الهيئـــة الوطنيـــة
للأمـــن السيبـــراني
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 أبريل إلى 18 أبريل. 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 April to 18th of April. 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-2026-34865	huawei - harmonyos	Out-of-bounds write vulnerability in the WEB module.Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	2026-04-13	10
CVE-2026-20147	cisco - multiple products	A vulnerability in Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have valid administrative credentials._x000D_ _x000D_ This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. In single-node ISE deployments, successful exploitation of this vulnerability could cause the affected ISE node to become unavailable, resulting in a denial of service (DoS) condition. In that condition, endpoints that have not already authenticated would be unable to access the network until the node is restored.	2026-04-15	9.9
CVE-2026-20180	cisco - Cisco Identity Services Engine Software	A vulnerability in Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have at least Read Only Admin credentials._x000D_ _x000D_ This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. In single-node ISE deployments, successful exploitation of these vulnerabilities could cause the affected ISE node to become unavailable, resulting in a denial of service (DoS) condition. In that condition, endpoints that have not already authenticated would be unable to access the network until the node is restored.	2026-04-15	9.9
CVE-2026-20186	cisco - Cisco Identity Services Engine Software	A vulnerability in Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker to execute arbitrary commands on the underlying operating system of an affected device. To exploit this vulnerability, the attacker must have at least Read Only Admin credentials._x000D_ _x000D_ This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to obtain user-level access to the underlying operating system and then elevate privileges to root. In single-node ISE deployments, successful exploitation of these vulnerabilities could cause the affected ISE node to become unavailable, resulting in a denial of service (DoS) condition. In that condition, endpoints that have not already authenticated would be unable to access the network until the node is restored.	2026-04-15	9.9
CVE-2026-31414	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_expect: use expect->helper Use expect->helper in ctnetlink and /proc to dump the helper name. Using nfct_help() without holding a reference to the master conntrack is unsafe. Use exp->master->helper in ctnetlink path if userspace does not provide an explicit helper when creating an expectation to retain the existing behaviour. The ctnetlink expectation path holds the reference on the	2026-04-13	9.8

		master conntrack and nf_conntrack_expect lock and the nfnetlink glue path refers to the master ct that is attached to the skb.		
CVE-2026-39808	fortinet - fortisandbox	A improper neutralization of special elements used in an os command ('os command injection') vulnerability in Fortinet FortiSandbox 4.4.0 through 4.4.8 may allow attacker to execute unauthorized code or commands via <insert attack vector here>	2026-04-14	9.8
CVE-2026-39813	fortinet - multiple products	A path traversal: '../filedir' vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.5, FortiSandbox 4.4.0 through 4.4.8 may allow attacker to escalation of privilege via <insert attack vector here>	2026-04-14	9.8
CVE-2026-33824	microsoft - multiple products	Double free in Windows IKE Extension allows an unauthorized attacker to execute code over a network.	2026-04-14	9.8
CVE-2026-20184	cisco - Cisco Webex Meetings	A vulnerability in the integration of single sign-on (SSO) with Control Hub in Cisco Webex Services could have allowed an unauthenticated, remote attacker to impersonate any user within the service._x000D_ _x000D_ This vulnerability existed because of improper certificate validation. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by connecting to a service endpoint and supplying a crafted token. A successful exploit could have allowed the attacker to gain unauthorized access to legitimate Cisco Webex services.	2026-04-15	9.8
CVE-2026-27303	adobe - connect	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. 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.	2026-04-14	9.6
CVE-2026-6296	google - chrome	Heap buffer overflow in ANGLE in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-04-15	9.6
CVE-2026-27243	adobe - connect	Adobe Connect versions 2025.3, 12.10 and earlier are 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 visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	2026-04-14	9.3
CVE-2026-27245	adobe - connect	Adobe Connect versions 2025.3, 12.10 and earlier are 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 visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	2026-04-14	9.3
CVE-2026-27246	adobe - connect	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a DOM-based 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 visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	2026-04-14	9.3
CVE-2026-34615	adobe - connect	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a Deserialization of Untrusted Data vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to 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.	2026-04-14	9.3
CVE-2026-27304	adobe - multiple products	ColdFusion versions 2023.18, 2025.6 and earlier are 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.	2026-04-14	9.3
CVE-2026-31908	apache - apisix	Header injection vulnerability in Apache APISIX. The attacker can take advantage of certain configuration in forward-auth plugin to inject malicious headers. This issue affects Apache APISIX: from 2.12.0 through 3.15.0. Users are recommended to upgrade to version 3.16.0, which fixes the issue.	2026-04-14	9.1
CVE-2025-41118	grafana - multiple products	Pyroscope is an open-source continuous profiling database. The database supports various storage backends, including Tencent Cloud Object Storage (COS). If the database is configured to use Tencent COS as the storage backend, an attacker could extract the secret_key configuration value from the Pyroscope API. To exploit this vulnerability, an attacker needs direct access to the Pyroscope API. We highly recommend limiting the public internet exposure of all our databases, such that they are only accessible by trusted users or internal systems. This vulnerability is fixed in versions: 1.15.x: 1.15.2 and above. 1.16.x: 1.16.1 and above. 1.17.x: 1.17.0 and above (i.e. all versions). Thanks to Théo Cusnir for reporting this vulnerability to us via our bug bounty program.	2026-04-15	9.1
CVE-2026-6388	red hat - Red Hat OpenShift GitOps	A flaw was found in ArgoCD Image Updater. This vulnerability allows an attacker, with permissions to create or modify an ImageUpdater resource in a multi-tenant environment, to bypass namespace boundaries. By exploiting insufficient validation, the attacker can trigger unauthorized image updates on applications managed by other tenants. This leads to cross-namespace privilege escalation, impacting application integrity through unauthorized application updates.	2026-04-15	9.1
CVE-2026-26149	microsoft - Microsoft Power	Improper neutralization of escape, meta, or control sequences in Microsoft Power Apps allows an authorized attacker to perform spoofing over a network.	2026-04-14	9

	Apps Desktop Client			
CVE-2026-35337	apache - storm	Deserialization of Untrusted Data vulnerability in Apache Storm. Versions Affected: before 2.8.6. Description: When processing topology credentials submitted via the Nimbus Thrift API, Storm deserializes the base64-encoded TGT blob using ObjectInputStream.readObject() without any class filtering or validation. An authenticated user with topology submission rights could supply a crafted serialized object in the "TGT" credential field, leading to remote code execution in both the Nimbus and Worker JVMs. Mitigation: 2.x users should upgrade to 2.8.6. Users who cannot upgrade immediately should monkey-patch an ObjectInputFilter allow-list to ClientAuthUtils.deserializeKerberosTicket() restricting deserialized classes to javax.security.auth.kerberos.KerberosTicket and its known dependencies. A guide on how to do this is available in the release notes of 2.8.6. Credit: This issue was discovered by K.	2026-04-13	8.8
CVE-2026-33858	apache - airflow	Dag Authors, who normally should not be able to execute code in the webserver context could craft XCom payload causing the webserver to execute arbitrary code. Since Dag Authors are already highly trusted, severity of this issue is Low. Users are recommended to upgrade to Apache Airflow 3.2.0, which resolves this issue.	2026-04-13	8.8
CVE-2026-39815	fortinet - fortiddos-f	A improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiDDoS-F 7.2.1 through 7.2.2 may allow attacker to execute unauthorized code or commands via sending crafted HTTP requests	2026-04-14	8.8
CVE-2026-26167	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.	2026-04-14	8.8
CVE-2026-26178	microsoft - multiple products	Integer size truncation in Windows Advanced Rasterization Platform (WARP) allows an unauthorized attacker to elevate privileges locally.	2026-04-14	8.8
CVE-2026-32157	microsoft - multiple products	Use after free in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-04-14	8.8
CVE-2026-32171	microsoft - azure_logic_apps	Insufficiently protected credentials in Azure Logic Apps allows an authorized attacker to elevate privileges over a network.	2026-04-14	8.8
CVE-2026-32225	microsoft - multiple products	Protection mechanism failure in Windows Shell allows an unauthorized attacker to bypass a security feature over a network.	2026-04-14	8.8
CVE-2026-33120	microsoft - Microsoft SQL Server 2022 (GDR)	Untrusted pointer dereference in SQL Server allows an authorized attacker to execute code over a network.	2026-04-14	8.8
CVE-2026-6299	google - chrome	Use after free in Prerender in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-04-15	8.8
CVE-2026-6300	google - chrome	Use after free in CSS in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-15	8.8
CVE-2026-6301	google - chrome	Type Confusion in Turbofan in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-15	8.8
CVE-2026-6302	google - chrome	Use after free in Video in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-15	8.8
CVE-2026-6303	google - chrome	Use after free in Codecs in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-15	8.8
CVE-2026-6305	google - chrome	Heap buffer overflow in PDFium in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: High)	2026-04-15	8.8
CVE-2026-6306	google - chrome	Heap buffer overflow in PDFium in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: High)	2026-04-15	8.8
CVE-2026-6307	google - chrome	Type Confusion in Turbofan in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-15	8.8
CVE-2026-6315	google - chrome	Use after free in Permissions in Google Chrome on Android prior to 147.0.7727.101 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2026-04-15	8.8
CVE-2026-6316	google - chrome	Use after free in Forms in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-04-15	8.8
CVE-2026-6317	google - chrome	Use after free in Cast in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2026-04-15	8.8

CVE-2026-6318	google - chrome	Use after free in Codecs in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-04-15	8.8
CVE-2026-6358	google - chrome	Use after free in XR in Google Chrome on Android prior to 147.0.7727.101 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Critical)	2026-04-15	8.8
CVE-2026-6359	google - chrome	Use after free in Video in Google Chrome on Windows prior to 147.0.7727.101 allowed a remote attacker who had compromised the renderer process to perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	2026-04-15	8.8
CVE-2026-6360	google - chrome	Use after free in FileSystem in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	2026-04-15	8.8
CVE-2026-6363	google - chrome	Type Confusion in V8 in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	2026-04-15	8.8
CVE-2026-30898	apache - airflow	An example of BashOperator in Airflow documentation suggested a way of passing dag_run.conf in the way that could cause unsanitized user input to be used to escalate privileges of UI user to allow execute code on worker. Users should review if any of their own DAGs have adopted this incorrect advice.	2026-04-18	8.8
CVE-2026-25654	siemens - SINEC NMS	A vulnerability has been identified in SINEC NMS (All versions < V4.0 SP3). Affected products do not properly validate user authorization when processing password reset requests. This could allow an authenticated remote attacker to bypass authorization checks, leading to the ability to reset the password of any arbitrary user account.	2026-04-14	8.7
CVE-2026-27668	siemens - RUGGEDCOM CROSSBOW Secure Access Manager Primary (SAM-P)	A vulnerability has been identified in RUGGEDCOM CROSSBOW Secure Access Manager Primary (SAM-P) (All versions < V5.8). User Administrators are allowed to administer groups they belong to. This could allow an authenticated User Administrator to escalate their own privileges and grant themselves access to any device group at any access level.	2026-04-14	8.7
CVE-2026-27928	microsoft - multiple products	Improper input validation in Windows Hello allows an unauthorized attacker to bypass a security feature over a network.	2026-04-14	8.7
CVE-2026-34617	adobe - connect	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a Cross-Site Scripting (XSS) vulnerability that could result in privilege escalation. A low-privileged 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.	2026-04-14	8.7
CVE-2026-34622	adobe - multiple products	Acrobat Reader versions 26.001.21411, 24.001.30360, 24.001.30362 and earlier are affected by an Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') 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.	2026-04-14	8.6
CVE-2026-27305	adobe - multiple products	ColdFusion versions 2023.18, 2025.6 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue does not require user interaction.	2026-04-14	8.6
CVE-2026-27290	adobe - framemaker	Adobe Framemaker versions 2022.8 and earlier are affected by an Untrusted Search Path vulnerability that might allow attackers to execute arbitrary code in the context of the current user. If the application uses a search path to locate critical resources such as programs, then an attacker could modify that search path to point to a malicious program, which the targeted application would then execute. Exploitation of this issue does not require user interaction.	2026-04-14	8.6
CVE-2026-4145	lenovo - Software Fix	During an internal security assessment, a potential vulnerability was discovered in Lenovo Software Fix that could allow a local authenticated user to perform arbitrary code execution with elevated privileges.	2026-04-15	8.5
CVE-2026-32091	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Microsoft Brokering File System allows an unauthorized attacker to elevate privileges locally.	2026-04-14	8.4
CVE-2026-32162	microsoft - multiple products	Acceptance of extraneous untrusted data with trusted data in Windows COM allows an unauthorized attacker to elevate privileges locally.	2026-04-14	8.4
CVE-2026-32190	microsoft - multiple products	Use after free in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-04-14	8.4
CVE-2026-32221	microsoft - multiple products	Heap-based buffer overflow in Microsoft Graphics Component allows an unauthorized attacker to execute code locally.	2026-04-14	8.4
CVE-2026-33114	microsoft - multiple products	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-04-14	8.4
CVE-2026-33115	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-04-14	8.4
CVE-2026-27306	adobe - multiple products	ColdFusion versions 2023.18, 2025.6 and earlier are affected by an Improper Input Validation vulnerability that could result in arbitrary code execution in the context of the current user. Attacker requires elevated privileges. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	8.4
CVE-2026-23853	dell - PowerProtect Data Domain	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a use of weak credentials vulnerability. An unauthenticated attacker with local access could potentially exploit this vulnerability, leading to unauthorized access to the system.	2026-04-17	8.4
CVE-2026-6297	google - chrome	Use after free in Proxy in Google Chrome prior to 147.0.7727.101 allowed an attacker in a privileged network position to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-04-15	8.3
CVE-2026-6304	google - chrome	Use after free in Graphite in Google Chrome prior to 147.0.7727.101 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)	2026-04-15	8.3

CVE-2026-6309	google - chrome	Use after free in Viz in Google Chrome prior to 147.0.7727.101 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)	2026-04-15	8.3
CVE-2026-6310	google - chrome	Use after free in Dawn in Google Chrome prior to 147.0.7727.101 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)	2026-04-15	8.3
CVE-2026-6311	google - chrome	Uninitialized Use in Accessibility in Google Chrome on Windows prior to 147.0.7727.101 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)	2026-04-15	8.3
CVE-2026-6314	google - chrome	Out of bounds write in GPU in Google Chrome prior to 147.0.7727.101 allowed a remote attacker who had compromised the GPU process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-04-15	8.3
CVE-2026-34632	adobe - Adobe Photoshop Installer	Adobe Photoshop Installer was affected by an Uncontrolled Search Path Element vulnerability that could have resulted in arbitrary code execution in the context of the current user. A low-privileged local attacker could have exploited this vulnerability by manipulating the search path used by the application to locate critical resources, potentially causing unauthorized code execution. Exploitation of this issue required user interaction in that a user had to be running the installer.	2026-04-15	8.2
CVE-2026-3324	zohocorp - ManageEngine Log360	Zohocorp ManageEngine Log360 versions 13000 through 13013 are vulnerable to authentication bypass on certain actions due to improper filter configuration.	2026-04-16	8.2
CVE-2026-22828	fortinet - multiple products	A heap-based buffer overflow vulnerability in Fortinet FortiAnalyzer Cloud 7.6.2 through 7.6.4, FortiManager Cloud 7.6.2 through 7.6.4 may allow a remote unauthenticated attacker to execute arbitrary code or commands via specifically crafted requests. Successful exploitation would require a large amount of effort in preparation because of ASLR and network segmentation	2026-04-14	8.1
CVE-2026-33827	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 a network.	2026-04-14	8.1
CVE-2025-54550	apache - airflow	The example example_xcom that was included in airflow documentation implemented unsafe pattern of reading value from xcom in the way that could be exploited to allow UI user who had access to modify XComs to perform arbitrary execution of code on the worker. Since the UI users are already highly trusted, this is a Low severity vulnerability. It does not affect Airflow release - example_dags are not supposed to be enabled in production environment, however users following the example could replicate the bad pattern. Documentation of Airflow 3.2.0 contains version of the example with improved resiliance for that case. Users who followed that pattern are advised to adjust their implementations accordingly.	2026-04-15	8.1
CVE-2026-5785	zohocorp - multiple products	Zohocorp ManageEngine PAM360 versions before 8531 and ManageEngine Password Manager Pro versions from 8600 to 13230 are vulnerable to Authenticated SQL injection in the query report module.	2026-04-16	8.1
CVE-2026-27912	microsoft - multiple products	Improper authorization in Windows Kerberos allows an authorized attacker to elevate privileges over an adjacent network.	2026-04-14	8
CVE-2026-33826	microsoft - multiple products	Improper input validation in Windows Active Directory allows an authorized attacker to execute code over an adjacent network.	2026-04-14	8
CVE-2026-31413	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: bpf: Fix unsound scalar forking in maybe_fork_scalars() for BPF_OR maybe_fork_scalars() is called for both BPF_AND and BPF_OR when the source operand is a constant. When dst has signed range [-1, 0], it forks the verifier state: the pushed path gets dst = 0, the current path gets dst = -1. For BPF_AND this is correct: 0 & K == 0. For BPF_OR this is wrong: 0 | K == K, not 0. The pushed path therefore tracks dst as 0 when the runtime value is K, producing an exploitable verifier/runtime divergence that allows out-of-bounds map access. Fix this by passing env->insn_idx (instead of env->insn_idx + 1) to push_stack(), so the pushed path re-executes the ALU instruction with dst = 0 and naturally computes the correct result for any opcode.	2026-04-12	7.8
CVE-2026-31419	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: bonding: fix use-after-free in bond_xmit_broadcast() bond_xmit_broadcast() reuses the original skb for the last slave (determined by bond_is_last_slave()) and clones it for others. Concurrent slave enslave/release can mutate the slave list during RCU-protected iteration, changing which slave is "last" mid-loop. This causes the original skb to be double-consumed (double-freed). Replace the racy bond_is_last_slave() check with a simple index comparison (i + 1 == slaves_count) against the pre-snapshot slave count taken via READ_ONCE() before the loop. This preserves the	2026-04-13	7.8

		zero-copy optimization for the last slave while making the "last" determination stable against concurrent list mutations. The UAF can trigger the following crash: ========== BUG: KASAN: slab-use-after-free in skb_clone Read of size 8 at addr ffff888100ef8d40 by task exploit/147 CPU: 1 UID: 0 PID: 147 Comm: exploit Not tainted 7.0.0-rc3+ #4 PREEMPTLAZY Call Trace: <TASK> dump_stack_lvl (lib/dump_stack.c:123) print_report (mm/kasan/report.c:379 mm/kasan/report.c:482) kasan_report (mm/kasan/report.c:597) skb_clone (include/linux/skbuff.h:1724 include/linux/skbuff.h:1792 include/linux/skbuff.h:3396 net/core/skbuff.c:2108) bond_xmit_broadcast (drivers/net/bonding/bond_main.c:5334) bond_start_xmit (drivers/net/bonding/bond_main.c:5567 drivers/net/bonding/bond_main.c:5593) dev_hard_start_xmit (include/linux/netdevice.h:5325 include/linux/netdevice.h:5334 net/core/dev.c:3871 net/core/dev.c:3887) __dev_queue_xmit (include/linux/netdevice.h:3601 net/core/dev.c:4838) ip6_finish_output2 (include/net/neighbour.h:540 include/net/neighbour.h:554 net/ipv6/ip6_output.c:136) ip6_finish_output (net/ipv6/ip6_output.c:208 net/ipv6/ip6_output.c:219) ip6_output (net/ipv6/ip6_output.c:250) ip6_send_skb (net/ipv6/ip6_output.c:1985) udp_v6_send_skb (net/ipv6/udp.c:1442) udpv6_sendmsg (net/ipv6/udp.c:1733) __sys_sendto (net/socket.c:730 net/socket.c:742 net/socket.c:2206) __x64_sys_sendto (net/socket.c:2209) do_syscall_64 (arch/x86/entry/syscall_64.c:63 arch/x86/entry/syscall_64.c:94) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) </TASK> Allocated by task 147: Freed by task 147: The buggy address belongs to the object at ffff888100ef8c80 which belongs to the cache skbuff_head_cache of size 224 The buggy address is located 192 bytes inside of freed 224-byte region [ffff888100ef8c80, ffff888100ef8d60) Memory state around the buggy address: ffff888100ef8c00: fb fb fb fb fc fc fc fc fc fc fc fc fc fc fc fc ffff888100ef8c80: fa fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb >ffff888100ef8d00: fb fb fb fb fb fb fb fb fb fb fb fb fc fc fc fc ^ ffff888100ef8d80: fc fc fc fc fc fc fc fc fa fb fb fb fb fb fb fb ffff888100ef8e00: fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb fb ==========		
CVE-2026-27238	adobe - multiple products	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-27283	adobe - multiple products	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-27284	adobe - multiple products	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-27291	adobe - multiple products	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-20930	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Management Services allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-23657	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-04-14	7.8
CVE-2026-26143	microsoft - multiple products	Improper input validation in Microsoft PowerShell allows an unauthorized attacker to bypass a security feature locally.	2026-04-14	7.8
CVE-2026-26153	microsoft - multiple products	Out-of-bounds read in Windows Encrypting File System (EFS) allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-26156	microsoft - multiple products	Heap-based buffer overflow in Windows Hyper-V allows an unauthorized attacker to execute code locally.	2026-04-14	7.8
CVE-2026-26159	microsoft - multiple products	Missing authentication for critical function in Windows Remote Desktop Licensing Service allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8

CVE-2026-26160	microsoft - multiple products	Missing authentication for critical function in Windows Remote Desktop Licensing Service allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-26161	microsoft - multiple products	Untrusted pointer dereference in Windows Sensor Data Service allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-26162	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows OLE allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-26163	microsoft - multiple products	Double free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-26168	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-26170	microsoft - multiple products	Improper input validation in Microsoft PowerShell allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-26172	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.	2026-04-14	7.8
CVE-2026-26176	microsoft - multiple products	Heap-based buffer overflow in Windows Client Side Caching driver (csc.sys) allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-26179	microsoft - multiple products	Double free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-26180	microsoft - multiple products	Heap-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-26181	microsoft - multiple products	Use after free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-26183	microsoft - multiple products	Improper access control in Windows RPC API allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-26184	microsoft - multiple products	Buffer over-read in Windows Projected File System allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-27907	microsoft - multiple products	Integer underflow (wrap or wraparound) in Windows Storage Spaces Controller allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-27909	microsoft - multiple products	Use after free in Microsoft Windows Search Component allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-27910	microsoft - multiple products	Improper handling of insufficient permissions or privileges in Windows Installer allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-27911	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows User Interface Core allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-27914	microsoft - multiple products	Improper access control in Microsoft Management Console allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-27915	microsoft - multiple products	Use after free in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-27916	microsoft - multiple products	Use after free in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-27918	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Shell allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-27919	microsoft - multiple products	Untrusted pointer dereference in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-27920	microsoft - multiple products	Untrusted pointer dereference in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-27923	microsoft - multiple products	Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-27924	microsoft - multiple products	Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-27927	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Projected File System allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32069	microsoft - multiple products	Double free in Windows Projected File System allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32074	microsoft - multiple products	Double free in Windows Projected File System allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32076	microsoft - multiple products	Out-of-bounds read in Windows Storage Spaces Controller allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32077	microsoft - multiple products	Untrusted pointer dereference in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32078	microsoft - multiple products	Use after free in Windows Projected File System allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32089	microsoft - multiple products	Use after free in Windows Speech Brokered Api allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32090	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Speech Brokered Api allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32152	microsoft - multiple products	Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32153	microsoft - multiple products	Use after free in Microsoft Windows Speech allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32154	microsoft - multiple products	Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32155	microsoft - multiple products	Use after free in Desktop Window Manager allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32158	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.	2026-04-14	7.8

CVE-2026-32159	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.	2026-04-14	7.8
CVE-2026-32160	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.	2026-04-14	7.8
CVE-2026-32163	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows User Interface Core allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32164	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows User Interface Core allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32165	microsoft - multiple products	Use after free in Windows User Interface Core allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32168	microsoft - Azure Monitor	Improper input validation in Azure Monitor Agent allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32183	microsoft - multiple products	Improper neutralization of special elements used in a command ('command injection') in Windows Snipping Tool allows an unauthorized attacker to execute code locally.	2026-04-14	7.8
CVE-2026-32184	microsoft - Microsoft HPC Pack 2019	Deserialization of untrusted data in Microsoft High Performance Compute Pack (HPC) allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32189	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-04-14	7.8
CVE-2026-32192	microsoft - Azure Monitor	Deserialization of untrusted data in Azure Monitor Agent allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-32197	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-04-14	7.8
CVE-2026-32198	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-04-14	7.8
CVE-2026-32199	microsoft - multiple products	Use after free in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-04-14	7.8
CVE-2026-32200	microsoft - multiple products	Use after free in Microsoft Office PowerPoint allows an unauthorized attacker to execute code locally.	2026-04-14	7.8
CVE-2026-32222	microsoft - multiple products	Untrusted pointer dereference in Windows Win32K - ICOMP allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-33095	microsoft - multiple products	Use after free in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-04-14	7.8
CVE-2026-33098	microsoft - multiple products	Use after free in Windows Container Isolation FS Filter Driver allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-33101	microsoft - multiple products	Use after free in Windows Print Spooler Components allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-33825	microsoft - defender_antimalware_platform	Insufficient granularity of access control in Microsoft Defender allows an authorized attacker to elevate privileges locally.	2026-04-14	7.8
CVE-2026-34627	adobe - multiple products	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-34628	adobe - multiple products	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-34629	adobe - multiple products	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-27289	adobe - photoshop	Photoshop Desktop versions 27.4 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-27310	adobe - multiple products	Bridge versions 16.0.2, 15.1.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-27311	adobe - multiple products	Bridge versions 16.0.2, 15.1.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-27312	adobe - multiple products	Bridge versions 16.0.2, 15.1.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-27313	adobe - multiple products	Bridge versions 16.0.2, 15.1.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-34618	adobe - multiple products	Illustrator versions 30.2, 29.8.5 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-34630	adobe - multiple products	Bridge versions 16.0.2, 15.1.4 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-27287	adobe - multiple products	InCopy versions 20.5.2, 21.2 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-34631	adobe - multiple products	InCopy versions 20.5.2, 21.2 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8

CVE-2026-27292	adobe - framemaker	Adobe Framemaker versions 2022.8 and earlier are affected by a Use After Free vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-27293	adobe - framemaker	Adobe Framemaker versions 2022.8 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-27294	adobe - framemaker	Adobe Framemaker versions 2022.8 and earlier are affected by an out-of-bounds read vulnerability when parsing a crafted file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-27295	adobe - framemaker	Adobe Framemaker versions 2022.8 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	7.8
CVE-2026-27296	adobe - framemaker	Adobe Framemaker versions 2022.8 and earlier are affected by an Integer Underflow (Wrap 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.	2026-04-14	7.8
CVE-2026-27297	adobe - framemaker	Adobe Framemaker versions 2022.8 and earlier are affected by an Integer Underflow (Wrap 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.	2026-04-14	7.8
CVE-2026-27298	adobe - framemaker	Adobe Framemaker versions 2022.8 and earlier are affected by an Access of Resource Using Incompatible Type ('Type Confusion') 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.	2026-04-14	7.8
CVE-2025-36568	dell - multiple products	Dell PowerProtect Data Domain BoostFS for client of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain an insufficiently protected credentials vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to credential exposure. The attacker may be able to use the exposed credentials to access the system with privileges of the compromised account.	2026-04-17	7.8
CVE-2026-34853	huawei - multiple products	Permission bypass vulnerability in the LBS module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-04-13	7.7
CVE-2026-27913	microsoft - multiple products	Improper input validation in Windows BitLocker allows an unauthorized attacker to bypass a security feature locally.	2026-04-14	7.7
CVE-2026-34619	adobe - multiple products	ColdFusion versions 2023.18, 2025.6 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to access unauthorized files or directories outside the intended restrictions. Exploitation of this issue does not require user interaction.	2026-04-14	7.7
CVE-2026-23775	dell - multiple products	Dell PowerProtect Data Domain appliances with Data Domain Operating System (DD OS) of Feature Release versions 8.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.10 contain an insertion of sensitive information into log file vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to credential exposures. Authentication attempts as the compromised user would need to be authorized by a high privileged DD user. This vulnerability only affects systems with retention lock enabled.	2026-04-17	7.6
CVE-2026-31417	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net/x25: Fix overflow when accumulating packets Add a check to ensure that `x25_sock.fraglen` does not overflow. The `fraglen` also needs to be resetted when purging `fragment_queue` in `x25_clear_queues()`.	2026-04-13	7.5
CVE-2025-66236	apache - airflow	Before Airflow 3.2.0, it was unclear that secure Airflow deployments require the Deployment Manager to take appropriate actions and pay attention to security details and security model of Airflow. Some assumptions the Deployment Manager could make were not clear or explicit enough, even though Airflow's intentions and security model of Airflow did not suggest different assumptions. The overall security model [1], workload isolation [2], and JWT authentication details [3] are now described in more detail. Users concerned with role isolation and following the Airflow security model of Airflow are advised to upgrade to Airflow 3.2, where several security improvements have been implemented. They should also read and follow the relevant documents to make sure that their deployment is secure enough. It also clarifies that the Deployment Manager is ultimately responsible for securing your Airflow deployment. This had also been communicated via Airflow 3.2.0 Blog announcement [4]. [1] Security Model: https://airflow.apache.org/docs/apache-airflow/stable/security/jwt_token_authentication.html [2] Workload isolation: https://airflow.apache.org/docs/apache-airflow/stable/security/workload.html [3] JWT Token authentication: https://airflow.apache.org/docs/apache-airflow/stable/security/jwt_token_authentication.html [4] Airflow 3.2.0 Blog announcement: https://airflow.apache.org/blog/airflow-3.2.0/ Users are recommended to upgrade to version 3.2.0, which fixes this issue.	2026-04-13	7.5
CVE-2026-31923	apache - apisix	Cleartext Transmission of Sensitive Information vulnerability in Apache APISIX. This can occur due to `ssl_verify` in openid-connect plugin configuration being set to false by default.	2026-04-14	7.5

		This issue affects Apache APISIX: from 0.7 through 3.15.0. Users are recommended to upgrade to version 3.16.0, which fixes the issue.		
CVE-2026-23708	fortinet - multiple products	A improper authentication vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR on-premise 7.6.0 through 7.6.3, FortiSOAR on-premise 7.5.0 through 7.5.2 may allow an unauthenticated attacker to bypass authentication via replaying captured 2FA request. The attack requires being able to intercept and decrypt authentication traffic and precise timing to replay the request before token expiration, which raises the attack complexity.	2026-04-14	7.5
CVE-2026-23666	microsoft - multiple products	Improper input validation in .NET Framework allows an unauthorized attacker to deny service over a network.	2026-04-14	7.5
CVE-2026-26154	microsoft - multiple products	Improper input validation in Windows Server Update Service allows an unauthorized attacker to perform tampering over a network.	2026-04-14	7.5
CVE-2026-26171	microsoft - multiple products	Uncontrolled resource consumption in .NET allows an unauthorized attacker to deny service over a network.	2026-04-14	7.5
CVE-2026-32071	microsoft - multiple products	Null pointer dereference in Windows Local Security Authority Subsystem Service (LSASS) allows an unauthorized attacker to deny service over a network.	2026-04-14	7.5
CVE-2026-32178	microsoft - multiple products	Improper neutralization of special elements in .NET allows an unauthorized attacker to perform spoofing over a network.	2026-04-14	7.5
CVE-2026-32203	microsoft - multiple products	Stack-based buffer overflow in .NET and Visual Studio allows an unauthorized attacker to deny service over a network.	2026-04-14	7.5
CVE-2026-33096	microsoft - multiple products	Out-of-bounds read in Windows HTTP.sys allows an unauthorized attacker to deny service over a network.	2026-04-14	7.5
CVE-2026-33116	microsoft - multiple products	Loop with unreachable exit condition ('infinite loop') in .NET, .NET Framework, Visual Studio allows an unauthorized attacker to deny service over a network.	2026-04-14	7.5
CVE-2026-27282	adobe - multiple products	ColdFusion versions 2023.18, 2025.6 and earlier are 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 access. Exploitation of this issue requires user interaction.	2026-04-14	7.5
CVE-2026-30778	apache - skywalking	The SkyWalking OAP /debugging/config/dump endpoint may leak sensitive configuration information of MySQL/PostgreSQL. This issue affects Apache SkyWalking: from 9.7.0 through 10.3.0. Users are recommended to upgrade to version 10.4.0, which fixes the issue.	2026-04-15	7.5
CVE-2026-6308	google - chrome	Out of bounds read in Media in Google Chrome prior to 147.0.7727.101 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2026-04-15	7.5
CVE-2026-6319	google - chrome	Use after free in Payments in Google Chrome on Android prior to 147.0.7727.101 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: Medium)	2026-04-15	7.5
CVE-2024-2374	wso2 - multiple products	The XML parsers within multiple WSO2 products accept user-supplied XML data without properly configuring to prevent the resolution of external entities. This omission allows malicious actors to craft XML payloads that exploit the parser's behavior, leading to the inclusion of external resources. By leveraging this vulnerability, an attacker can read confidential files from the file system and access limited HTTP resources reachable by the product. Additionally, the vulnerability can be exploited to perform denial of service attacks by exhausting server resources through recursive entity expansion or fetching large external resources.	2026-04-16	7.5
CVE-2026-31987	apache - airflow	JWT Tokens used by tasks were exposed in logs. This could allow UI users to act as Dag Authors. Users are advised to upgrade to Airflow version that contains fix. Users are recommended to upgrade to version 3.2.0, which fixes this issue.	2026-04-16	7.5
CVE-2026-6507	red hat - multiple products	A flaw was found in dnsmasq. A remote attacker could exploit an out-of-bounds write vulnerability by sending a specially crafted BOOTREPLY (Bootstrap Protocol Reply) packet to a dnsmasq server configured with the `--dhcp-split-relay` option. This can lead to memory corruption, causing the dnsmasq daemon to crash and resulting in a denial of service (DoS).	2026-04-17	7.5
CVE-2026-30912	apache - airflow	In case of SQL errors, exception/stack trace of errors was exposed in API even if "api/expose_stack_traces" was set to false. That could lead to exposing additional information to potential attacker. Users are recommended to upgrade to Apache Airflow 3.2.0, which fixes the issue.	2026-04-18	7.5
CVE-2026-32228	apache - airflow	UI / API User with asset materialize permission could trigger dags they had no access to. Users are advised to migrate to Airflow version 3.2.0 that fixes the issue.	2026-04-18	7.5
CVE-2026-32156	microsoft - multiple products	Use after free in Windows Universal Plug and Play (UPnP) Device Host allows an unauthorized attacker to execute code locally.	2026-04-14	7.4
CVE-2026-41035	samba - rsync	In rsync 3.0.1 through 3.4.1, receive_xattr relies on an untrusted length value during a qsort call, leading to a receiver use-after-free. The victim must run rsync with -X (aka --xattrs). On Linux, many (but not all) common configurations are vulnerable. Non-Linux platforms are more widely vulnerable.	2026-04-16	7.4
CVE-2026-34856	huawei - harmonyos	UAF vulnerability in the communication module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-04-13	7.3
CVE-2026-32149	microsoft - multiple products	Improper input validation in Windows Hyper-V allows an authorized attacker to execute code locally.	2026-04-14	7.3
CVE-2026-6384	red hat - multiple products	A flaw was found in gimp. This buffer overflow vulnerability in the GIF image loading component's `ReadJeffsImage` function allows an attacker to write beyond an allocated buffer by processing a specially crafted GIF file. This can lead to a denial of service or potentially arbitrary code execution.	2026-04-15	7.3
CVE-2026-23772	dell - Storage Manager	Dell Storage Manager - Replay Manager for Microsoft Servers, version(s) 8.0, contain(s) an Improper Privilege Management vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-04-16	7.3

CVE-2025-61848	fortinet - multiple products	An improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.4, FortiAnalyzer 7.4.0 through 7.4.8, FortiAnalyzer 7.2 all versions, FortiAnalyzer 7.0 all versions, FortiAnalyzer Cloud 7.6.0 through 7.6.4, FortiAnalyzer Cloud 7.4.0 through 7.4.8, FortiAnalyzer Cloud 7.2 all versions, FortiAnalyzer Cloud 7.0 all versions, FortiManager 7.6.0 through 7.6.4, FortiManager 7.4.0 through 7.4.8, FortiManager 7.2 all versions, FortiManager 7.0 all versions, FortiManager Cloud 7.6.0 through 7.6.4, FortiManager Cloud 7.4.0 through 7.4.8, FortiManager Cloud 7.2 all versions, FortiManager Cloud 7.0 all versions may allow a privileged authenticated attacker to execute unauthorized code or commands via JSON RPC API	2026-04-14	7.2
CVE-2026-40688	fortinet - multiple products	An out-of-bounds write vulnerability [CWE-787] vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.3, FortiWeb 7.6.0 through 7.6.6, FortiWeb 7.4.0 through 7.4.11 may allow a remote privileged attacker to execute arbitrary code or command via crafted HTTP requests.	2026-04-14	7.2
CVE-2026-6361	google - chrome	Heap buffer overflow in PDFium in Google Chrome on Windows prior to 147.0.7727.101 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: High)	2026-04-15	7.2
CVE-2026-23778	dell - multiple products	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a command injection vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability to gain root-level access.	2026-04-17	7.2
CVE-2026-23776	dell - multiple products	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60, contain(s) an Improper Certificate Validation vulnerability in certificate-based login. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Elevation of privileges.	2026-04-17	7.2
CVE-2026-25917	apache - airflow	Dag Authors, who normally should not be able to execute code in the webserver context could craft XCom payload causing the webserver to execute arbitrary code. Since Dag Authors are already highly trusted, severity of this issue is Low. Users are recommended to upgrade to Apache Airflow 3.2.0, which fixes the issue.	2026-04-18	7.2
CVE-2026-34476	apache - skywalking_mcp	Server-Side Request Forgery via SW-URL Header vulnerability in Apache SkyWalking MCP. This issue affects Apache SkyWalking MCP: 0.1.0. Users are recommended to upgrade to version 0.2.0, which fixes this issue.	2026-04-13	7.1
CVE-2026-26151	microsoft - multiple products	Insufficient ui warning of dangerous operations in Windows Remote Desktop allows an unauthorized attacker to perform spoofing over a network.	2026-04-14	7.1
CVE-2026-32188	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information locally.	2026-04-14	7.1
CVE-2026-31426	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ACPI: EC: clean up handlers on probe failure in acpi_ec_setup() When ec_install_handlers() returns -EPROBE_DEFER on reduced-hardware platforms, it has already started the EC and installed the address space handler with the struct acpi_ec pointer as handler context. However, acpi_ec_setup() propagates the error without any cleanup. The caller acpi_ec_add() then frees the struct acpi_ec for non-boot instances, leaving a dangling handler context in ACPICA. Any subsequent AML evaluation that accesses an EC OpRegion field dispatches into acpi_ec_space_handler() with the freed pointer, causing a use-after-free: BUG: KASAN: slab-use-after-free in mutex_lock (kernel/locking/mutex.c:289) Write of size 8 at addr ffff88800721de38 by task init/1 Call Trace: <TASK> mutex_lock (kernel/locking/mutex.c:289) acpi_ec_space_handler (drivers/acpi/ec.c:1362) acpi_ev_address_space_dispatch (drivers/acpi/acpica/evregion.c:293) acpi_ex_access_region (drivers/acpi/acpica/exfldio.c:246) acpi_ex_field_datum_io (drivers/acpi/acpica/exfldio.c:509) acpi_ex_extract_from_field (drivers/acpi/acpica/exfldio.c:700) acpi_ex_read_data_from_field (drivers/acpi/acpica/exfield.c:327) acpi_ex_resolve_node_to_value (drivers/acpi/acpica/exresolv.c:392) </TASK> Allocated by task 1: acpi_ec_alloc (drivers/acpi/ec.c:1424) acpi_ec_add (drivers/acpi/ec.c:1692) Freed by task 1: kfree (mm/slub.c:6876) acpi_ec_add (drivers/acpi/ec.c:1751) The bug triggers on reduced-hardware EC platforms (ec->gpe < 0) when the GPIO IRQ provider defers probing. Once the stale handler exists, any unprivileged sysfs read that causes AML to touch an EC OpRegion (battery, thermal, backlight) exercises the dangling pointer.	2026-04-13	7

		Fix this by calling ec_remove_handlers() in the error path of acpi_ec_setup() before clearing first_ec. ec_remove_handlers() checks each EC_FLAGS_* bit before acting, so it is safe to call regardless of how far ec_install_handlers() progressed: -ENODEV (handler not installed): only calls acpi_ec_stop() -EPROBE_DEFER (handler installed): removes handler, stops EC		
CVE-2026-25184	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Applocker Filter Driver (applockerfltr.sys) allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-26152	microsoft - multiple products	Insecure storage of sensitive information in Windows Cryptographic Services allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-26165	microsoft - multiple products	Use after free in Windows Shell allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-26166	microsoft - multiple products	Double free in Windows Shell allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-26173	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-26174	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Server Update Service allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-26177	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-26182	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-27908	microsoft - multiple products	Use after free in Windows TDI Translation Driver (tdx.sys) allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-27917	microsoft - multiple products	Use after free in Windows WFP NDIS Lightweight Filter Driver (wfplwfs.sys) allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-27921	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows TCP/IP allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-27922	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-27926	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Cloud Files Mini Filter Driver allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-27929	microsoft - multiple products	Time-of-check time-of-use (toctou) race condition in Windows LUAFV allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32068	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SSDP Service allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32070	microsoft - multiple products	Use after free in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32073	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32075	microsoft - multiple products	Use after free in Windows Universal Plug and Play (UPnP) Device Host allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32080	microsoft - multiple products	Use after free in Windows WalletService allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32082	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SSDP Service allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32083	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows SSDP Service allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32086	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Function Discovery Service (fdwsd.dll) allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32087	microsoft - multiple products	Heap-based buffer overflow in Function Discovery Service (fdwsd.dll) allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32093	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Function Discovery Service (fdwsd.dll) allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32150	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Function Discovery Service (fdwsd.dll) allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32195	microsoft - multiple products	Stack-based buffer overflow in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32219	microsoft - multiple products	Double free in Microsoft Brokering File System allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-32224	microsoft - multiple products	Use after free in Windows Server Update Service allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-33099	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-33100	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-33104	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Win32K - GRFX allows an authorized attacker to elevate privileges locally.	2026-04-14	7
CVE-2026-4134	lenovo - Software Fix	During an internal security assessment, a potential vulnerability was discovered in Lenovo Software Fix, that during installation could allow a local authenticated user to execute code with elevated privileges.	2026-04-15	7
CVE-2026-28553	huawei - multiple products	Vulnerability of improper permission control in the theme setting module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-04-13	6.9
CVE-2026-21013	samsung - galaxy_wearable	Incorrect default permission in Galaxy Wearable prior to version 2.2.68.26 allows local attackers to access sensitive information.	2026-04-13	6.9

CVE-2026-24032	siemens - SINEC NMS	A vulnerability has been identified in SINEC NMS (All versions < V4.0 SP3 with UMC). The affected application contains an authentication weakness due to insufficient validation of user identity in the UMC component._x000D_ This could allow an unauthenticated remote attacker to bypass authentication and gain unauthorized access to the application. (ZDI-CAN-27564)	2026-04-14	6.9
CVE-2026-37980	red hat - Red Hat Build of Keycloak	A flaw was found in Keycloak, specifically in the organization selection login page. A remote attacker with `manage-realm` or `manage-organizations` administrative privileges can exploit a Stored Cross-Site Scripting (XSS) vulnerability. This flaw occurs because the `organization.alias` is placed into an inline JavaScript `onclick` handler, allowing a crafted JavaScript payload to execute in a user's browser when they view the login page. Successful exploitation enables arbitrary JavaScript execution, potentially leading to session theft, unauthorized account actions, or further attacks against users of the affected realm.	2026-04-14	6.9
CVE-2026-2399	schneider-electric - powerchute_serial_shutdown	CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause critical files overwritten with text data when a Web Admin user alters the POST /REST/upssleep request payload.	2026-04-14	6.9
CVE-2026-2402	schneider-electric - powerchute_serial_shutdown	CWE-307 Improper Restriction of Excessive Authentication Attempts vulnerability exists that would allow an attacker to gain access to the user account by performing an arbitrary number of authentication attempts with different credentials on a sequence of requests to multiple endpoints.	2026-04-14	6.9
CVE-2026-2404	schneider-electric - powerchute_serial_shutdown	CWE-116 Improper Encoding or Escaping of Output vulnerability exists that could cause log injection and forged log when an attacker alters the POST /j_security check request payload.	2026-04-14	6.9
CVE-2026-0827	lenovo - multiple products	During an internal security assessment, a potential vulnerability was discovered in Lenovo Diagnostics and the HardwareScanAddin used in Lenovo Vantage that, during installation or when using hardware scan, could allow a local authenticated user to perform an arbitrary file write with elevated privileges.	2026-04-15	6.9
CVE-2026-34864	huawei - harmonyos	Boundary-unlimited vulnerability in the application read module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-04-13	6.8
CVE-2026-21012	samsung - multiple products	External control of file name in AODManager prior to SMR Apr-2026 Release 1 allows privileged local attacker to create file with system privilege.	2026-04-13	6.8
CVE-2026-32223	microsoft - multiple products	Heap-based buffer overflow in Windows USB Print Driver allows an unauthorized attacker to elevate privileges with a physical attack.	2026-04-14	6.8
CVE-2026-34863	huawei - multiple products	Out-of-bounds write vulnerability in the file system. Impact: Successful exploitation of this vulnerability may affect availability.	2026-04-13	6.7
CVE-2026-25691	fortinet - multiple products	A improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.5, FortiSandbox 4.4.0 through 4.4.8, FortiSandbox 4.2 all versions, FortiSandbox Cloud 5.0.4, FortiSandbox PaaS 5.0.4 may allow a privileged attacker with super-admin profile and CLI access to delete an arbitrary directory via HTTP crafted requests.	2026-04-14	6.7
CVE-2026-39809	fortinet - multiple products	A improper neutralization of special elements used in an sql command ('sql injection') vulnerability in Fortinet FortiClientEMS 7.4.0 through 7.4.5, FortiClientEMS 7.2.0 through 7.2.12, FortiClientEMS 7.0 all versions may allow attacker to execute unauthorized code or commands via sending crafted requests	2026-04-14	6.7
CVE-2026-39814	fortinet - multiple products	A relative path traversal vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.2, FortiWeb 7.6.0 through 7.6.6, FortiWeb 7.4.1 through 7.4.12, FortiWeb 7.2.7 through 7.2.12, FortiWeb 7.0.10 through 7.0.12 may allow attacker to execute unauthorized code or commands via <insert attack vector here>	2026-04-14	6.7
CVE-2026-0390	microsoft - multiple products	Reliance on untrusted inputs in a security decision in Windows Boot Loader allows an authorized attacker to bypass a security feature locally.	2026-04-14	6.7
CVE-2026-32167	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.	2026-04-14	6.7
CVE-2026-32176	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.	2026-04-14	6.7
CVE-2026-23779	dell - multiple products	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a command injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability to gain root-level access.	2026-04-17	6.7
CVE-2026-35072	dell - PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of special elements used in an OS command ('OS command injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	2026-04-17	6.7
CVE-2026-35073	dell - PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of special elements used in an OS command injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	2026-04-17	6.7
CVE-2026-35074	dell - PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of special elements used in an OS Command Injection vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	2026-04-17	6.7
CVE-2026-35153	dell - PowerProtect Data Domain	Dell PowerProtect Data Domain, versions 7.7.1.0 through 8.7.0.0, LTS2025 release versions 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.60 contain an improper neutralization of argument delimiters in a command ('argument injection') vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to arbitrary command execution with root privileges.	2026-04-17	6.7

CVE-2026-21709	veeam - multiple products	A vulnerability allowing a local attacker with administrator privileges to bypass Windows Driver Signature Enforcement.	2026-04-17	6.7
CVE-2026-21010	samsung - multiple products	Improper input validation in Retail Mode prior to SMR Apr-2026 Release 1 allows local attackers to trigger privileged functions.	2026-04-13	6.6
CVE-2025-43937	dell - multiple products	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an insertion of sensitive information into log file vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to the disclosure of certain user credentials. The attacker may be able to use the exposed credentials to access the vulnerable application with privileges of the compromised account.	2026-04-16	6.6
CVE-2025-46607	dell - PowerProtect Data Domain	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper authentication vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	2026-04-17	6.6
CVE-2025-46641	dell - PowerProtect Data Domain	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper authentication vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	2026-04-17	6.6
CVE-2025-53847	fortinet - multiple products	A missing authentication for critical function vulnerability in Fortinet FortiOS 7.6.0 through 7.6.3, FortiOS 7.4.0 through 7.4.8, FortiOS 7.2.0 through 7.2.11, FortiOS 7.0.0 through 7.0.17, FortiOS 6.4 all versions, FortiOS 6.2.9 through 6.2.17 allows attacker to execute unauthorized code or commands via specially crafted packets.	2026-04-14	6.5
CVE-2026-22155	fortinet - multiple products	A cleartext transmission of sensitive information vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.2, FortiSOAR on-premise 7.5.0 through 7.5.1, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow attacker to information disclosure via <insert attack vector here>	2026-04-14	6.5
CVE-2026-22573	fortinet - multiple products	An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5 all versions, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.3, FortiSOAR on-premise 7.5 all versions, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated remote attacker to perform path traversal attack via File Content Extraction actions.	2026-04-14	6.5
CVE-2026-26155	microsoft - multiple products	Microsoft Local Security Authority Subsystem Service Information Disclosure Vulnerability	2026-04-14	6.5
CVE-2026-27925	microsoft - multiple products	Use after free in Windows Universal Plug and Play (UPnP) Device Host allows an unauthorized attacker to disclose information over an adjacent network.	2026-04-14	6.5
CVE-2026-32151	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Shell allows an authorized attacker to disclose information over a network.	2026-04-14	6.5
CVE-2026-32201	microsoft - multiple products	Improper input validation in Microsoft Office SharePoint allows an unauthorized attacker to perform spoofing over a network.	2026-04-14	6.5
CVE-2026-25219	apache - airflow	The `access_key` and `connection_string` connection properties were not marked as sensitive names in secrets masker. This means that user with read permission could see the values in Connection UI, as well as when Connection was accidentaly logged to logs, those values could be seen in the logs. Azure Service Bus used those properties to store sensitive values. Possibly other providers could be also affected if they used the same fields to store sensitive data. If you used Azure Service Bus connection with those values set or if you have other connections with those values storing sensitve values, you should upgrade Airflow to 3.1.8	2026-04-15	6.5
CVE-2026-20078	cisco - Cisco Unity Connection	Multiple vulnerabilities in Cisco Unity Connection could allow an authenticated, remote attacker to download arbitrary files from an affected system. To exploit these vulnerabilities, the attacker must have valid administrative credentials. _x000D_ _x000D_ These vulnerabilities are due to improper sanitization of user input to the web-based management interface. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request. A successful exploit could allow the attacker to download arbitrary files from an affected system.	2026-04-15	6.5
CVE-2026-20081	cisco - Cisco Unity Connection	Multiple vulnerabilities in Cisco Unity Connection could allow an authenticated, remote attacker to download arbitrary files from an affected system. To exploit these vulnerabilities, the attacker must have valid administrative credentials. _x000D_ _x000D_ These vulnerabilities are due to improper sanitization of user input to the web-based management interface. An attacker could exploit these vulnerabilities by sending a crafted HTTPS request. A successful exploit could allow the attacker to download arbitrary files from an affected system.	2026-04-15	6.5
CVE-2026-6364	google - chrome	Out of bounds read in Skia in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted file. (Chromium security severity: Medium)	2026-04-15	6.5
CVE-2026-6385	red hat - multiple products	A flaw was found in FFmpeg. A remote attacker could exploit this vulnerability by providing a specially crafted MPEG-PS/VOB media file containing a malicious DVD subtitle stream. This vulnerability is caused by a signed integer overflow in the DVD subtitle parser's fragment reassembly bounds checks, leading to a heap out-of-bounds write. Successful exploitation can result in a denial of service (DoS) due to an application crash, and potentially lead to arbitrary code execution.	2026-04-15	6.5
CVE-2026-34861	huawei - harmonyos	Race condition vulnerability in the thermal management module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-04-13	6.3
CVE-2026-34862	huawei - harmonyos	Race condition vulnerability in the power consumption statistics module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-04-13	6.3
CVE-2025-40745	siemens - multiple products	A vulnerability has been identified in Siemens Software Center (All versions < V3.5.8.2), Simcenter 3D (All versions < V2506.6000), Simcenter Femap (All versions < V2506.0002), Simcenter STAR-CCM+ (All versions < V2602), Solid Edge SE2025 (All versions < V225.0 Update 13), Solid Edge SE2026 (All versions < V226.0 Update 04), Tecnomatix Plant Simulation (All versions < V2504.0008). Affected applications do not properly validate client certificates to connect to Analytics Service	2026-04-14	6.3

		endpoint. This could allow an unauthenticated remote attacker to perform man in the middle attacks.		
CVE-2026-34626	adobe - multiple products	Acrobat Reader versions 26.001.21411, 24.001.30360, 24.001.30362 and earlier are affected by an Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') vulnerability that could result in arbitrary file system read in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	6.3
CVE-2026-27299	adobe - framemaker	Adobe Framemaker versions 2022.8 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An attacker could leverage this vulnerability to access sensitive files or data on the system. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	6.3
CVE-2026-6362	google - chrome	Use after free in Codecs in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to potentially perform out of bounds memory access via a crafted video file. (Chromium security severity: High)	2026-04-15	6.3
CVE-2026-32072	microsoft - multiple products	Improper authentication in Windows Active Directory allows an unauthorized attacker to perform spoofing locally.	2026-04-14	6.2
CVE-2025-46605	dell - PowerProtect Data Domain	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain a session fixation vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	2026-04-17	6.2
CVE-2025-46606	dell - PowerProtect Data Domain	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 8.4 through 8.5 contain an improper restriction of excessive authentication attempts vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to unauthorized access.	2026-04-17	6.2
CVE-2026-34852	huawei - harmonyos	Stack overflow vulnerability in the media platform. Impact: Successful exploitation of this vulnerability may affect availability.	2026-04-13	6.1
CVE-2026-21331	adobe - connect	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Scope is changed.	2026-04-14	6.1
CVE-2026-26169	microsoft - multiple products	Buffer over-read in Windows Kernel Memory allows an authorized attacker to disclose information locally.	2026-04-14	6.1
CVE-2026-32088	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Biometric Service allows an unauthorized attacker to bypass a security feature with a physical attack.	2026-04-14	6.1
CVE-2026-32196	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.	2026-04-14	6.1
CVE-2026-33822	microsoft - multiple products	Out-of-bounds read in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-04-14	6.1
CVE-2026-34614	adobe - connect	Adobe Connect versions 2025.3, 12.10 and earlier are affected by a reflected Cross-Site Scripting (XSS) vulnerability. If an attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser. Scope is changed.	2026-04-14	6.1
CVE-2026-20059	cisco - Cisco Unity Connection	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to conduct a reflected XSS attack against a user of the interface._x000D_ _x000D_ This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	2026-04-15	6.1
CVE-2026-20170	cisco - Cisco Webex Contact Center	A vulnerability in the Desktop Agent functionality of Cisco Webex Contact Center could have allowed an unauthenticated, remote attacker to conduct cross-site scripting attacks. Cisco has addressed this vulnerability in the Cisco Webex Contact Center service, and no customer action is needed._x000D_ _x000D_ This vulnerability existed because HTML and script content was not properly handled. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by persuading a user to follow a malicious link. A successful exploit could have allowed the attacker to steal sensitive information from the browser, including authentication and session information.	2026-04-15	6.1
CVE-2026-40919	red hat - multiple products	A flaw was found in GIMP. This vulnerability, a buffer overflow in the `file-seattle-filmworks` plugin, can be exploited when a user opens a specially crafted Seattle Filmworks file. A remote attacker could leverage this to cause a denial of service (DoS), leading to the plugin crashing and potentially impacting the stability of the GIMP application.	2026-04-15	6.1
CVE-2024-10242	wso2 - multiple products	The authentication endpoint fails to adequately validate user-supplied input before reflecting it back in the response. This allows an attacker to inject malicious script payloads into the input parameters, which are then executed by the victim's browser. Successful exploitation can enable an attacker to redirect the user's browser to a malicious website, modify the UI of the web page, or retrieve information from the browser. However, the impact is limited as session-related sensitive cookies are protected by the httpOnly flag, preventing session hijacking.	2026-04-16	6.1
CVE-2025-6024	wso2 - multiple products	The authentication endpoint fails to encode user-supplied input before rendering it in the web page, allowing for script injection. An attacker can leverage this by injecting malicious scripts into the authentication endpoint. This can result in the user's browser being redirected to a malicious website, manipulation of the web page's user interface, or the retrieval of information from the browser. However, session hijacking is not possible due to the httpOnly flag protecting session-related cookies.	2026-04-16	6.1
CVE-2025-61624	fortinet - multiple products	An Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') [CWE-22] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.4, FortiOS 7.4.0 through 7.4.9, FortiOS 7.2 all versions, FortiOS 7.0 all versions, FortiOS 6.4 all versions, FortiPAM 1.7.0, FortiPAM 1.6 all versions,	2026-04-14	6

		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 7.6.4, FortiProxy 7.4.0 through 7.4.11, FortiProxy 7.2 all versions, FortiProxy 7.0 all versions, FortiSwitchManager 7.2.0 through 7.2.7, FortiSwitchManager 7.0.0 through 7.0.6 may allow an authenticated attacker with admin profile and at least read-write permissions to write or delete arbitrary files via specific CLI commands.		
CVE-2025-68649	fortinet - multiple products	An improper limitation of a pathname to a restricted directory ('path traversal') vulnerability in Fortinet FortiAnalyzer 7.6.0 through 7.6.4, FortiAnalyzer 7.4.0 through 7.4.7, FortiAnalyzer 7.2 all versions, FortiAnalyzer 7.0 all versions, FortiAnalyzer Cloud 7.6.0 through 7.6.4, FortiAnalyzer Cloud 7.4.0 through 7.4.7, FortiAnalyzer Cloud 7.2 all versions, FortiAnalyzer Cloud 7.0 all versions, FortiManager 7.6.0 through 7.6.4, FortiManager 7.4.0 through 7.4.7, FortiManager 7.2 all versions, FortiManager 7.0 all versions, FortiManager Cloud 7.6.0 through 7.6.4, FortiManager Cloud 7.4.0 through 7.4.7, FortiManager Cloud 7.2 all versions, FortiManager Cloud 7.0 all versions may allow a privileged attacker to delete files from the underlying filesystem via crafted CLI requests.	2026-04-14	6
CVE-2026-39810	fortinet - forticlientems	A use of hard-coded cryptographic key vulnerability in Fortinet FortiClientEMS 7.4.0 through 7.4.5 may allow attacker to information disclosure via decrypting database dump.	2026-04-14	6
CVE-2026-20136	cisco - Cisco Identity Services Engine Software	A vulnerability in the CLI of Cisco Identity Services Engine (ISE) and Cisco ISE Passive Identity Connector (ISE-PIC) could allow an authenticated, local attacker with administrative privileges to perform a command injection attack on the underlying operating system and elevate privileges to root._x000D_ _x000D_ This vulnerability is due to insufficient validation of user supplied input. An attacker could exploit this vulnerability by providing crafted input to a specific CLI command. A successful exploit could allow the attacker to elevate their privileges to root on the underlying operating system.	2026-04-15	6
CVE-2025-12624	wso2 - identity_server	Active access tokens are not revoked or invalidated when a user account is locked within WSO2 Identity Server. This failure to enforce revocation allows previously issued, valid tokens to remain usable, enabling continued access to protected resources by locked user accounts. The security consequence is that a locked user account can maintain access to protected resources through the use of existing, unexpired access tokens. This creates a security gap where access control policies are bypassed, potentially leading to unauthorized data access or actions until the tokens naturally expire.	2026-04-16	6
CVE-2026-34859	huawei - multiple products	UAF vulnerability in the kernel module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	2026-04-13	5.9
CVE-2026-32226	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in .NET Framework allows an unauthorized attacker to deny service over a network.	2026-04-14	5.9
CVE-2026-28263	dell - PowerProtect Data Domain	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain a cross-site Scripting vulnerability. A high privileged attacker with remote access could potentially exploit this vulnerability, leading to Script injection.	2026-04-17	5.9
CVE-2026-34854	huawei - multiple products	UAF vulnerability in the kernel module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	2026-04-13	5.7
CVE-2026-34855	huawei - multiple products	Out-of-bounds write vulnerability in the kernel module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	2026-04-13	5.7
CVE-2026-4913	ivanti - multiple products	Improper protection of an alternate path in Ivanti N-ITSM before version 2025.4 allows a remote authenticated attacker to retain access when their account has been disabled.	2026-04-14	5.7
CVE-2026-21742	fortinet - multiple products	A cleartext transmission of sensitive information vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.2, FortiSOAR on-premise 7.5.0 through 7.5.1, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated attacker to view cleartext password in response for Secure Message Exchange and Radius queries, if configured	2026-04-14	5.7
CVE-2026-23653	microsoft - Microsoft Visual Studio Code CoPilot Chat Extension	Improper neutralization of special elements used in a command ('command injection') in GitHub Copilot and Visual Studio Code allows an authorized attacker to disclose information over a network.	2026-04-14	5.7
CVE-2026-23670	microsoft - multiple products	Untrusted pointer dereference in Windows Virtualization-Based Security (VBS) Enclave allows an authorized attacker to bypass a security feature locally.	2026-04-14	5.7
CVE-2026-34867	huawei - multiple products	Double free vulnerability in the multi-mode input system. Impact: Successful exploitation of this vulnerability may affect availability.	2026-04-13	5.6
CVE-2026-27285	adobe - multiple products	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application or disrupt its functionality. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	5.5
CVE-2026-27286	adobe - multiple products	InDesign Desktop versions 20.5.2, 21.2 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	5.5
CVE-2026-20806	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows COM allows an authorized attacker to disclose information locally.	2026-04-14	5.5
CVE-2026-27258	adobe - dng_software_development_kit	DNG SDK versions 1.7.1 2502 and earlier are affected by an out-of-bounds write vulnerability that could lead to application denial-of-service. An attacker could leverage this vulnerability to corrupt memory, causing the application to crash or become unresponsive. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	5.5
CVE-2026-27930	microsoft - multiple products	Out-of-bounds read in Windows GDI allows an unauthorized attacker to disclose information locally.	2026-04-14	5.5
CVE-2026-27931	microsoft - multiple products	Out-of-bounds read in Windows GDI allows an unauthorized attacker to disclose information locally.	2026-04-14	5.5

CVE-2026-32079	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	2026-04-14	5.5
CVE-2026-32081	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	2026-04-14	5.5
CVE-2026-32084	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows File Explorer allows an authorized attacker to disclose information locally.	2026-04-14	5.5
CVE-2026-32085	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Remote Procedure Call allows an authorized attacker to disclose information locally.	2026-04-14	5.5
CVE-2026-32181	microsoft - multiple products	Improper privilege management in Microsoft Windows allows an authorized attacker to deny service locally.	2026-04-14	5.5
CVE-2026-32212	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.	2026-04-14	5.5
CVE-2026-32214	microsoft - multiple products	Improper access control in Universal Plug and Play (upnp.dll) allows an authorized attacker to disclose information locally.	2026-04-14	5.5
CVE-2026-32215	microsoft - multiple products	Insertion of sensitive information into log file in Windows Kernel allows an authorized attacker to disclose information locally.	2026-04-14	5.5
CVE-2026-32216	microsoft - multiple products	Null pointer dereference in Windows Redirected Drive Buffering allows an authorized attacker to deny service locally.	2026-04-14	5.5
CVE-2026-32217	microsoft - multiple products	Insertion of sensitive information into log file in Windows Kernel allows an authorized attacker to disclose information locally.	2026-04-14	5.5
CVE-2026-32218	microsoft - multiple products	Insertion of sensitive information into log file in Windows Kernel allows an authorized attacker to disclose information locally.	2026-04-14	5.5
CVE-2026-33103	microsoft - Microsoft Dynamics 365 (on-premises) version 9.0	Improper access control in Microsoft Dynamics 365 (on-premises) allows an authorized attacker to disclose information locally.	2026-04-14	5.5
CVE-2026-27222	adobe - multiple products	Bridge versions 16.0.2, 15.1.4 and earlier are affected by a Divide By Zero vulnerability that could lead to application denial-of-service. An attacker could exploit this vulnerability to crash the application or render it unresponsive. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	5.5
CVE-2026-27300	adobe - framemaker	Adobe Framemaker versions 2022.8 and earlier are affected by an Access of Uninitialized Pointer vulnerability that could lead to memory exposure. 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.	2026-04-14	5.5
CVE-2026-27301	adobe - framemaker	Adobe Framemaker versions 2022.8 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could lead to memory exposure. An attacker could leverage this vulnerability to disclose sensitive information stored in memory. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-04-14	5.5
CVE-2026-20161	cisco - Cisco ThousandEyes Enterprise Agent	A vulnerability in the CLI of Cisco ThousandEyes Enterprise Agent could allow an authenticated, local attacker with low privileges to overwrite arbitrary files on the local system of an affected device._x000D_ _x000D_ This vulnerability is due to improper access controls on files that are on the local file system of an affected device. An attacker could exploit this vulnerability by placing a symbolic link in a specific location on the local file system. A successful exploit could allow the attacker to bypass file system permissions and overwrite arbitrary files on the affected device.	2026-04-15	5.5
CVE-2026-6245	red hat - multiple products	A flaw was found in the System Security Services Daemon (SSSD). The pam_passkey_child_read_data() function within the PAM passkey responder fails to properly handle raw bytes received from a pipe. Because the data is treated as a NUL-terminated C string without explicit termination, it results in an out-of-bounds read when processed by functions like snprintf(). A local attacker could potentially trigger this vulnerability by initiating a crafted passkey authentication request, causing the SSSD PAM responder to crash, resulting in a local Denial of Service (DoS).	2026-04-15	5.5
CVE-2026-40915	red hat - multiple products	A flaw was found in GIMP. A remote attacker could exploit an integer overflow vulnerability in the FITS image loader by providing a specially crafted FITS file. This integer overflow leads to a zero-byte memory allocation, which is then subjected to a heap buffer overflow when processing pixel data. Successful exploitation could result in a denial of service (DoS) or potentially arbitrary code execution.	2026-04-15	5.5
CVE-2026-40918	red hat - multiple products	A flaw was found in GIMP. Processing a specially crafted PVR image file with large dimensions can lead to a denial of service (DoS). This occurs due to a stack-based buffer overflow and an out-of-bounds read in the PVR image loader, causing the application to crash. Systems that process untrusted PVR image files are affected.	2026-04-15	5.5
CVE-2026-21011	samsung - multiple products	Incorrect privilege assignment in Bluetooth in Maintenance mode prior to SMR Apr-2026 Release 1 allows physical attackers to bypass Extend Unlock.	2026-04-13	5.4
CVE-2026-35565	apache - storm	Stored Cross-Site Scripting (XSS) via Unsanitized Topology Metadata in Apache Storm UI Versions Affected: before 2.8.6 Description: The Storm UI visualization component interpolates topology metadata including component IDs, stream names, and grouping values directly into HTML via innerHTML in parseNode() and parseEdge() without sanitization at any layer. An authenticated user with topology submission rights could craft a topology containing malicious HTML/JavaScript in component identifiers (e.g., a bolt ID containing an onerror event handler). This payload flows through Nimbus → Thrift → the Visualization API → vis.js tooltip rendering, resulting in stored cross-site scripting. In multi-tenant deployments where topology submission is available to less-trusted users but the UI	2026-04-13	5.4

		is accessed by operators or administrators, this enables privilege escalation through script execution in an admin's browser session. Mitigation: 2.x users should upgrade to 2.8.6. Users who cannot upgrade immediately should monkey-patch the parseNode() and parseEdge() functions in the visualization JavaScript file to HTML-escape all API-supplied values including nodeId, :capacity, :latency, :component, :stream, and :grouping before interpolation into tooltip HTML strings, and should additionally restrict topology submission to trusted users via Nimbus ACLs as a defense-in-depth measure. A guide on how to do this is available in the release notes of 2.8.6. Credit: This issue was discovered while investigating another report by K.		
CVE-2026-4914	ivanti - multiple products	Stored XSS in Ivanti N-ITSM before version 2025.4 allows a remote authenticated attacker to obtain limited information from other user sessions. User interaction is required.	2026-04-14	5.4
CVE-2024-23104	fortinet - fortivoice	An exposure of sensitive information to an unauthorized actor vulnerability in Fortinet FortiNDR 7.6.0, FortiNDR 7.4.0 through 7.4.8, FortiNDR 7.2 all versions, FortiNDR 7.1 all versions, FortiNDR 7.0 all versions, FortiVoice 7.0.0 through 7.0.1 may allow a remote authenticated attacker with at least read-only permission on system maintenance to access backup information via crafted HTTP requests	2026-04-14	5.4
CVE-2025-61886	fortinet - multiple products	An Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability [CWE-79] vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.4, FortiSandbox PaaS 5.0.0 through 5.0.4 may allow an attacker to perform an XSS attack via crafted HTTP requests.	2026-04-14	5.4
CVE-2026-27288	adobe - multiple products	Adobe Experience Manager versions 6.5.24, FP11.7 and earlier are 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.	2026-04-14	5.4
CVE-2026-34623	adobe - multiple products	Adobe Experience Manager versions 6.5.24, FP11.7 and earlier are 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 specially crafted web page.	2026-04-14	5.4
CVE-2026-34624	adobe - multiple products	Adobe Experience Manager versions 6.5.24, FP11.7 and earlier are 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.	2026-04-14	5.4
CVE-2026-34625	adobe - multiple products	Adobe Experience Manager versions 6.5.24, FP11.7 and earlier are 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.	2026-04-14	5.4
CVE-2026-1636	lenovo - Service Bridge	A potential DLL hijacking vulnerability was reported in Lenovo Service Bridge that, under certain conditions, could allow a local authenticated user to execute code with elevated privileges.	2026-04-15	5.4
CVE-2026-6383	red hat - Red Hat OpenShift Virtualization 4	A flaw was found in KubeVirt's Role-Based Access Control (RBAC) evaluation logic. The authorization mechanism improperly truncates subresource names, leading to incorrect permission evaluations. This allows authenticated users with specific custom roles to gain unauthorized access to subresources, potentially disclosing sensitive information or performing actions they are not permitted to do. Additionally, legitimate users may be denied access to resources.	2026-04-15	5.4
CVE-2024-4867	wso2 - multiple products	The WSO2 API Manager developer portal accepts user-supplied input without enforcing expected validation constraints or proper output encoding. This deficiency allows a malicious actor to inject script content that is executed within the context of a user's browser. By leveraging this cross-site scripting vulnerability, a malicious actor can cause the browser to redirect to a malicious website, make changes to the UI of the web page, or retrieve information from the browser. However, session hijacking is not possible as all session-related sensitive cookies are protected by the httpOnly flag.	2026-04-16	5.4
CVE-2026-40948	apache software foundation - Apache Airflow Providers Keycloak	The Keycloak authentication manager in `apache-airflow-providers-keycloak` did not generate or validate the OAuth 2.0 `state` parameter on the login / login-callback flow, and did not use PKCE. An attacker with a Keycloak account in the same realm could deliver a crafted callback URL to a victim's browser and cause the victim to be logged into the attacker's Airflow session (login-CSRF / session fixation), where any credentials the victim subsequently stored in Airflow Connections would be harvestable by the attacker. Users are advised to upgrade `apache-airflow-providers-keycloak` to 0.7.0 or later.	2026-04-18	5.4
CVE-2026-31924	apache - apisix	Cleartext Transmission of Sensitive Information vulnerability in Apache APISIX. tencent-cloud-cls log export uses plaintext HTTP This issue affects Apache APISIX: from 2.99.0 through 3.15.0. Users are recommended to upgrade to version 3.16.0, which fixes the issue.	2026-04-14	5.3
CVE-2026-2400	schneider-electric - powerchute_serial_shutdown	CWE-93 Improper Neutralization of CRLF Sequences ('CRLF Injection') vulnerability exists that could cause application user credentials to reset when a Web Admin user alters the POST /setPCBEDesc request payload.	2026-04-14	5.3
CVE-2026-2403	schneider-electric - powerchute_serial_shutdown	CWE-1284 Improper Validation of Specified Quantity in Input vulnerability exists that could cause Event and Data Log truncation impacting log integrity when a Web Admin user alters the POST /logsettings request payload.	2026-04-14	5.3
CVE-2026-2405	schneider-electric - powerchute_serial_shutdown	CWE-400 Uncontrolled Resource Consumption vulnerability exists that could cause excessive troubleshooting zip file creation and denial of service when a Web Admin user floods the system with POST /helpabout requests.	2026-04-14	5.3

CVE-2026-20152	cisco - Cisco Secure Web Appliance	A vulnerability in the authentication service feature of Cisco AsyncOS Software for Cisco Secure Web Appliance could allow an unauthenticated, remote attacker to bypass authentication policy requirements._x000D_ _x000D_ This vulnerability is due to improper validation of user-supplied authentication input in HTTP requests. An attacker could exploit this vulnerability by sending HTTP requests that contain specific authentication requests to an affected device. A successful exploit could allow the attacker to bypass policy enforcement on the device. There is no direct impact to the Cisco Secure Web Appliance. However, as a result of exploiting this vulnerability, an attacker could send HTTP requests that should be restricted through the device.	2026-04-15	5.3
CVE-2026-21726	grafana - loki	The CVE-2021-36156 fix validates the namespace parameter for path traversal sequences after a single URL decode, by double encoding, an attacker can read files at the Ruler API endpoint /loki/api/v1/rules/{namespace} Thanks to Prasanth Sundararajan for reporting this vulnerability.	2026-04-15	5.3
CVE-2026-6494	red hat - Red Hat Ansible Automation Platform 2	A flaw was found in the AAP MCP server. An unauthenticated remote attacker can exploit a log injection vulnerability by sending specially crafted input to the `toolsetroute` parameter. This parameter is not properly sanitized before being written to logs, allowing the attacker to inject control characters such as newlines and ANSI escape sequences. This enables the attacker to obscure legitimate log entries and insert forged ones, which could facilitate social engineering attacks, potentially leading to an operator executing dangerous commands or visiting malicious URLs.	2026-04-17	5.3
CVE-2026-21003	samsung - multiple products	Improper input validation in data related to network restrictions prior to SMR Apr-2026 Release 1 allows physical attackers to bypass the restrictions.	2026-04-13	5.2
CVE-2026-4135	lenovo - Software Fix	During an internal security assessment, a potential vulnerability was discovered in Lenovo Software Fix, that during installation could allow a local authenticated user to perform an arbitrary file write with elevated privileges.	2026-04-15	5.2
CVE-2026-21008	samsung - multiple products	Exposure of sensitive information in S Share prior to SMR Apr-2026 Release 1 allows adjacent attacker to access sensitive information.	2026-04-13	5.1
CVE-2026-21014	samsung - camera	Improper access control in Samsung Camera prior to version 16.5.00.28 allows local attacker to access location data. User interaction is required for triggering this vulnerability.	2026-04-13	5.1
CVE-2026-34866	huawei - harmonyos	Out-of-bounds write vulnerability in the WEB module.Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	2026-04-13	5.1
CVE-2026-33892	siemens - multiple products	A vulnerability has been identified in Industrial Edge Management Pro V1 (All versions >= V1.7.6 < V1.15.17), Industrial Edge Management Pro V2 (All versions >= V2.0.0 < V2.1.1), Industrial Edge Management Virtual (All versions >= V2.2.0 < V2.8.0). Affected management systems do not properly enforce user authentication on remote connections to devices._x000D_ This could facilitate an unauthenticated remote attacker to circumvent authentication and impersonate a legitimate user._x000D_ Successful exploitation requires that the attacker has identified the header and port used for remote connections to devices and that the remote connection feature is enabled for the device._x000D_ _x000D_ Exploitation allows the attacker to tunnel to the device. Security features on this device itself (e.g. app specific authentication) are not affected.	2026-04-14	5.1
CVE-2025-36579	dell - multiple products	Dell Client Platform BIOS contains a Weak Password Recovery Mechanism vulnerability. An unauthenticated attacker with physical access to the system could potentially exploit this vulnerability, leading to unauthorized access.	2026-04-16	5.1
CVE-2026-40916	red hat - multiple products	A flaw was found in GIMP. A stack buffer overflow vulnerability in the TIM image loader's 4BPP decoding path allows a local user to cause a Denial of Service (DoS). By opening a specially crafted TIM image file, the application crashes due to an unconditional overflow when writing to a variable-length array.	2026-04-15	5
CVE-2026-40917	red hat - multiple products	A flaw was found in GIMP. This vulnerability, a heap buffer over-read in the `icns_slurp()` function, occurs when processing specially crafted ICNS image files. An attacker could provide a malicious ICNS file, potentially leading to application crashes or information disclosure on systems that process such files.	2026-04-15	5
CVE-2026-39811	fortinet - multiple products	A integer overflow or wraparound vulnerability in Fortinet FortiWeb 8.0.0 through 8.0.3, FortiWeb 7.6.0 through 7.6.6, FortiWeb 7.4 all versions, FortiWeb 7.2 all versions, FortiWeb 7.0 all versions may allow attacker to denial of service via <insert attack vector here>	2026-04-14	4.9
CVE-2026-20148	cisco - multiple products	A vulnerability in Cisco ISE and Cisco ISE-PIC could allow an authenticated, remote attacker to perform path traversal attacks on the underlying operating system and read 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 on the affected system.	2026-04-15	4.9
CVE-2026-39812	fortinet - multiple products	A improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.5, FortiSandbox 4.4.0 through 4.4.8, FortiSandbox 4.2 all versions, FortiSandbox PaaS 5.0.0 through 5.0.5, FortiSandbox PaaS 4.4.0 through 4.4.8, FortiSandbox PaaS 4.2 all versions may allow attacker to execute unauthorized code or commands via <insert attack vector here>	2026-04-14	4.8
CVE-2026-20132	cisco - Cisco Identity Services Engine Software	Multiple vulnerabilities in the web-based management interface of Cisco Identity Services Engine (ISE) could allow an authenticated, remote attacker with administrative write privileges to conduct a stored cross-site scripting (XSS) attack or a reflected XSS attack against a user of the web-based management interface of an affected device._x000D_ _x000D_ These vulnerabilities are due to insufficient sanitization of user-supplied data that is stored in the web page. An attacker could exploit these vulnerabilities by convincing a user of the interface to click a specific link or view an affected web page. The injected script code may be executed in the	2026-04-15	4.8

		context of the web-based management interface or allow the attacker to access sensitive browser-based information.		
CVE-2026-34857	huawei - multiple products	UAF vulnerability in the communication module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-04-13	4.7
CVE-2026-21006	samsung - multiple products	Improper access control in Samsung DeX prior to SMR Apr-2026 Release 1 allows physical attackers to access to hidden notification contents.	2026-04-13	4.7
CVE-2026-20060	cisco - Cisco Unity Connection	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an unauthenticated, remote attacker to redirect a user to a malicious web page._x000D_ _x000D_ This vulnerability is due to improper input validation of HTTP request parameters. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to redirect a user to a malicious web page.	2026-04-15	4.7
CVE-2026-22154	fortinet - multiple products	An improper neutralization of input during web page generation ('cross-site scripting') vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.3, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.3, FortiSOAR on-premise 7.5.0 through 7.5.2, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated remote attacker to perform a stored cross site scripting (XSS) attack via crafted HTTP Requests.	2026-04-14	4.6
CVE-2026-20928	microsoft - multiple products	Improper removal of sensitive information before storage or transfer in Windows Recovery Environment Agent allows an unauthorized attacker to bypass a security feature with a physical attack.	2026-04-14	4.6
CVE-2026-20945	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.	2026-04-14	4.6
CVE-2026-26175	microsoft - multiple products	Use of uninitialized resource in Windows Boot Manager allows an unauthorized attacker to bypass a security feature with a physical attack.	2026-04-14	4.6
CVE-2026-21007	samsung - multiple products	Improper check for exceptional conditions in Device Care prior to SMR Apr-2026 Release 1 allows physical attackers to bypass Knox Guard.	2026-04-13	4.4
CVE-2026-27906	microsoft - multiple products	Improper input validation in Windows Hello allows an authorized attacker to bypass a security feature locally.	2026-04-14	4.4
CVE-2026-32220	microsoft - multiple products	Improper access control in Windows Virtualization-Based Security (VBS) Enclave allows an authorized attacker to bypass a security feature locally.	2026-04-14	4.4
CVE-2025-43935	dell - multiple products	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an improper resource shutdown or release vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service.	2026-04-16	4.4
CVE-2026-33929	apache - multiple products	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability in Apache PDFBox Examples. This issue affects the ExtractEmbeddedFiles example in Apache PDFBox: from 2.0.24 through 2.0.36, from 3.0.0 through 3.0.7. Users are recommended to update to version 2.0.37 or 3.0.8 once available. Until then, they should apply the fix provided in GitHub PR 427. The ExtractEmbeddedFiles example contained a path traversal vulnerability (CWE-22) mentioned in CVE-2026-23907. However the change in the releases 2.0.36 and 3.0.7 is flawed because it doesn't consider the file path separator. Because of that, a user having writing rights on /home/ABC could be victim to a malicious PDF resulting in a write attempt to any path starting with /home/ABC, e.g. "/home/ABCDEF". Users who have copied this example into their production code should apply the mentioned change. The example has been changed accordingly and is available in the project repository.	2026-04-14	4.3
CVE-2025-59809	fortinet - multiple products	A server-side request forgery (ssrf) vulnerability [CWE-918] vulnerability in Fortinet FortiSOAR PaaS 7.6.4, FortiSOAR PaaS 7.6.0 through 7.6.2, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.4, FortiSOAR on-premise 7.6.0 through 7.6.2, FortiSOAR on-premise 7.5.0 through 7.5.2, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated attacker to discover services running on local ports via crafted requests.	2026-04-14	4.3
CVE-2026-22576	fortinet - multiple products	A storing passwords in a recoverable format vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.4, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.4, FortiSOAR on-premise 7.5.0 through 7.5.2, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated remote attacker to retrieve passwords for multiple installed connectors via server address modification in connector configuration.	2026-04-14	4.3
CVE-2026-32202	microsoft - multiple products	Protection mechanism failure in Windows Shell allows an unauthorized attacker to perform spoofing over a network.	2026-04-14	4.3
CVE-2026-33829	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Snipping Tool allows an unauthorized attacker to perform spoofing over a network.	2026-04-14	4.3
CVE-2026-20061	cisco - Cisco Unity Connection	A vulnerability in the web-based management interface of Cisco Unity Connection could allow an authenticated, remote attacker to perform an SQL injection attack against an affected device. To exploit this vulnerability, the attacker must have valid user credentials on the affected device._x000D_ _x000D_ This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending a crafted HTTP(S) request to the web-based management interface of an affected device. A successful exploit could allow the attacker to view data on the affected device.	2026-04-15	4.3

CVE-2026-6298	google - chrome	Heap buffer overflow in Skia in Google Chrome prior to 147.0.7727.101 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Critical)	2026-04-15	4.3
CVE-2026-23777	dell - PowerProtect Data Domain	Dell PowerProtect Data Domain with Data Domain Operating System (DD OS) of Feature Release versions 7.7.1.0 through 8.5, LTS2025 release version 8.3.1.0 through 8.3.1.20, LTS2024 release versions 7.13.1.0 through 7.13.1.50, contain an exposure of sensitive information to an unauthorized actor vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to information exposure.	2026-04-17	4.3
CVE-2026-34860	huawei - multiple products	Access control vulnerability in the memo module. Impact: Successful exploitation of this vulnerability will affect availability and confidentiality.	2026-04-13	4.1
CVE-2026-34858	huawei - multiple products	UAF vulnerability in the communication module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-04-13	4.1
CVE-2026-21009	samsung - multiple products	Improper check for exceptional conditions in Recents prior to SMR Apr-2026 Release 1 allows physical attacker to bypass App Pinning.	2026-04-13	4.1
CVE-2026-22574	fortinet - multiple products	A storing passwords in a recoverable format vulnerability in Fortinet FortiSOAR PaaS 7.6.0 through 7.6.4, FortiSOAR PaaS 7.5.0 through 7.5.2, FortiSOAR PaaS 7.4 all versions, FortiSOAR PaaS 7.3 all versions, FortiSOAR on-premise 7.6.0 through 7.6.4, FortiSOAR on-premise 7.5.0 through 7.5.2, FortiSOAR on-premise 7.4 all versions, FortiSOAR on-premise 7.3 all versions may allow an authenticated remote attacker to retrieve Service account password via server address modification in LDAP configuration.	2026-04-14	4.1
CVE-2025-43883	dell - multiple products	Dell PowerScale OneFS, versions prior to 9.12.0.0, contains an improper check for unusual or exceptional conditions vulnerability. A high privileged attacker with local access could potentially exploit this vulnerability, leading to denial of service.	2026-04-16	4.1
CVE-2026-32690	apache - airflow	Secrets in Variables saved as JSON dictionaries were not properly redacted - in case thee variables were retrieved by the user the secrets stored as nested fields were not masked. If you do not store variables with sensitive values in JSON form, you are not affected. Otherwise please upgrade to Apache Airflow 3.2.0 that has the fix implemented	2026-04-18	3.7
CVE-2024-8010	wso2 - multiple products	The component accepts XML input through the publisher without disabling external entity resolution. This allows malicious actors to submit a crafted XML payload that exploits the unescaped external entity references. By leveraging this vulnerability, a malicious actor can read confidential files from the product's file system or access limited HTTP resources reachable via HTTP GET requests to the vulnerable product.	2026-04-16	3.5
CVE-2026-21727	grafana - multiple products	--- title: Cross-Tenant Legacy Correlation Disclosure and Deletion draft: false hero: image: /static/img/heros/hero-legal2.svg content: "# Cross-Tenant Legacy Correlation Disclosure and Deletion" date: 2026-01-29 product: Grafana severity: Low cve: CVE-2026-21727 cvss_score: "3.3" cvss_vector: "CVSS:3.3/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N" fixed_versions: - ">=11.6.11 >=12.0.9 >=12.1.6 >=12.2.4" --- A cross-tenant isolation vulnerability was found in Grafana’s Correlations feature affecting legacy correlation records. Due to a backward compatibility condition allowing org_id = 0 records to be returned across organizations, a user with datasource management privileges could read and permanently delete legacy correlation data belonging to another organization. This issue affects correlations created prior to Grafana 10.2 and is fixed in >=11.6.11, >=12.0.9, >=12.1.6, and >=12.2.4. Thanks to Gyu-hyeok Lee (g2h) for reporting this vulnerability.	2026-04-15	3.3
CVE-2026-6312	google - chrome	Insufficient policy enforcement in Passwords in Google Chrome prior to 147.0.7727.101 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-04-15	3.1
CVE-2026-6313	google - chrome	Insufficient policy enforcement in CORS in Google Chrome prior to 147.0.7727.101 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-04-15	3.1
CVE-2026-27316	fortinet - multiple products	A insufficiently protected credentials vulnerability in Fortinet FortiSandbox 5.0.0 through 5.0.5, FortiSandbox 4.4 all versions, FortiSandbox PaaS 5.0.1 through 5.0.5 may allow an authenticathed administrator to read LDAP server credentials via client-side inspection.	2026-04-14	2.7
CVE-2026-34849	huawei - multiple products	UAF vulnerability in the screen management module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-04-13	2.5
CVE-2026-21741	fortinet - fortinac-f	An URL Redirection to Untrusted Site ('Open Redirect') vulnerability [CWE-601] vulnerability in Fortinet FortiNAC-F 7.6.0 through 7.6.5, FortiNAC-F 7.4 all versions, FortiNAC-F 7.2 all versions may allow a remote privileged attacker with system administrator role to redirect users to an arbitrary website via crafted CSV file.	2026-04-14	2.4
CVE-2026-2401	schneider-electric - powerchute_serial_shutdown	CWE-532 Insertion of Sensitive Information into Log File vulnerability exists that could cause confidential information to be exposed when a Web Admin user executes a malicious file provided by an attacker.	2026-04-14	2.4
CVE-2026-27307	adobe - multiple products	ColdFusion versions 2023.18, 2025.6 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. A high-privileged	2026-04-14	2.4

		attacker could exploit this vulnerability and exhaust system resources, reducing application speed. Exploitation of this issue does not require user interaction.		
CVE-2026-27308	adobe - multiple products	ColdFusion versions 2023.18, 2025.6 and earlier are affected by an Uncontrolled Resource Consumption vulnerability that could lead to application denial-of-service. A high-privileged attacker could exploit this vulnerability and exhaust system resources, reducing application speed. Exploitation of this issue does not require user interaction.	2026-04-14	2.4
CVE-2026-34851	huawei - multiple products	Race condition vulnerability in the event notification module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-04-13	2.2
CVE-2026-34850	huawei - multiple products	Race condition vulnerability in the notification service. Impact: Successful exploitation of this vulnerability may affect availability.	2026-04-13	1.9
CVE-2025-12141	grafana - grafana	In Grafana's alerting system, users with edit permissions for a contact point, specifically the permissions “alert.notifications:write” or “alert.notifications.receivers:test” that are granted as part of the fixed role "Contact Point Writer", which is part of the basic role Editor - can edit contact points created by other users, modify the endpoint URL to a controlled server. By invoking the test functionality, attackers can capture and extract redacted secure settings, such as authentication credentials for third-party services (e.g., Slack tokens). This leads to unauthorized access and potential compromise of external integrations.	2026-04-15	1.3

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.