function in Windows Spaceport.sys allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50351	microsoft - multiple products	Improper access control in Windows Audio Compression Manager (ACM) allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50675	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50697	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-54109	microsoft - multiple products	Integer overflow or wraparound in Windows Resilient File System (ReFS) allows an authorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-54112	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-54114	microsoft - multiple products	Use after free in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-54986	microsoft - multiple products	Heap-based buffer overflow in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-54987	microsoft - multiple products	Heap-based buffer overflow in Windows Overlay Filter allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-54991	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-54993	microsoft - multiple products	Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55001	microsoft - multiple products	Improper certificate validation in Windows Active Directory allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-55002	microsoft - multiple products	External control of file name or path in SQL Server allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-55004	microsoft - multiple products	Double free in Microsoft Printer Drivers allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-55006	microsoft - multiple products	Insufficient granularity of access control in Microsoft Exchange Server allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-55009	microsoft - multiple products	Deserialization of untrusted data in Microsoft Exchange Server allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-55011	microsoft - malware_protection_engine	Integer underflow (wrap or wraparound) in Microsoft Defender allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55012	microsoft - malware_protection_engine	Integer overflow or wraparound in Microsoft Defender allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55014	microsoft - remote_help	Improper access control in Windows Remote Help Defense allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8

CVE-2026-55899	microsoft - multiple products	Stack-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55948	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-56155	microsoft - multiple products	Insufficient granularity of access control in Active Directory Federation Services (AD FS) allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-57107	microsoft - windows_admin_center	Improper authentication in Windows Admin Center allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58601	microsoft - multiple products	Heap-based buffer overflow in Virtual Hard Disk (VHD) Miniport Driver allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58602	microsoft - multiple products	Use after free in Windows Kernel Mode Driver allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58609	microsoft - multiple products	Out-of-bounds read in Microsoft Graphics Component allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-58610	microsoft - multiple products	Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-58618	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-58631	microsoft - windows_admin_center	Improper authorization in Windows Admin Center allows an authorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-58635	microsoft - multiple products	Improper neutralization of special elements used in a command ('command injection') in Windows Narrator Braille allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58636	microsoft - pc_manager	Improper link resolution before file access ('link following') in Window PC Manager allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-47290	microsoft - multiple products	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-47642	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-47967	adobe - multiple products	Audition is 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.	2026-07-14	7.8
CVE-2026-47968	adobe - multiple products	Audition is 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.	2026-07-14	7.8
CVE-2026-48309	adobe - multiple products	Audition is 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.	2026-07-14	7.8
CVE-2026-48365	adobe - multiple products	Audition is 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.	2026-07-14	7.8
CVE-2026-48368	adobe - multiple products	Audition is 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.	2026-07-14	7.8
CVE-2026-50301	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50305	microsoft - multiple products	Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50306	microsoft - multiple products	Use after free in Windows TCP/IP allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50309	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50313	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50314	microsoft - multiple products	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50315	microsoft - multiple products	Null pointer dereference in Windows Image Acquisition allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50317	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Operating Systems allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8

CVE-2026-50321	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Driver allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50326	microsoft - multiple products	Use after free in Windows Unified Consent System allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50327	microsoft - multiple products	Heap-based buffer overflow in Windows Media allows an authorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50329	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50331	microsoft - multiple products	Use after free in Windows Application Model allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50332	microsoft - multiple products	Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50335	microsoft - multiple products	Improper access control in Windows Operating Systems allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50336	microsoft - multiple products	Heap-based buffer overflow in Windows Media allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50337	microsoft - multiple products	Incorrect type conversion or cast in Windows Notification allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50343	microsoft - multiple products	Improper privilege management in Microsoft Install Service allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50344	microsoft - multiple products	Improper authorization in Windows OLE allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50346	microsoft - multiple products	Improper authorization in RPC Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50347	microsoft - multiple products	Heap-based buffer overflow in Windows Data dll allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50353	microsoft - multiple products	Use after free in Windows DirectX allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50357	microsoft - multiple products	Numeric truncation error in Windows Resilient File System (ReFS) allows an authorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50361	microsoft - multiple products	Double free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50362	microsoft - multiple products	Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50363	microsoft - multiple products	Heap-based buffer overflow in Windows Push Notifications allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50367	microsoft - multiple products	Incorrect access of indexable resource ('range error') in Windows Sensor Data Service allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50373	microsoft - multiple products	Improper access control in Microsoft Windows Search Component allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50378	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Key Guard allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50386	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50387	microsoft - multiple products	Stack-based buffer overflow in Windows GDI allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50388	microsoft - multiple products	Out-of-bounds read in Windows NTFS allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50391	microsoft - multiple products	Improper privilege management in Windows Group Policy allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50399	microsoft - multiple products	Out-of-bounds read in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8

CVE-2026-50400	microsoft - multiple products	Stack-based buffer overflow in Windows App Installer allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50402	microsoft - multiple products	Incorrect conversion between numeric types in Windows NTFS allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50405	microsoft - multiple products	Insufficient granularity of access control in Windows Filtering Platform (WFP) allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50407	microsoft - multiple products	Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50412	microsoft - multiple products	Stack-based buffer overflow in Windows NTFS allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50417	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50421	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Connected User Experiences and Telemetry allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50422	microsoft - multiple products	Out-of-bounds read in Windows NTFS allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50423	microsoft - multiple products	Improper access control in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50425	microsoft - multiple products	Use after free in Windows Internal System User Profile allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50427	microsoft - multiple products	Use after free in Content Delivery Manager allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50433	microsoft - multiple products	Use after free in Windows Media allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50435	microsoft - multiple products	Buffer over-read in Windows Overlay Filter allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50436	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50440	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Audio Service allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50441	microsoft - multiple products	Untrusted pointer dereference in Windows Resilient File System (ReFS) allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50448	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50450	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Wireless Wide Area Network Service allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50454	microsoft - multiple products	Relative path traversal in Windows User Interface Core allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50457	microsoft - multiple products	Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50458	microsoft - multiple products	Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50461	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50462	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.	2026-07-14	7.8
CVE-2026-50466	microsoft - multiple products	Use after free in Windows Brokering File System allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50467	microsoft - multiple products	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50469	microsoft - multiple products	Improper link resolution before file access ('link following') in Windows Projected File System allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8

CVE-2026-50471	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50476	microsoft - multiple products	Use after free in Microsoft Windows allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50478	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50479	microsoft - multiple products	Untrusted pointer dereference in Windows USB Hub Driver allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50480	microsoft - multiple products	Heap-based buffer overflow in Windows Web Proxy Auto-Discovery Protocol (WPAD) allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50484	microsoft - multiple products	Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50486	microsoft - multiple products	Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50488	microsoft - multiple products	Improper neutralization of special elements used in a command ('command injection') in Windows Clipboard User Service allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50493	microsoft - multiple products	Use after free in Windows Graphics Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50494	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50498	microsoft - multiple products	Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability	2026-07-14	7.8
CVE-2026-50499	microsoft - multiple products	Heap-based buffer overflow in Windows Print Spooler Components allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50501	microsoft - multiple products	Stack-based buffer overflow in Windows Resilient File System (ReFS) allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50509	microsoft - multiple products	Deserialization of untrusted data in Windows Wireless Wide Area Network Service allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50510	microsoft - github_copilot	Improper restriction of names for files and other resources in Github Copilot allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50655	microsoft - multiple products	Heap-based buffer overflow in Windows Media allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50665	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	7.8
CVE-2026-50667	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows NTFS allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50673	microsoft - multiple products	Null pointer dereference in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50676	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50677	microsoft - multiple products	Use after free in Windows Media allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50679	microsoft - multiple products	Heap-based buffer overflow in Microsoft Windows Search Component allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50688	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-50689	microsoft - multiple products	Use after free in Windows Clipboard Server allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-54115	microsoft - multiple products	Integer overflow or wraparound in Windows Active Directory allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-54124	microsoft - multiple products	Integer overflow or wraparound in Windows Terminal allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-54125	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8

CVE-2026-54131	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55017	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55018	microsoft - multiple products	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55022	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55024	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55025	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55029	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55031	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55032	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55033	microsoft - multiple products	Integer overflow or wraparound in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55036	microsoft - multiple products	Buffer over-read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55037	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55038	microsoft - multiple products	Stack-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55039	microsoft - multiple products	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55041	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55043	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55044	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55048	microsoft - multiple products	Integer overflow or wraparound in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55049	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55053	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55055	microsoft - multiple products	Stack-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55056	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55058	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55120	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55123	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55125	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-07-14	7.8

CVE-2026-55127	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55128	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55129	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55130	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55131	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55132	microsoft - multiple products	Double free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55133	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office OneNote allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55134	microsoft - multiple products	Stack-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55136	microsoft - multiple products	Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55137	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55140	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55141	microsoft - multiple products	Stack-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55947	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-55949	microsoft - multiple products	Use of uninitialized resource in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-56156	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-56175	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-56176	microsoft - multiple products	Out-of-bounds read in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-56182	microsoft - multiple products	Integer overflow or wraparound in Windows NTFS allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-56189	microsoft - multiple products	Heap-based buffer overflow in Microsoft Windows Media Foundation allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-56643	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-56644	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-56650	microsoft - multiple products	Heap-based buffer overflow in Windows Network File System allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-57088	microsoft - multiple products	Improper access control in Extensible Storage Engine (ESENT) allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-57091	microsoft - multiple products	Stack-based buffer overflow in Windows File History Service allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-57096	microsoft - multiple products	Heap-based buffer overflow in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-57968	microsoft - windows_subsystem_for_linux	Buffer over-read in Windows Subsystem for Linux allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8

CVE-2026-58527	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58530	microsoft - multiple products	Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-58532	microsoft - multiple products	Integer overflow or wraparound in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58536	microsoft - multiple products	Use after free in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58537	microsoft - multiple products	Use after free in Microsoft NAT Helper Components (ipnathlp.dll) allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58538	microsoft - multiple products	Heap-based buffer overflow in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58540	microsoft - multiple products	Improper authorization in Windows Installer allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58541	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows DWM allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58542	microsoft - multiple products	Heap-based buffer overflow in Windows Media allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-58613	microsoft - multiple products	Use after free in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58628	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Wireless Networking allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58632	microsoft - multiple products	Use after free in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58633	microsoft - multiple products	Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-58634	microsoft - multiple products	Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-47305	microsoft - multiple products	Protection mechanism failure in Visual Studio allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50646	microsoft - .net_framework	Protection mechanism failure in .NET Framework allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50649	microsoft - .net_framework	Deserialization of untrusted data in .NET allows an unauthorized attacker to execute code locally.	2026-07-14	7.8
CVE-2026-50650	microsoft - .net_framework	Improper control of generation of code ('code injection') in .NET Framework allows an unauthorized attacker to elevate privileges locally.	2026-07-14	7.8
CVE-2026-47971	adobe - multiple products	Media Encoder is 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.	2026-07-14	7.8
CVE-2026-47976	adobe - multiple products	Media Encoder is 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.	2026-07-14	7.8
CVE-2026-48269	adobe - multiple products	Premiere Pro is 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.	2026-07-14	7.8
CVE-2026-48270	adobe - multiple products	Premiere Pro is 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.	2026-07-14	7.8
CVE-2026-48272	adobe - creative_cloud_desktop_application	Creative Cloud Desktop is affected by an Uncontrolled Search Path Element vulnerability that could result in arbitrary code execution in the context of the current user. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	7.8
CVE-2026-48274	adobe - multiple products	After Effects is 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.	2026-07-14	7.8
CVE-2026-48311	adobe - multiple products	Bridge is 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.	2026-07-14	7.8
CVE-2026-48339	adobe - multiple products	Bridge is 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.	2026-07-14	7.8
CVE-2026-48340	adobe - multiple products	Bridge is affected by an Untrusted Pointer Dereference 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.	2026-07-14	7.8

CVE-2026-48341	adobe - multiple products	Bridge is 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.	2026-07-14	7.8
CVE-2026-48342	adobe - multiple products	Bridge is 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.	2026-07-14	7.8
CVE-2026-48343	adobe - multiple products	Bridge is 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.	2026-07-14	7.8
CVE-2026-48344	adobe - creative_cloud_desktop_application	Creative Cloud Desktop is affected by a Time-of-check Time-of-use (TOCTOU) Race Condition vulnerability that could result in arbitrary code execution in the context of the current user. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	7.8
CVE-2026-48366	adobe - multiple products	Media Encoder is 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.	2026-07-14	7.8
CVE-2026-48367	adobe - multiple products	After Effects is 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.	2026-07-14	7.8
CVE-2026-48369	adobe - multiple products	Premiere Pro is 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.	2026-07-14	7.8
CVE-2026-48370	adobe - multiple products	Media Encoder is 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.	2026-07-14	7.8
CVE-2026-48335	adobe - multiple products	Illustrator is 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.	2026-07-14	7.8
CVE-2026-48336	adobe - multiple products	Illustrator is 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.	2026-07-14	7.8
CVE-2026-48337	adobe - multiple products	Illustrator is 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.	2026-07-14	7.8
CVE-2026-40633	dell - multiple products	Dell PowerScale OneFS versions 9.5.0.0 through 9.10.1.7, versions 9.11.0.0 through 9.13.0.2 contains an Insertion of Sensitive Information into Log File vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information disclosure.	2026-07-15	7.8
CVE-2026-15809	red hat - multiple products	A flaw was found in CRI-O. The fix for a previous vulnerability (CVE-2022-4318) was incorrect, allowing it to be bypassed. An attacker capable of setting environment variables on a container can inject a newline character into the HOME environment variable. This issue allows the addition of arbitrary lines into /etc/passwd by use of a specially crafted environment variable.	2026-07-15	7.8
CVE-2026-58558	huawei - multiple products	Permission control vulnerability in the file system. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-07-15	7.8
CVE-2026-56687	dell - ThinOS 10	Dell ThinOS 10, versions prior to 2605_10.2100, contain an Obsolete Feature in UI vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Unauthorized access.	2026-07-15	7.8

CVE-2026-53366	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved:
		
		ipv4: account for fraggap on the paged allocation path
		
		In __ip_append_data(), when the paged-allocation branch is taken,
		alloclen and pagedlen are computed as
		
		alloclen = fragheaderlen + transhdrlen;
		pagedlen = datalen - transhdrlen;
		
		datalen already includes fraggap, but the fraggap bytes carried over
		from the previous skb are copied into the new skb's linear area at
		offset transhdrlen by the subsequent skb_copy_and_csum_bits(). The
		linear area is therefore undersized by fraggap bytes while pagedlen is
		overstated by the same amount.
		
		The non-paged branch sets alloclen to fraglen, which already accounts
		for fraggap because datalen does. Bring the paged branch in line by
		adding fraggap to alloclen and subtracting it from pagedlen.
		
		After this adjustment, copy no longer collapses to -fraggap on the
		paged path, so remove the stale comment describing that old arithmetic.
			2026-07-16	7.8

CVE-2026-14903	ivanti - Xtraction	Path traversal in Ivanti Xtraction before version 2026.2.1 allows a remote authenticated attacker to read arbitrary files outside the web root.	2026-07-14	7.7
CVE-2026-48347	adobe - multiple products	Animate is affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') 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. Scope is changed.	2026-07-14	7.7
CVE-2026-48348	adobe - multiple products	Animate is affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-07-14	7.7

CVE-2026-48328	adobe - multiple products	ColdFusion is affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	7.7
CVE-2026-48332	adobe - multiple products	ColdFusion is affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	7.7
CVE-2026-14251	red hat - multiple products	A flaw was found in the OpenShift GitOps operator. The ClusterRole reconciler does not validate resource ownership when reconciling ClusterRole objects. A namespace-scoped Argo CD instance can trigger deletion of a ClusterRole owned by a cluster-scoped Argo CD instance by crafting a name collision, resulting in a denial of service.	2026-07-15	7.7
CVE-2026-47996	adobe - multiple products	Adobe Commerce is affected by an Incorrect Authorization vulnerability that could result in a Security feature bypass. A high-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read access. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	7.6
CVE-2026-15574	red hat - Red Hat OpenShift AI (RHOAI)	A flaw was found in the vllm-orchestrator-gateway component. The system's production binary logs all incoming authorization headers and full chat payloads, which may contain personally identifiable information (PII) and secrets, to persistent logs. This sensitive data, including bearer tokens and chat content, can be accessed by any user with logging privileges. This vulnerability leads to information disclosure, potentially allowing an attacker to harvest credentials and sensitive conversation content.	2026-07-13	7.5
CVE-2026-15584	red hat - Pen Drive Powered by Red Hat Lightspeed	A privilege escalation vulnerability was found in the incluster-checks tool for OpenShift. The tool creates privileged debug pods with host filesystem access in the shared default namespace, where any user with the standard edit role can exec into them and obtain root access on cluster nodes.	2026-07-13	7.5
CVE-2025-53379	fortinet - multiple products	A out-of-bounds read vulnerability in Fortinet FortiAuthenticator 6.6.0 through 6.6.2, FortiAuthenticator 6.5 all versions may allow a remote unauthenticated attacker to retrieve sensitive information via a specially crafted request.	2026-07-14	7.5
CVE-2026-59836	fortinet - multiple products	A improper certificate validation vulnerability in Fortinet FortiClientEMS 7.4.3 through 7.4.5, FortiClientEMS 7.4.0 through 7.4.1, FortiClientEMS 7.2 all versions may allow attacker to information disclosure via <insert attack vector here>	2026-07-14	7.5
CVE-2026-59841	fortinet - fortisiem	A improper restriction of communication channel to intended endpoints vulnerability in Fortinet FortiSIEMWindowsAgent 7.4.0 through 7.4.1 may allow attacker to escalation of privilege via <insert attack vector here>	2026-07-14	7.5
CVE-2026-40378	microsoft - multiple products	Memory allocation with excessive size value in Windows Local Security Authority Subsystem Service (LSASS) allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-45646	microsoft - multiple products	Allocation of resources without limits or throttling in ASP.NET Core allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-49171	microsoft - multiple products	Use after free in Microsoft Windows Speech allows an authorized attacker to elevate privileges locally.	2026-07-14	7.5
CVE-2026-49181	microsoft - multiple products	Integer underflow (wrap or wraparound) in Windows DHCP Client allows an unauthorized attacker to elevate privileges over a network.	2026-07-14	7.5
CVE-2026-49787	microsoft - multiple products	Allocation of resources without limits or throttling in Windows HTTP.sys allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-49788	microsoft - multiple products	Allocation of resources without limits or throttling in HTTP/2 allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50506	microsoft - multiple products	Allocation of resources without limits or throttling in ASP.NET Core allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50652	microsoft - .net_framework	Deserialization of untrusted data in Azure Active Directory allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50653	microsoft - .net_framework	Loop with unreachable exit condition ('infinite loop') in Azure Active Directory allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50695	microsoft - multiple products	Stack-based buffer overflow in Active Directory Federation Services allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50696	microsoft - multiple products	Heap-based buffer overflow in Windows Internet Key Exchange (IKE) Protocol allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-54119	microsoft - multiple products	Loop with unreachable exit condition ('infinite loop') in Windows Active Directory allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-54983	microsoft - multiple products	Stack-based buffer overflow in Active Directory Federation Services (AD FS) allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-56170	microsoft - multiple products	Allocation of resources without limits or throttling in ASP.NET Core allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50304	microsoft - multiple products	Stack-based buffer overflow in Active Directory Federation Services allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5

CVE-2026-50328	microsoft - multiple products	Uncaught exception in Windows Server Update Service allows an unauthorized attacker to perform tampering over a network.	2026-07-14	7.5
CVE-2026-50330	microsoft - multiple products	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to elevate privileges over a network.	2026-07-14	7.5
CVE-2026-50355	microsoft - multiple products	Stack-based buffer overflow in Active Directory Federation Services allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50368	microsoft - multiple products	Stack-based buffer overflow in Active Directory Federation Services allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50379	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges over a network.	2026-07-14	7.5
CVE-2026-50411	microsoft - multiple products	Stack-based buffer overflow in Active Directory Federation Services (AD FS) allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50414	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges over a network.	2026-07-14	7.5
CVE-2026-50424	microsoft - multiple products	Untrusted pointer dereference in Windows Domain Controller allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50463	microsoft - multiple products	Out-of-bounds read in Windows Kernel allows an unauthorized attacker to disclose information over a network.	2026-07-14	7.5
CVE-2026-50470	microsoft - multiple products	Out-of-bounds read in Windows Network Policy Server SNMP allows an unauthorized attacker to disclose information over a network.	2026-07-14	7.5
CVE-2026-50496	microsoft - multiple products	Out-of-bounds read in Windows Network Policy Server SNMP allows an unauthorized attacker to disclose information over a network.	2026-07-14	7.5
CVE-2026-50500	microsoft - multiple products	Use after free in Windows Netlogon allows an authorized attacker to elevate privileges over a network.	2026-07-14	7.5
CVE-2026-50505	microsoft - multiple products	Use after free in Windows Message Queuing allows an authorized attacker to execute code over a network.	2026-07-14	7.5
CVE-2026-50647	microsoft - multiple products	Loop with unreachable exit condition ('infinite loop') in Active Directory Federation Services (AD FS) allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50685	microsoft - multiple products	Double free in Windows DHCP Server allows an authorized attacker to execute code over a network.	2026-07-14	7.5
CVE-2026-56648	microsoft - multiple products	Time-of-check time-of-use (toctou) race condition in Windows Network File System allows an authorized attacker to elevate privileges over a network.	2026-07-14	7.5
CVE-2026-57089	microsoft - multiple products	Use after free in Windows SMB Server Network Transport Driver (srvnet.sys) allows an unauthorized attacker to execute code over a network.	2026-07-14	7.5
CVE-2026-57108	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in .NET Core allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-58531	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SMB allows an authorized attacker to elevate privileges over a network.	2026-07-14	7.5
CVE-2026-58627	microsoft - multiple products	Uncontrolled resource consumption in Windows DHCP Server allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-47302	microsoft - .net_framework	Allocation of resources without limits or throttling in .NET allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-15709	red hat - multiple products	A flaw was found in libsoup's WebSocket implementation when using the permessage-deflate extension. The extension's decompression loop (inflate()) processes data in chunks without enforcing an upper boundary limit on the output buffer size. While libsoup limits the incoming compressed frame size via max_incoming_payload_size, it fails to track or limit memory allocation during decompression. A separate check for decompressed size (max_total_message_size) exists but executes only after inflation is complete, and it is entirely disabled by default for client connections. A remote, unauthenticated attacker can exploit this by sending a small, highly compressed payload (a decompression bomb), causing unbounded memory allocation that triggers an Out-of-Memory (OOM) crash and a Denial of Service (DoS).	2026-07-14	7.5
CVE-2026-15711	red hat - multiple products	A vulnerability was found in libsoup's WebSocket frame parsing implementation. The library fails to validate length rules specified in RFC 6455 §5.5, which mandates that all WebSocket control frames (e.g., PING, PONG, CLOSE) contain a payload of 125 bytes or less. A remote, unauthenticated attacker can exploit this by sending a non-compliant, oversized control frame. Because the parser handles this protocol violation improperly instead of throwing an immediate connection termination error, it triggers a internal processing crash, resulting in a remote denial of service (DoS) for applications utilizing libsoup WebSockets.	2026-07-14	7.5

CVE-2026-50524	microsoft - multiple products	Improper validation of specified type of input in .NET Framework allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50525	microsoft - .net_framework	Allocation of resources without limits or throttling in .NET allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50527	microsoft - .net_framework	Stack-based buffer overflow in .NET Framework allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50648	microsoft - .net_framework	Allocation of resources without limits or throttling in .NET Framework allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-50651	microsoft - multiple products	Allocation of resources without limits or throttling in .NET allows an unauthorized attacker to deny service over a network.	2026-07-14	7.5
CVE-2026-15764	google - chrome	Use after free in Ozone in Google Chrome on Linux prior to 150.0.7871.125 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2026-07-14	7.5
CVE-2026-15765	google - chrome	Use after free in Ozone in Google Chrome prior to 150.0.7871.125 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2026-07-14	7.5
CVE-2026-15777	google - chrome	Use after free in UI in Google Chrome on Linux prior to 150.0.7871.125 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-07-14	7.5
CVE-2026-48295	adobe - multiple products	CAI Content Credentials is affected by an Insufficiently Protected Credentials vulnerability that could result in disclosure of sensitive information. An attacker could leverage this vulnerability to gain unauthorized read access. Exploitation of this issue does not require user interaction.	2026-07-14	7.5
CVE-2026-48351	adobe - multiple products	CAI Content Credentials is 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.	2026-07-14	7.5
CVE-2026-48352	adobe - multiple products	CAI Content Credentials is 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.	2026-07-14	7.5
CVE-2026-20153	cisco - Cisco RoomOS Software	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco RoomOS engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities._x000D_ _x000D_ The vulnerabilities tracked by CVE-2026-20153 are related to improper input validation that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-20.	2026-07-15	7.5
CVE-2026-20157	cisco - Cisco RoomOS Software	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco RoomOS engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities._x000D_ _x000D_ The vulnerabilities tracked by CVE-2026-20157 are related to missing encryption that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-311.	2026-07-15	7.5
CVE-2026-20158	cisco - Cisco RoomOS Software	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco RoomOS engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities._x000D_ _x000D_ The vulnerabilities tracked by CVE-2026-20158 are related to improper control of a resource through its lifetime that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-664.	2026-07-15	7.5
CVE-2026-20187	cisco - Cisco RoomOS Software	As part of Cisco's ongoing commitment to proactive security and product quality, the Cisco RoomOS engineering team has conducted a comprehensive internal security review. This review resulted in a software hardening release that addresses multiple internally discovered vulnerabilities._x000D_ _x000D_ The vulnerabilities tracked by CVE-2026-20187 are related to improper handling of exceptional conditions that are grouped under the Common Weakness Enumeration (CWE) Pillar CWE-703.	2026-07-15	7.5
CVE-2026-21729	grafana - Loki	Loki queries with large limits can cause large memory allocations which can impact the availability of the service, depending on its deployment strategy.	2026-07-16	7.5
CVE-2026-59861	microsoft - kiota	Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.32.0, Kiota's Ruby generator embedded OpenAPI default fields, property names, and other schema-derived strings through CodeMethodWriter.cs and SanitizeForQuotedLiteral() in Writers/StringExtensions.cs into Ruby double-quoted literals without escaping #, allowing attacker-controlled #{expr}, #$var, or #@var interpolation markers to inject arbitrary Ruby code into generated model classes. This issue is fixed in version 1.32.0.	2026-07-16	7.5
CVE-2026-59862	microsoft - kiota	Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.32.0, Kiota's Python generator let attacker-controlled enum value descriptions from x-ms-enum.values[].description flow through KiotaBuilder.SetEnumOptions into Documentation.DescriptionTemplate and PythonConventionService.RemoveInvalidDescriptionCharacters without newline sanitization, allowing generated inline comments to split and execute attacker-controlled Python code at module scope when generated modules were imported. This issue is fixed in version 1.32.0.	2026-07-16	7.5
CVE-2026-53598	microsoft - prompty	Prompty is a markdown file format (.prompty) for LLM prompts. Prior to 2.0.0-beta.2, Prompty loaders expanded ${file:...} references in .prompty frontmatter without enforcing that resolved paths stayed within the prompt directory or allowed roots, allowing an attacker-controlled	2026-07-16	7.5

		prompt file to read local files through absolute paths, .. traversal, or symlink escapes. This issue is fixed in versions 2.0.0-beta.2.		
CVE-2026-59117	microsoft - terminal	Integer overflow or wraparound in Windows Terminal allows an unauthorized attacker to execute code over a network.	2026-07-16	7.5
CVE-2026-15480	trendnet - TEW-635BRM	A vulnerability was identified in Trendnet TEW-635BRM up to 1.00.03. This affects the function start_httpd of the file /sbin/rc of the component Web Service. Such manipulation of the argument device_name leads to stack-based buffer overflow. The attack can be executed remotely. The exploit is publicly available and might be used. The vendor explains: "We are unable to confirm if the vulnerability exists. This item has been EOL since 2011. We will make an official announcement of possible vulnerabilities, and recommend users to switch devices." This vulnerability only affects products that are no longer supported by the maintainer.	2026-07-12	7.4
CVE-2026-15481	trendnet - TEW-635BRM	A security flaw has been discovered in Trendnet TEW-635BRM up to 1.00.03. This vulnerability affects the function ipoa_test of the file /sbin/rc of the component IPoA WAN Connection Setup. Performing a manipulation of the argument ipoa_ipaddr results in command injection. The attack is possible to be carried out remotely. The exploit has been released to the public and may be used for attacks. The vendor explains: "We are unable to confirm if the vulnerability exists. This item has been EOL since 2011. We will make an official announcement of possible vulnerabilities, and recommend users to switch devices." This vulnerability only affects products that are no longer supported by the maintainer.	2026-07-12	7.4
CVE-2026-54127	microsoft - multiple products	Use after free in Windows Hyper-V allows an unauthorized attacker to elevate privileges locally.	2026-07-14	7.4
CVE-2026-48287	adobe - multiple products	CAI Content Credentials is affected by an Untrusted Search Path vulnerability that could result in arbitrary code execution in the context of the current user. Exploit depends on conditions beyond the attacker's control. 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.	2026-07-14	7.4
CVE-2026-49789	microsoft - multiple products	Stack-based buffer overflow in Windows NTFS allows an authorized attacker to elevate privileges locally.	2026-07-14	7.3
CVE-2026-49790	microsoft - multiple products	Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability	2026-07-14	7.3
CVE-2026-50364	microsoft - multiple products	Improper link resolution before file access ('link following') in Windows Server Backup allows an authorized attacker to elevate privileges locally.	2026-07-14	7.3
CVE-2026-58640	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.	2026-07-14	7.3
CVE-2026-50482	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an authorized attacker to execute code locally.	2026-07-14	7.3
CVE-2026-55021	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-07-14	7.3
CVE-2026-55034	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-07-14	7.3
CVE-2026-55126	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-07-14	7.3
CVE-2026-9046	lenovo - multiple products	A potential insecure permissions vulnerability was reported in Legion Zone and the Lenovo App Store Windows applications, distributed exclusively in the Chinese market, that when installed on a non-system partition, could allow a local user to execute arbitrary code.	2026-07-16	7.3
CVE-2026-15410	sonicwall - multiple products	Post-authentication improper control of generation of code ('Code Injection') vulnerability has been identified in the SMA1000 Appliance Management Console (AMC) which in specific conditions could potentially enable a remote authenticated attacker as administrator to execute arbitrary OS commands.	2026-07-14	7.2
CVE-2026-47992	adobe - multiple products	Adobe Commerce is affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could result in arbitrary code execution in the context of the current user. A high-privileged attacker could exploit this vulnerability to execute malicious SQL commands, potentially gaining elevated access or control over the victim's account or session. Exploitation of this issue does not require user interaction.	2026-07-14	7.2
CVE-2026-49165	microsoft - multiple products	Use of uninitialized resource in Microsoft Windows App Store allows an authorized attacker to disclose information locally.	2026-07-14	7.1
CVE-2026-49791	microsoft - multiple products	Improper link resolution before file access ('link following') in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to elevate privileges locally.	2026-07-14	7.1
CVE-2026-50354	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7.1
CVE-2026-55144	microsoft - multiple products	Missing cryptographic step in Windows CryptoAPI allows an authorized attacker to perform tampering locally.	2026-07-14	7.1
CVE-2026-56193	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	7.1

CVE-2026-50428	microsoft - multiple products	Out-of-bounds read in Windows Container Isolation FS Filter Driver (unionfs.sys) allows an authorized attacker to disclose information locally.	2026-07-14	7.1
CVE-2026-50451	microsoft - multiple products	Missing authentication for critical function in Windows Routing and Remote Access Service (RRAS) allows an authorized attacker to elevate privileges locally.	2026-07-14	7.1
CVE-2026-50465	microsoft - multiple products	Improper access control in Microsoft Windows DNS allows an authorized attacker to perform tampering locally.	2026-07-14	7.1
CVE-2026-50682	microsoft - multiple products	Out-of-bounds read in Windows Active Directory allows an authorized attacker to deny service over a network.	2026-07-14	7.1
CVE-2026-55122	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-07-14	7.1
CVE-2026-57101	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.	2026-07-14	7.1
CVE-2026-58529	microsoft - multiple products	Out-of-bounds read in Active Directory Federation Services (AD FS) allows an authorized attacker to disclose information over a network.	2026-07-14	7.1
CVE-2026-52865	f5 - multiple products	When NGINX Ingress Controller processes Ingress or TransportServer resources, an authenticated, remote attacker with permission to create or modify Ingress or TransportServer resources can cause the NGINX Ingress Controller process to terminate. Impact: The NGINX Ingress Controller control plane process terminates and enters a persistent crash loop while the malformed Ingress or TransportServer resource remains in the cluster. This vulnerability allows a remote, authenticated attacker with at least Ingress or TransportServer resource write access to cause a denial-of-service (DoS) on the NGINX Ingress Controller system. There is no data plane exposure; this is a control plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-07-15	7.1
CVE-2026-59867	microsoft - kiota	Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.32.5, Kiota resolved OpenAPI $ref values by fetching remote http(s) URLs and reading local absolute or out-of-tree file paths, allowing `kiota generate` on an attacker-controlled or attacker-influenced description to perform build-time SSRF, remote file inclusion, and local file inclusion by inlining external schemas such as REMOTE_KIOTA_PROP or Leaked into generated clients. This issue is fixed in version 1.32.5 by AllowedExternalOriginsStreamLoader and the --allowed-external-origins option.	2026-07-16	7.1
CVE-2026-48571	microsoft - multiple products	Use after free in Windows App Installer allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-48572	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows App Installer allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-49162	microsoft - multiple products	Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-49183	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Clipboard Server allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-49784	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Windows App Store allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-49802	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-49803	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows AppX Deployment Service allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-49805	microsoft - multiple products	Improper access control in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-49806	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50296	microsoft - multiple products	Use after free in Graphics Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50297	microsoft - multiple products	Improper access control in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50323	microsoft - multiple products	Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	7

CVE-2026-50325	microsoft - multiple products	Improper access control in Windows Win32K allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50356	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Windows App Store allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50384	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Clip Service allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-54111	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-54129	microsoft - multiple products	Use after free in Windows Hyper-V allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-54989	microsoft - multiple products	Use after free in Quality Windows Audio/Video Experience (QWAVE) service allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-54996	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-58526	microsoft - multiple products	Use after free in Windows Storage allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50307	microsoft - multiple products	Use after free in Windows TCP/IP allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50322	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50345	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50348	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an unauthorized attacker to elevate privileges over a network.	2026-07-14	7
CVE-2026-50358	microsoft - multiple products	Use after free in Windows Media allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50359	microsoft - multiple products	Use after free in Microsoft XML Core Services allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50371	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows LUAFV allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50372	microsoft - multiple products	Buffer over-read in Windows Redirected Drive Buffering allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50390	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50392	microsoft - multiple products	Use after free in Windows Secure Kernel Mode allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50393	microsoft - multiple products	Use after free in Windows Kernel-Mode Drivers allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50396	microsoft - multiple products	Use after free in Windows Kernel-Mode Drivers allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50397	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50403	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50404	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Media allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50406	microsoft - multiple products	Use after free in Windows Backup Engine allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50410	microsoft - multiple products	Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50449	microsoft - multiple products	Use after free in Windows Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	7

CVE-2026-50452	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an unauthorized attacker to elevate privileges over a network.	2026-07-14	7
CVE-2026-50459	microsoft - multiple products	Use after free in Windows Kernel allows an unauthorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50490	microsoft - multiple products	Use after free in Windows Installer allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50491	microsoft - multiple products	Out-of-bounds read in Code Integrity DLL (ci.dll) allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50503	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Runtime allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50658	microsoft - defender_for_endpoint	Time-of-check time-of-use (toctou) race condition in Microsoft Defender allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50669	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50672	microsoft - multiple products	Use after free in Windows NTFS allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50674	microsoft - multiple products	Use after free in Windows USB Print Driver allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-56173	microsoft - multiple products	Use after free in Windows WebView allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-56183	microsoft - multiple products	Use after free in Windows MIDI Service Module allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-56187	microsoft - multiple products	Use after free in Windows MIDI Service Module allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-57093	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-58544	microsoft - multiple products	Use after free in Windows Management Services allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-58619	microsoft - multiple products	Use after free in Windows Sensor Data Service allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-58629	microsoft - multiple products	Use after free in Windows DirectX allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-58637	microsoft - multiple products	Use after free in Windows Client-Side Caching (CSC) Service allows an authorized attacker to elevate privileges locally.	2026-07-14	7
CVE-2026-50526	microsoft - multiple products	Improper link resolution before file access ('link following') in .NET allows an authorized attacker to perform tampering locally.	2026-07-14	7
CVE-2026-59863	microsoft - kiota	Kiota is an OpenAPI based HTTP Client code generator. Prior to 1.32.5, Kiota honored a poisoned .kiota/workspace.json workspace configuration without validating per-client or per-plugin outputPath values during kiota client generate and kiota plugin generate, allowing a malicious repository or pull request to use absolute paths, rooted POSIX / paths, UNC \\ or // paths, Windows drive X:\ paths, or .. traversal segments to write generated client files outside the workspace root on a developer or CI host. This issue is fixed in version 1.32.5.	2026-07-16	7
CVE-2026-13103	lenovo - App Store	A potential path traversal vulnerability was reported in Lenovo App Store, distributed exclusively in the Chinese market, that could allow a local authenticated user to execute arbitrary code.	2026-07-16	7
CVE-2026-13104	lenovo - App Store	A potential vulnerability was reported in Lenovo App Store, distributed exclusively in the Chinese market, that could allow a local authenticated user to execute arbitrary code with elevated privileges.	2026-07-16	7
CVE-2026-58598	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Backup Engine allows an authorized attacker to elevate privileges locally.	2026-07-16	7
CVE-2026-53566	citrix - Citrix Secure Access Client for Windows	Out-of-bounds read vulnerability in Citrix Citrix Secure Access Client for Windows. This issue affects Citrix Secure Access Client for Windows: before 26.6.1.20.	2026-07-14	6.8
CVE-2026-49168	microsoft - multiple products	Integer overflow or wraparound in Windows Storage Spaces Direct allows an unauthorized attacker to elevate privileges with a physical attack.	2026-07-14	6.8
CVE-2026-50298	microsoft - multiple products	Integer overflow or wraparound in Windows Spaceport.sys allows an unauthorized attacker to elevate privileges with a physical attack.	2026-07-14	6.8

CVE-2026-50299	microsoft - multiple products	Integer overflow or wraparound in Windows Storage Spaces Direct allows an unauthorized attacker to execute code with a physical attack.	2026-07-14	6.8
CVE-2026-54132	microsoft - multiple products	Heap-based buffer overflow in Windows Kernel allows an unauthorized attacker to elevate privileges with a physical attack.	2026-07-14	6.8
CVE-2026-50426	microsoft - multiple products	Relative path traversal in DNS Server allows an authorized attacker to execute code over an adjacent network.	2026-07-14	6.8
CVE-2026-50492	microsoft - multiple products	Heap-based buffer overflow in Windows Resilient File System (ReFS) allows an unauthorized attacker to execute code with a physical attack.	2026-07-14	6.8
CVE-2026-50668	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to elevate privileges with a physical attack.	2026-07-14	6.8
CVE-2026-58528	microsoft - multiple products	Out-of-bounds read in Windows USB Audio Class driver (usbaudio.sys) allows an unauthorized attacker to disclose information with a physical attack.	2026-07-14	6.8
CVE-2026-48338	adobe - multiple products	ColdFusion is 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 does not require user interaction. Scope is changed.	2026-07-14	6.8
CVE-2026-48312	adobe - multiple products	CAI Content Credentials is affected by an Improper Input Validation 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.	2026-07-14	6.8
CVE-2026-10587	lenovo - multiple products	A potential out-of-bounds write vulnerability could allow a local privileged attacker to modify power management settings in System Management Mode.	2026-07-16	6.8
CVE-2026-10589	lenovo - multiple products	A potential out of bounds write vulnerability could allow a local privileged attacker to execute code in System Management Mode.	2026-07-16	6.8
CVE-2026-6511	lenovo - Smart Connect	During an internal security assessment, a potential improper access control vulnerability was discovered in Lenovo Smart Connect for Windows that could allow a local authenticated user to access files owned by a different user on the same system.	2026-07-16	6.8
CVE-2026-49501	dell - multiple products	Dell PowerScale OneFS versions 9.5.0.0 through 9.10.1.7, and versions 9.11.0.0 through 9.13.0.2 contains an Improper Privilege Management vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-07-15	6.7
CVE-2026-10588	lenovo - multiple products	A potential vulnerability could allow a local privileged attacker to disclose the address of protected System Management Mode memory.	2026-07-16	6.7
CVE-2026-10590	lenovo - multiple products	A potential missing authentication vulnerability could allow a local privileged attacker to use WMI commands to arbitrarily trigger a System Management Interrupt handler.	2026-07-16	6.7
CVE-2026-59837	fortinet - multiple products	A stack-based buffer overflow vulnerability in Fortinet FortiOS 7.4.0 through 7.4.1, FortiOS 7.2 all versions, FortiPAM 1.8.0 through 1.8.2, FortiPAM 1.7 all versions, FortiPAM 1.6 all versions, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions, FortiProxy 7.4.0 through 7.4.13, FortiProxy 7.2 all versions may allow a privileged authenticated attacker who can bypass stack protection and ASLR to execute arbitrary code or commands via crafted HTTP requests.	2026-07-14	6.6
CVE-2026-49804	microsoft - multiple products	Heap-based buffer overflow in Windows USB Video Driver allows an unauthorized attacker to elevate privileges with a physical attack.	2026-07-14	6.6
CVE-2026-50678	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-07-14	6.6
CVE-2026-58554	huawei - multiple products	Permission control vulnerability in the Settings module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-07-15	6.6
CVE-2026-58555	huawei - HarmonyOS	Permission bypass vulnerability in the card module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-07-15	6.6
CVE-2026-49876	apache - gravitino	Authenticated SSRF in Gravitino JobManager allows server-side HTTP requests to internal network and cloud metadata endpoints via unvalidated job template URIs. A vulnerability in Apache Gravitino. This issue affects Apache Gravitino: from 1.0.0 through 1.2.1. Users are recommended to upgrade to version 1.3.0, which fixes the issue.	2026-07-13	6.5
CVE-2026-62147	red hat - multiple products	The Tempo Operator's gateway component failed to consistently apply namespace-scoped redaction on some query API response paths when query RBAC was enabled, allowing an authenticated user to read span attributes belonging to other tenants' namespaces.	2026-07-13	6.5
CVE-2026-49488	apache - openmeetings	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache OpenMeetings. This issue affects Apache OpenMeetings: from 5.0.0 before 9.1.0. An attacker with moderator rights in any room can read arbitrary files accessible to the OS account running the OM server, including credentials and secrets, via a crafted download request. Users are recommended to upgrade to version 9.1.0, which fixes the issue.	2026-07-14	6.5
CVE-2026-34348	microsoft - multiple products	Protection mechanism failure in Windows Event Logging Service allows an authorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-47282	microsoft - visual_studio_code	Insufficiently protected credentials in GitHub Copilot and Visual Studio Code allows an unauthorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-49799	microsoft - multiple products	Uncontrolled resource consumption in Windows Local Security Authority Subsystem Service (LSASS) allows an authorized attacker to deny service over a network.	2026-07-14	6.5

CVE-2026-54108	microsoft - multiple products	External control of file name or path in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-07-14	6.5
CVE-2026-55003	microsoft - multiple products	Use of uninitialized resource in Windows RDP allows an unauthorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-56185	microsoft - windows_admin_center	Improper authentication in Windows Admin Center allows an authorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-57976	microsoft - multiple products	Null pointer dereference in Active Directory Domain Services allows an authorized attacker to deny service over a network.	2026-07-14	6.5
CVE-2026-57979	microsoft - multiple products	Out-of-bounds read in Windows RDP allows an unauthorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-58279	microsoft - azure_cyclecloud	Missing authorization in Azure CycleCloud allows an authorized attacker to elevate privileges over a network.	2026-07-14	6.5
CVE-2026-50366	microsoft - multiple products	Null pointer dereference in Active Directory Domain Services allows an authorized attacker to deny service over a network.	2026-07-14	6.5
CVE-2026-50376	microsoft - multiple products	Use of uninitialized resource in Windows RDP allows an unauthorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-50445	microsoft - multiple products	Buffer over-read in Windows RDP allows an unauthorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-50468	microsoft - multiple products	Buffer over-read in SQL Server allows an authorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-50497	microsoft - multiple products	Off-by-one error in Windows Remote Desktop Protocol allows an unauthorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-50504	microsoft - multiple products	Buffer over-read in Remote Desktop Client allows an unauthorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-54116	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in SQL Server allows an authorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-54126	microsoft - multiple products	Out-of-bounds read in Windows RDP allows an unauthorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-55051	microsoft - multiple products	Server-side request forgery (ssrf) in Microsoft Office SharePoint allows an authorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-55054	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-56168	microsoft - multiple products	Null pointer dereference in Windows SMB Server allows an authorized attacker to deny service over a network.	2026-07-14	6.5
CVE-2026-57982	microsoft - multiple products	Use of uninitialized resource in Windows RDP allows an authorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-58533	microsoft - multiple products	Use of uninitialized resource in Windows RDP allows an unauthorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-58535	microsoft - multiple products	Use of uninitialized resource in Windows RDP allows an unauthorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-58539	microsoft - multiple products	Out-of-bounds read in Windows RDP allows an unauthorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-58546	microsoft - multiple products	Use of uninitialized resource in Windows RDP allows an unauthorized attacker to disclose information over a network.	2026-07-14	6.5
CVE-2026-15714	red hat - multiple products	An out-of-bounds read vulnerability was found in libsoup's multipart processing subsystem. The flaw exists in the soup_multipart_input_stream_read_headers() function inside soup-multipart-input-stream.c, which does not adequately restrict or validate the size of incoming multipart boundary strings. When processing a crafted HTTP response containing a malformed or oversized boundary parameter, the internal stream reader reads past the allocated buffer bounds. A remote, unauthenticated attacker can exploit this behavior to cause a service denial (DoS) through application failure or potentially read fragments of unauthorized memory metadata.	2026-07-14	6.5
CVE-2026-50659	microsoft - .net_framework	Improper encoding or escaping of output in .NET allows an authorized attacker to perform spoofing over a network.	2026-07-14	6.5
CVE-2026-15766	google - chrome	Uninitialized Use in Skia in Google Chrome prior to 150.0.7871.125 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-07-14	6.5

CVE-2026-15768	google - chrome	Insufficient policy enforcement in HTML-in-Canvas in Google Chrome prior to 150.0.7871.125 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	2026-07-14	6.5
CVE-2026-15770	google - chrome	Uninitialized Use in V8 in Google Chrome prior to 150.0.7871.125 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-07-14	6.5
CVE-2026-15775	google - chrome	Inappropriate implementation in V8 in Google Chrome prior to 150.0.7871.125 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	2026-07-14	6.5
CVE-2026-15778	google - chrome	Insufficient validation of untrusted input in Navigation in Google Chrome prior to 150.0.7871.125 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-07-14	6.5
CVE-2026-58559	huawei - multiple products	DoS vulnerability in the vibration service. Impact: Successful exploitation of this vulnerability may affect availability.	2026-07-15	6.5
CVE-2026-55440	microsoft - UFO	Microsoft UFO open-source framework for intelligent automation across devices and platforms. Prior to 3.0.7, the COMMAND_RESULTS handler in ufo/server/ws/handler.py called get_or_create_session in ufo/server/services/session_manager.py without owner_client_id, allowing an authenticated client to create an unowned attacker-chosen session_id such as constellation_task_id = f"{task_name}@{task_id}" and deny the legitimate owner or exhaust memory with phantom sessions. This issue is fixed in version 3.0.7.	2026-07-16	6.5
CVE-2026-55000	microsoft - multiple products	Use after free in Windows USB Print Driver allows an unauthorized attacker to elevate privileges with a physical attack.	2026-07-14	6.4
CVE-2026-57097	microsoft - multiple products	Untrusted search path in Microsoft XML allows an unauthorized attacker to bypass a security feature with a physical attack.	2026-07-14	6.4
CVE-2026-15757	netgear - DGND3700v1	A security flaw was discovered in the NETGEAR DGND3700v1 that could allow someone on the same local WiFi network to send unauthorized commands to the device. This issue was identified through testing in a controlled research environment using a simulated version of the router's software and has not been confirmed on physical production devices.	2026-07-14	6.3
CVE-2026-50374	microsoft - multiple products	Use after free in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges with a physical attack.	2026-07-14	6.3
CVE-2026-50375	microsoft - multiple products	Heap-based buffer overflow in Windows DirectX allows an authorized attacker to elevate privileges locally.	2026-07-14	6.3
CVE-2026-55145	microsoft - copilot	Improper neutralization of special elements used in a command ('command injection') in Outlook Copilot allows an authorized attacker to perform tampering over a network.	2026-07-14	6.3
CVE-2026-57973	microsoft - windows_subsystem_for_linux	Time-of-check time-of-use (toctou) race condition in Windows Subsystem for Linux allows an authorized attacker to perform tampering locally.	2026-07-14	6.3
CVE-2026-58543	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows USB Print Driver allows an authorized attacker to elevate privileges with a physical attack.	2026-07-14	6.3
CVE-2026-60065	f5 - NGINX Plus	When NGINX Plus is configured to use the Message Queuing Telemetry Transport (MQTT) filter module (ngx_stream_mqtt_filter_module), unauthenticated attackers can send requests with conditions beyond the attacker's control to cause a heap buffer over-read in the NGINX worker process, leading to a restart. Impact: This vulnerability may allow remote unauthenticated attackers to have limited control to restart the NGINX worker process. There is no control plane exposure; this is a data plane issue only. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-07-15	6.3
CVE-2026-49807	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows DirectX allows an unauthorized attacker to disclose information locally.	2026-07-14	6.2
CVE-2026-50294	microsoft - multiple products	Exposure of sensitive system information to an unauthorized control sphere in Windows Kernel allows an unauthorized attacker to disclose information locally.	2026-07-14	6.2
CVE-2026-50420	microsoft - multiple products	Out-of-bounds read in Windows HTTP.sys allows an unauthorized attacker to disclose information locally.	2026-07-14	6.2
CVE-2026-55026	microsoft - multiple products	Integer overflow or wraparound in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	6.2
CVE-2026-57095	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Win32K allows an unauthorized attacker to elevate privileges locally.	2026-07-14	6.2
CVE-2026-48296	adobe - multiple products	CAI Content Credentials is 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.	2026-07-14	6.2
CVE-2026-48298	adobe - multiple products	CAI Content Credentials is 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.	2026-07-14	6.2

CVE-2026-48302	adobe - multiple products	CAI Content Credentials is 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.	2026-07-14	6.2
CVE-2026-48354	adobe - multiple products	CAI Content Credentials is 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.	2026-07-14	6.2
CVE-2026-48357	adobe - multiple products	CAI Content Credentials is 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.	2026-07-14	6.2
CVE-2026-23573	fortinet - multiple products	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability [CWE-79] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.6, FortiOS 7.4 all versions, FortiOS 7.2 all versions, FortiPAM 1.8.0, FortiPAM 1.7 all versions, FortiPAM 1.6 all versions, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions, FortiProxy 7.4.0 through 7.4.3, FortiProxy 7.2.0 through 7.2.9 may allow an authenticated remote user to execute code or commands via crafted requests.	2026-07-14	6.1
CVE-2026-49174	microsoft - multiple products	Missing authentication for critical function in Microsoft Windows DNS allows an authorized attacker to perform tampering locally.	2026-07-14	6.1
CVE-2026-54988	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-07-14	6.1
CVE-2026-50383	microsoft - multiple products	Buffer over-read in Windows Print Spooler Components allows an authorized attacker to disclose information locally.	2026-07-14	6.1
CVE-2026-50453	microsoft - multiple products	Out-of-bounds read in Windows USB Audio Class driver (usbaudio.sys) allows an unauthorized attacker to disclose information with a physical attack.	2026-07-14	6.1
CVE-2026-50495	microsoft - multiple products	Improper access control in Microsoft Windows DNS allows an authorized attacker to perform tampering locally.	2026-07-14	6.1
CVE-2026-50661	microsoft - multiple products	Protection mechanism failure in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2026-07-14	6.1
CVE-2026-55898	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-07-14	6.1
CVE-2026-15779	red hat - multiple products	A flaw was found in samba's pam_winbind. When mkhomedir is enabled, pam_winbind chowns the target account's home directory without validating the path is not a critical system directory such as /. On affected systems, accounts with / as their home directory (a common default for system accounts) can have this triggered not only by root, but by a non-root user holding a narrow sudo delegation to run commands as that account, causing ownership of / to change and resulting in severe denial of service (SSH, sudo, and package-manager failures). The change does not grant write access to / (which ships with restrictive 0555 permissions on RHEL), so the impact is availability loss rather than further privilege escalation.	2026-07-15	6.1
CVE-2026-56087	dell - ThinOS 10	Dell ThinOS 10, versions prior to 2605_10.2100 contain a Protection Mechanism Failure vulnerability. An attacker with physical access could potentially exploit this vulnerability, leading to unauthorized access to encrypted data.	2026-07-15	6.1
CVE-2026-58643	microsoft - windows_admin_center	Improper neutralization of input during web page generation ('cross-site scripting') in Windows Admin Center allows an unauthorized attacker to perform spoofing over a network.	2026-07-16	6.1
CVE-2026-54429	siemens - SIMATIC S7-PLCSIM Advanced	A vulnerability has been identified in SIMATIC S7-PLCSIM Advanced (All versions). Affected devices do not properly handle high-volume multicast network traffic, which can exhaust available memory resources in the affected application. This could allow an unauthenticated attacker on the local network segment to cause a denial-of-service condition of the affected application. The affected application becomes inaccessible and requires a manual restart; no project data is lost. Successful exploitation requires a specific project configuration to be already active on the targeted instance.	2026-07-14	6
CVE-2026-12588	trellix - Trellix HX Console	An attacker with access to an HX 10.0.0 and previous versions, may send specially-crafted data to the HX console. The malicious detection would then trigger decompression of a large file that consumes an excessive amount of system resources thus causing a Denial of Service.	2026-07-14	6
CVE-2026-58638	microsoft - multiple products	Missing cryptographic step in Windows Boot Loader allows an authorized attacker to bypass a security feature locally.	2026-07-14	6
CVE-2026-50324	microsoft - multiple products	Loop with unreachable exit condition ('infinite loop') in Active Directory Federation Services (AD FS) allows an unauthorized attacker to deny service over a network.	2026-07-14	5.9
CVE-2026-56649	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Network File System allows an unauthorized attacker to execute code over a network.	2026-07-14	5.9
CVE-2026-15712	red hat - Red Hat Enterprise Linux 10	A heap buffer over-read vulnerability was discovered in libsoup's (versions: libsoup 3.0 to 3.7.0) HTTP/2 connection tracking framework. When the library processes an HTTP/2 GOAWAY frame, it improperly handles the "Additional Debug Data" payload by assuming the data stream is a safely NUL-terminated C-string. Because the parser lacks strict length-boundary verification before reading this data, a remote, unauthenticated attacker can intentionally send a malformed GOAWAY frame missing the appropriate null delimiter. This causes the library to read past the end of the allocated buffer, triggering an application crash that results in a denial of service (DoS), or potentially exposing fragments of memory contents.	2026-07-14	5.9

CVE-2026-15713	red hat - multiple products	A vulnerability was found in libsoup's HTTP/2 protocol implementation. The library fails to correctly release memory context blocks under specific stream termination conditions, such as when an HTTP/2 connection encounters window exhaustion or explicit stream resets. A remote, unauthenticated attacker acting as a malicious network peer can trick the connection engine into allocating stream states that are subsequently leaked during cleanup. Over a sustained period, this flaw allows the remote attacker to consume the system's heap allocations incrementally, triggering a denial of service (DoS) through an ultimate Out-of-Memory (OOM) application crash.	2026-07-14	5.9
CVE-2026-47997	adobe - multiple products	Adobe Commerce is 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 read access. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue does not require user interaction.	2026-07-14	5.9
CVE-2026-47998	adobe - multiple products	Adobe Commerce is 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 read access. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue does not require user interaction.	2026-07-14	5.9
CVE-2026-48308	adobe - multiple products	Premiere Pro is affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-14	5.9
CVE-2026-59838	fortinet - multiple products	A improper neutralization of script-related html tags in a web page (basic xss) vulnerability in Fortinet FortiSIEM 7.4.0, FortiSIEM 7.3.0 through 7.3.4, FortiSIEM 7.2.0 through 7.2.6, FortiSIEM 7.1 all versions, FortiSIEM 7.0 all versions, FortiSIEM 6.7 all versions, FortiSIEM 6.6 all versions, FortiSIEM 6.5 all versions, FortiSIEM 6.4 all versions may allow attacker to execute unauthorized code or commands via <insert attack vector here>	2026-07-15	5.9
CVE-2026-62655	netgear - multiple products	A security flaw was found in certain NETGEAR Orbi models that could allow an unauthorized user to cause the device to stop responding or restart unexpectedly, disrupting network connectivity and making the device temporarily unavailable.	2026-07-14	5.7
CVE-2026-53364	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_conn: Fix memory leak in hci_le_big_terminate() hci_le_big_terminate() allocates iso_list_data via kzalloc_obj but returns 0 without freeing it when neither pa_sync_term nor big_sync_term flags are set after evaluating the PA and BIG sync connection state. This early-return path was introduced when hci_le_big_terminate() was refactored to take struct hci_conn instead of raw u8 parameters, adding PA/BIG flag evaluation logic. The existing kfree() on hci_cmd_sync_queue failure does not cover this path.	2026-07-13	5.5
CVE-2026-53365	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: vsock/virtio: fix zerocopy completion for multi-skb sends When a large message is fragmented into multiple skbs, the zerocopy uarg is only allocated and attached to the last skb in the loop. Non-final skbs carry pinned user pages with no completion tracking, so the kernel has no way to notify userspace when those pages are safe to reuse. If the loop breaks early the uarg is never allocated at all, leaking pinned pages with no completion notification. Fix this by following the approach used by TCP: allocate the zerocopy uarg (if not provided by the caller) before the send loop and attach it to every skb via skb_zcopy_set(), which takes a reference per skb. Each skb's completion properly decrements the refcount, and the notification only fires after the last skb is freed. On failure, if no data was sent, the uarg is cleanly aborted via net_zcopy_put_abort(). This issue was initially discovered by sashiko while reviewing commit 1cb36e252211 ("vsock/virtio: fix MSG_ZEROCOPY pinned-pages accounting") but was pre-existing.	2026-07-13	5.5
CVE-2026-59839	fortinet - multiple products	A improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiOS 7.6.0 through 7.6.6, FortiOS 7.4.0 through 7.4.9, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions, FortiPAM 1.8.0, FortiPAM 1.7.0 through 1.7.2, FortiPAM 1.6 all versions, FortiPAM 1.5 all versions, FortiPAM 1.4 all versions, FortiPAM 1.3 all versions, FortiPAM 1.2 all versions, FortiPAM 1.1 all versions, FortiPAM 1.0 all versions, FortiProxy 7.6.0 through 7.6.5, FortiProxy 7.4 through 7.4.13, FortiProxy 7.2 all versions, FortiProxy 7.0 all versions may allow attacker to execute unauthorized code or commands via <insert attack vector here>	2026-07-14	5.5
CVE-2026-33842	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-34328	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Audio Service allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-34346	microsoft - multiple products	Cleartext transmission of sensitive information in Windows Ancillary Function Driver for WinSock allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-34349	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Media allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-40422	microsoft - multiple products	Use of uninitialized resource in Windows File Explorer allows an authorized attacker to disclose information locally.	2026-07-14	5.5

CVE-2026-41087	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-45496	microsoft - visual_studio_code	Improper limitation of a pathname to a restricted directory ('path traversal') in Visual Studio Code allows an unauthorized attacker to bypass a security feature locally.	2026-07-14	5.5
CVE-2026-49180	microsoft - multiple products	Improper link resolution before file access ('link following') in Universal Plug and Play (upnp.dll) allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-49801	microsoft - multiple products	Use of uninitialized resource in Windows SMB allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50295	microsoft - multiple products	Improper privilege management in Microsoft Windows DNS allows an authorized attacker to bypass a security feature locally.	2026-07-14	5.5
CVE-2026-50300	microsoft - multiple products	Integer underflow (wrap or wraparound) in Windows Kernel allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50303	microsoft - multiple products	Use of a cryptographic primitive with a risky implementation in Windows Key Guard allows an authorized attacker to bypass a security feature locally.	2026-07-14	5.5
CVE-2026-50316	microsoft - multiple products	Insertion of sensitive information into log file in Windows Kernel allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50350	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Trusted Runtime Interface Driver allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50381	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Composite Image File System Driver allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-54997	microsoft - multiple products	Use of uninitialized resource in Windows SMB allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-58614	microsoft - multiple products	Out-of-bounds read in Windows Kernel allows an authorized attacker to bypass a security feature locally.	2026-07-14	5.5
CVE-2026-47969	adobe - multiple products	Audition is 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.	2026-07-14	5.5
CVE-2026-48580	microsoft - multiple products	Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-49177	microsoft - multiple products	Out-of-bounds read in Windows TCP/IP allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50334	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Notification allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50339	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Push Notifications allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50341	microsoft - multiple products	Buffer over-read in Windows NTFS allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50352	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Cryptographic Services allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50377	microsoft - multiple products	Out-of-bounds read in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	5.5
CVE-2026-50389	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50394	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Media allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50401	microsoft - multiple products	Out-of-bounds read in Windows Cloud Files Mini Filter Driver allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50408	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50409	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Overlay Filter allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50430	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Push Notifications allows an authorized attacker to disclose information locally.	2026-07-14	5.5

CVE-2026-50431	microsoft - multiple products	Windows Quality of Service (QoS) Packet Scheduler Information Disclosure Vulnerability	2026-07-14	5.5
CVE-2026-50434	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Push Notifications allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50437	microsoft - multiple products	Out-of-bounds read in Windows DWM Core Library allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50442	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50455	microsoft - multiple products	Use of uninitialized resource in Universal Plug and Play (upnp.dll) allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50456	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50473	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50475	microsoft - multiple products	Buffer over-read in Windows Kernel allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50483	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Microsoft Graphics Component allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50681	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Cryptographic Services allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-50690	microsoft - multiple products	Use of uninitialized resource in Windows SMB allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55023	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55027	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55028	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55035	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55042	microsoft - multiple products	Use of uninitialized resource in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55046	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55047	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55050	microsoft - multiple products	Out-of-bounds read in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55057	microsoft - multiple products	Integer overflow or wraparound in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55121	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55124	microsoft - multiple products	Improper validation of specified type of input in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55138	microsoft - multiple products	Untrusted pointer dereference in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55139	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-55142	microsoft - multiple products	Numeric truncation error in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-56178	microsoft - defender_for_endpoint	Time-of-check time-of-use (toctou) race condition in Microsoft Defender for Endpoint allows an authorized attacker to elevate privileges locally.	2026-07-14	5.5

CVE-2026-56184	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Win32K allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-56192	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-56195	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-57083	microsoft - multiple products	Use of uninitialized resource in Microsoft Windows Codecs Library allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-57084	microsoft - multiple products	Use of uninitialized resource in Windows File Explorer allows an unauthorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-57085	microsoft - multiple products	Out-of-bounds read in Windows Print Spooler Components allows an authorized attacker to disclose information locally.	2026-07-14	5.5
CVE-2026-58545	microsoft - multiple products	Improper access control in Windows Kernel allows an authorized attacker to bypass a security feature locally.	2026-07-14	5.5
CVE-2026-58547	microsoft - multiple products	Heap-based buffer overflow in Universal Plug and Play (upnp.dll) allows an authorized attacker to elevate privileges locally.	2026-07-14	5.5
CVE-2026-47979	adobe - multiple products	Media Encoder is 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.	2026-07-14	5.5
CVE-2026-48353	adobe - multiple products	CAI Content Credentials is affected by an Improper Input Validation 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.	2026-07-14	5.5
CVE-2026-20146	cisco - multiple products	A vulnerability in Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) could allow an authenticated, remote attacker to perform path traversal attacks on the underlying operating system to either read or delete arbitrary files. To exploit this vulnerability, the attacker must have valid administrative credentials. _x000D_ _x000D_ This vulnerability is due to improper validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected system. A successful exploit could allow the attacker to access sensitive files or delete arbitrary files on the affected system.	2026-07-15	5.5
CVE-2026-15719	mozilla - firefox	We are aware that exploit code for this is public however we are not aware of any attacks in the wild abusing this flaw. This vulnerability was fixed in Firefox 152.0.6, Firefox ESR 115.38, Firefox ESR 140.13, and Thunderbird 140.13.	2026-07-14	5.4
CVE-2026-56157	microsoft - multiple products	Improper access control in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-07-14	5.4
CVE-2026-62656	netgear - multiple products	A security flaw was found in certain NETGEAR RAX models that could allow a logged-in user to send specially crafted requests to the router and run unauthorized commands. This could enable the user to make unauthorized changes to the router and affect its security and operation.	2026-07-14	5.4
CVE-2026-48253	adobe - multiple products	Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-07-14	5.4
CVE-2026-48254	adobe - multiple products	Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-07-14	5.4
CVE-2026-48255	adobe - multiple products	Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-07-14	5.4
CVE-2026-48257	adobe - multiple products	Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-07-14	5.4
CVE-2026-48260	adobe - multiple products	Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-07-14	5.4
CVE-2026-48261	adobe - multiple products	Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-07-14	5.4
CVE-2026-48262	adobe - multiple products	Adobe Experience Manager is affected by a DOM-based Cross-Site Scripting (XSS) vulnerability. An attacker could exploit this issue by manipulating the DOM environment to execute malicious JavaScript within the context of the victim's browser. Exploitation of this issue requires user interaction in that a victim must visit a crafted webpage. Scope is changed.	2026-07-14	5.4

CVE-2026-48263	adobe - multiple products	Adobe Experience Manager is 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. Scope is changed.	2026-07-14	5.4
CVE-2026-48355	adobe - multiple products	Adobe Experience Manager is 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. Scope is changed.	2026-07-14	5.4
CVE-2026-48371	adobe - multiple products	Adobe Commerce is 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. Scope is changed.	2026-07-14	5.4
CVE-2026-26032	apache - ivy	The PackagerResolver of Apache Ivy is able to download online artifacts and to (re)package them in a format defined by a packager.xml file. This repackaging is done by an Ant script, which is stored in a subdirectory of the configured "buildRoot" directory. This subdirectory is calculated based on modules coordinates, like the organisation, name or version. If one of the coordinates contains "../" sequences - which are valid characters for Ivy coordinates in general- it is possible to break out of the configured "buildRoot" directory where other files can be overwritten. In order to exploit this vulnerability an attacker needs to have access to a packager repository and add or modify the coordinates in ivy.xml files to have such "../" sequences. Users of Apache Ivy 2.0.0 to 2.5.3 (inclusive) should upgrade to Ivy 2.6.0.	2026-07-15	5.4
CVE-2026-15485	trendnet - TEW-821DAP	A flaw has been found in TRENDnet TEW-821DAP 1.11B03. The impacted element is the function sub_43F2C4 of the file /goform/tools_nslookup of the component DNS Lookup Handler. This manipulation of the argument nslookup_target/dns_server causes os command injection. The attack can be initiated remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer.	2026-07-12	5.3
CVE-2026-15486	trendnet - TEW-821DAP	A vulnerability has been found in TRENDnet TEW-821DAP 1.11B03. This affects the function sub_42026C of the file /goform/tools_ddns of the component Firmware Update Handler. Such manipulation of the argument hostname/username/password leads to os command injection. The attack can be launched remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer.	2026-07-12	5.3
CVE-2026-15487	trendnet - TEW-821DAP	A vulnerability was found in TRENDnet TEW-821DAP 1.11B03. This impacts the function sub_41FBD0 of the file /goform/system_ntp of the component Firmware Update Handler. Performing a manipulation of the argument Hostname results in os command injection. The attack may be initiated remotely. The vendor explains: "We are unable to confirm the existence of the vulnerabilities for (...) TEW-821DAP (v1.0R) as these items have been EOL. " This vulnerability only affects products that are no longer supported by the maintainer.	2026-07-12	5.3
CVE-2026-14906	mozilla - firefox_mobile	Pages with malicious titles could potentially allow saved PDF content to overwrite PDF files or bundled content within the Firefox for iOS application sandbox. This vulnerability was fixed in Firefox for iOS 152.4.	2026-07-13	5.3
CVE-2026-44806	microsoft - multiple products	Missing release of memory after effective lifetime in Windows Cryptographic Services allows an unauthorized attacker to deny service over a network.	2026-07-14	5.3
CVE-2026-56164	microsoft - multiple products	Missing authentication for critical function in Microsoft Office SharePoint allows an unauthorized attacker to elevate privileges over a network.	2026-07-14	5.3
CVE-2026-50415	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Media allows an unauthorized attacker to disclose information over a network.	2026-07-14	5.3
CVE-2026-50432	microsoft - multiple products	Use after free in Windows Virtual Filtering Platform (VFP) allows an authorized attacker to deny service over a network.	2026-07-14	5.3
CVE-2026-15771	google - chrome	Insufficient validation of untrusted input in Media in Google Chrome on Windows prior to 150.0.7871.125 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)	2026-07-14	5.3
CVE-2026-60062	f5 - multiple products	The NGINX Agent config_dirs directive allows a low-privileged attacker to gain limited read and write access to files outside of the designated secure directory. The config_dirs directive required for this issue can also be configured through NGINX Instance Manager. A successful exploit may allow an attacker to cross a security boundary. Impact: A remotely authenticated low-privileged attacker could gain limited read and write access outside of the list of directories specified in the NGINX Agent configuration. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	2026-07-15	5.3
CVE-2026-50418	microsoft - multiple products	Improper access control in Windows System allows an unauthorized attacker to bypass a security feature locally.	2026-07-14	5.1
CVE-2026-58551	huawei - HarmonyOS	Out-of-bounds read vulnerability in the image codec module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-07-15	5.1
CVE-2026-58552	huawei - HarmonyOS	Out-of-bounds read vulnerability in the image codec module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-07-15	5.1
CVE-2026-58556	huawei - multiple products	Permission control vulnerability in the Bluetooth module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-07-15	5.1

CVE-2026-62657	netgear - multiple products	A security flaw in the router's certificate validation process was discovered in the NETGEAR XR1000 Gaming Router and certain Nighthawk models that could allow an unauthorized person to remotely access and take control of the device.	2026-07-14	4.9
CVE-2026-12478	red hat - Red Hat Enterprise Linux 10	The fix for CVE-2026-0716 (commit 6ff7ef0, libsoup 3.6.6) placed the integer overflow guard inside the if (masked) block, leaving unmasked server-to-client frames unprotected. A malicious WebSocket server can send a crafted unmasked frame with a payload length near UINT64_MAX to trigger an OOB read in a libsoup-based client when max_incoming_payload_size is set to 0.	2026-07-14	4.8
CVE-2026-50684	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Active Directory Federation Services (AD FS) allows an authorized attacker to perform spoofing over a network.	2026-07-14	4.8
CVE-2026-47999	adobe - multiple products	Adobe Commerce is 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.	2026-07-14	4.8
CVE-2026-58557	huawei - HarmonyOS	Design defect vulnerability in Expedition mode. Impact: Successful exploitation of this vulnerability may affect availability.	2026-07-15	4.8
CVE-2026-49167	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-07-14	4.7
CVE-2026-50310	microsoft - multiple products	Integer overflow or wraparound in Windows Devices Human Interface allows an authorized attacker to disclose information locally.	2026-07-14	4.7
CVE-2026-50312	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-07-14	4.7
CVE-2026-50657	microsoft - defender_for_endpoint	Exposure of private personal information to an unauthorized actor in Microsoft Defender allows an authorized attacker to disclose information locally.	2026-07-14	4.7
CVE-2026-62658	netgear - multiple products	A security flaw was discovered in certain NETGEAR Nighthawk RAX series routers that could allow someone already logged in to the device to run unauthorized commands or code on the router.	2026-07-14	4.7
CVE-2026-49794	microsoft - multiple products	Out-of-bounds read in Windows USB Audio Class driver (usbaudio.sys) allows an unauthorized attacker to disclose information with a physical attack.	2026-07-14	4.6
CVE-2026-55016	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-07-14	4.6
CVE-2026-55019	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-07-14	4.6
CVE-2026-55020	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-07-14	4.6
CVE-2026-55030	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-07-14	4.6
CVE-2026-55135	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-07-14	4.6
CVE-2026-62826	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office SharePoint allows an authorized attacker to perform spoofing over a network.	2026-07-16	4.6
CVE-2026-50485	microsoft - multiple products	Buffer over-read in Windows Hyper-V allows an authorized attacker to deny service over an adjacent network.	2026-07-14	4.5
CVE-2026-15718	mozilla - firefox	We are aware that exploit code for this is public however we are not aware of any attacks in the wild abusing this flaw. This vulnerability was fixed in Firefox 152.0.6, Firefox ESR 140.13, and Thunderbird 140.13.	2026-07-14	4.3
CVE-2026-62393	apache - kylin	Improper Handling of Insufficient Permissions or Privileges vulnerability in Apache Kylin. Improper authorization in job information retrieval, where an attacker may get access to unauthorized jobs in other projects. This issue affects Apache Kylin: from 4 through 5.0.3. Users are recommended to upgrade to version 5.0.4, which fixes the issue.	2026-07-14	4.3
CVE-2025-43892	fortinet - multiple products	A buffer over-read vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions may allow an authenticated remote attacker to return a portion of device memory in the redirect response via submitting a specially crafted request.	2026-07-14	4.3
CVE-2026-59840	fortinet - multiple products	A buffer over-read vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions, FortiProxy 7.6.0 through 7.6.5, FortiProxy 7.4.0 through 7.4.13, FortiProxy 7.2 all versions, FortiProxy 7.0 all versions may allow attacker to information disclosure via <insert attack vector here>	2026-07-14	4.3
CVE-2026-62659	netgear - WAX333	A security flaw was discovered in the NETGEAR WAX333 Access Point that could allow someone already logged in and connected to the local network to make unauthorized changes to the device's settings	2026-07-14	4.3
CVE-2026-48000	adobe - multiple products	Adobe Commerce is affected by an Improper Redirect (Open Redirect) vulnerability that could result in a Security feature bypass. An attacker could construct a malicious URL that redirects a victim to an attacker-controlled site, potentially enabling credential theft and account	2026-07-14	4.3

		takeover. Exploitation of this issue requires user interaction in that a victim must click on a malicious link.		
CVE-2026-54568	microsoft - UFO	Microsoft UFO open-source framework for intelligent automation across devices and platforms. From 3.0.0 until 3.0.6, a client connected to the UFO WebSocket server as a DEVICE could call DEVICE_INFO_REQUEST with another device's target_id and receive that device's server-side system_info through ufo/server/ws/handler.py, because handle_device_info_request and get_device_info did not enforce the constellation-only role or object-level authorization boundary. This issue is fixed in version 3.0.6.	2026-07-16	4.3
CVE-2026-57205	microsoft - simplechat	SimpleChat is a secure AI conversation application with personal and group workspaces for document-grounded interactions. Prior to 0.241.203, the authenticated GET /api/user/info/<user_id> and GET /api/user/profile-image/<user_id> endpoints in application/single_app/route_backend_users.py accepted a caller-supplied user_id and read the matching Cosmos DB user-settings document without object-level authorization, allowing a low-privilege authenticated user to retrieve another user's email address, display name, and profile image. This issue is fixed in version 0.241.203.	2026-07-16	4.3
CVE-2026-15945	red hat - multiple products	A flaw was found in the group search functionality of the Keycloak server's administrative API. When Fine-Grained Admin Permissions (FGAP) v2 is enabled, a delegated administrator can bypass access restrictions to view parent groups they are not authorized to see. By searching for a child group they have permission to view, the system incorrectly returns the full details of the parent group in the response, leading to the disclosure of sensitive group attributes and configuration.	2026-07-16	4.3
CVE-2026-50302	microsoft - multiple products	Improper certificate validation in Windows Cryptographic Services allows an unauthorized attacker to bypass a security feature over a network.	2026-07-14	4.2
CVE-2026-14902	ivanti - Xtraction	An open redirect in Ivanti Xtraction before version 2026.2.1 allows a remote unauthenticated attacker to redirect users to arbitrary external URLs.	2026-07-14	4
CVE-2026-58549	huawei - HarmonyOS	Out-of-bounds read vulnerability in the image codec module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-07-15	4
CVE-2026-58550	huawei - HarmonyOS	Out-of-bounds read vulnerability in the image codec module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-07-15	4
CVE-2026-58553	huawei - HarmonyOS	Out-of-bounds read vulnerability in the image codec module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-07-15	4
CVE-2026-48001	adobe - multiple products	Adobe Commerce is affected by an Information Exposure vulnerability that could lead to a limited disclosure of sensitive information. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue does not require user interaction.	2026-07-14	3.7
CVE-2025-62675	fortinet - multiple products	An Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') vulnerability [CWE-113] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4 all versions, FortiOS 7.2 all versions, FortiProxy 7.6.0 through 7.6.4, FortiProxy 7.4 all versions, FortiProxy 7.2 all versions may allow an attacker in possession of a valid web filter override token to inject arbitrary headers via tricking a user into clicking on a crafted link.	2026-07-14	3.4
CVE-2026-50416	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Win32K allows an authorized attacker to disclose information locally.	2026-07-14	3.3
CVE-2026-50419	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Kernel allows an authorized attacker to disclose information locally.	2026-07-14	3.3
CVE-2025-62826	fortinet - multiple products	An Improper Neutralization of CRLF Sequences in HTTP Headers ('HTTP Response Splitting') vulnerability [CWE-113] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4 all versions, FortiOS 7.2 all versions, FortiProxy 7.6.0 through 7.6.4, FortiProxy 7.4 all versions, FortiProxy 7.2 all versions may allow an attacker able to intercept and modify a user's captive portal authentication request to inject arbitrary headers via crafted HTTP requests.	2026-07-14	3.1
CVE-2026-48329	adobe - multiple products	ColdFusion is affected by an Insufficient Session Expiration 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 does not require user interaction.	2026-07-14	2.7
CVE-2026-15520	gnu - LibreDWG	A vulnerability was determined in GNU LibreDWG 0.13.4-154-g0b573035. This impacts the function decompress_R2004_section of the file src/decode.c of the component R2004 Section Decompression. Executing a manipulation can lead to heap-based buffer overflow. The attack requires local access. The exploit has been publicly disclosed and may be utilized. Upgrading to version 0.14.8396 will fix this issue. This patch is called 3d0f9fc2eddbd6579c99af3111c37c98f03475d0. You should upgrade the affected component.	2026-07-13	1.9

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.