الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

تمت مشاركة هذه المعلومة بإشارة مشاركة ***أبيض*** حيث يسمح بتبادلها أو نشرها من خلال القنوات العامة.

في ضوء دور الهيئة الوطنية للأمن السيبراني للمساعدة في حماية الفضاء السيبراني الوطني، تود الهيئة مشاركتكم النشرة الأسبوعية للثغرات المسجلة من قبل the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) للأسبوع من 7 يونيو إلى 13 يونيو. 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 7th of June to 13th of June. 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-2026-10520	ivanti - multiple products	An OS Command Injection vulnerability in Ivanti Sentry before the R10.5.2, R10.6.2 and R10.7.1 versions allows a remote unauthenticated user to achieve root-level remote code execution	2026-06-09	10
CVE-2026-47938	adobe - Adobe Campaign Classic (ACC)	Adobe Campaign Classic (ACC) versions 7.4.3 build 9394 and earlier are affected by a Server-Side Request Forgery (SSRF) vulnerability that could result in privilege escalation. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-09	10
CVE-2026-48303	adobe - multiple products	Adobe Campaign Classic (ACC) versions 7.4.3 build 9394 and earlier are affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-09	10
CVE-2026-10523	ivanti - Sentry	An Authentication Bypass vulnerability (CWE-288) in Ivanti Sentry before the R10.5.2, R10.6.2 and R10.7.1 versions allows a remote unauthenticated attacker to create arbitrary administrative accounts and obtain full administrative access	2026-06-09	9.9
CVE-2026-29167	apache - http_server	Use After Free vulnerability in Apache HTTP Server with mod_ldap in per-directory configuration This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	2026-06-08	9.8
CVE-2026-44631	apache - http_server	Buffer Underwrite vulnerability in Apache HTTP Server on crafted regular expressions in the configuration. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	2026-06-08	9.8
CVE-2026-46289	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: lib/scatterlist: fix length calculations in extract_kvec_to_sg Patch series "Fix bugs in extract_iter_to_sg()", v3. Fix bugs in the kvec and user variants of extract_iter_to_sg. This series is growing due to useful remarks made by sashiko.dev. The main bugs are: - The length for an sglist entry when extracting from a kvec can exceed the number of bytes in the page. This is obviously not intended. - When extracting a user buffer the sglist is temporarily used as a scratch buffer for extracted page pointers. If the sglist already contains some elements this scratch buffer could overlap with existing entries in the sglist. The series adds test cases to the kunit_iov_iter test that demonstrate all of these bugs. Additionally, there is a memory leak fix for the test itself. The bugs were orignally introduced into kernel v6.3 where the function lived in fs/netfs/iterator.c. It was later moved to lib/scatterlist.c in	2026-06-08	9.8

		v6.5. Thus the actual fix is only marked for backports to v6.5+. This patch (of 5): When extracting from a kvec to a scatterlist, do not cross page boundaries. The required length was already calculated but not used as intended. Adjust the copied length if the loop runs out of sglist entries without extracting everything. While there, return immediately from extract_iter_to_sg if there are no sglist entries at all. A subsequent commit will add kunit test cases that demonstrate that the patch is necessary.		

CVE-2026-46325	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved:
		
		RDMA/rxe: Fix iova-to-va conversion for MR page sizes != PAGE_SIZE
		
		The current implementation incorrectly handles memory regions (MRs) with
		page sizes different from the system PAGE_SIZE. The core issue is that
		rxe_set_page() is called with mr->page_size step increments, but the
		page_list stores individual struct page pointers, each representing
		PAGE_SIZE of memory.
		
		ib_sg_to_page() has ensured that when i>=1 either
		a) SG[i-1].dma_end and SG[i].dma_addr are contiguous
		or
		b) SG[i-1].dma_end and SG[i].dma_addr are mr->page_size aligned.
		
		This leads to incorrect iova-to-va conversion in scenarios:
		
		1) page_size < PAGE_SIZE (e.g., MR: 4K, system: 64K):
		  ibmr->iova = 0x181800
		  sg[0]: dma_addr=0x181800, len=0x800
		  sg[1]: dma_addr=0x173000, len=0x1000
		
		  Access iova = 0x181800 + 0x810 = 0x182010
		  Expected VA: 0x173010 (second SG, offset 0x10)
		  Before fix:
		  - index = (0x182010 >> 12) - (0x181800 >> 12) = 1
		  - page_offset = 0x182010 & 0xFFF = 0x10
		  - xarray[1] stores system page base 0x170000
		  - Resulting VA: 0x170000 + 0x10 = 0x170010 (wrong)
		
		2) page_size > PAGE_SIZE (e.g., MR: 64K, system: 4K):
		  ibmr->iova = 0x18f800
		  sg[0]: dma_addr=0x18f800, len=0x800
		  sg[1]: dma_addr=0x170000, len=0x1000
		
		  Access iova = 0x18f800 + 0x810 = 0x190010
		  Expected VA: 0x170010 (second SG, offset 0x10)
		  Before fix:
		  - index = (0x190010 >> 16) - (0x18f800 >> 16) = 1
		  - page_offset = 0x190010 & 0xFFFF = 0x10
		  - xarray[1] stores system page for dma_addr 0x170000
		  - Resulting VA: system page of 0x170000 + 0x10 = 0x170010 (wrong)
		
		Yi Zhang reported a kernel panic[1] years ago related to this defect.
		
		Solution:
		1. Replace xarray with pre-allocated rxe_mr_page array for sequential
		  indexing (all MR page indices are contiguous)
		2. Each rxe_mr_page stores both struct page* and offset within the
		  system page
		3. Handle MR page_size != PAGE_SIZE relationships:
		  - page_size > PAGE_SIZE: Split MR pages into multiple system pages
		  - page_size <= PAGE_SIZE: Store offset within system page
		4. Add boundary checks and compatibility validation
		
		This ensures correct iova-to-va conversion regardless of MR page size
		and system PAGE_SIZE relationship, while improving performance through
		array-based sequential access.
		
		Tests on 4K and 64K PAGE_SIZE hosts:
		- rdma-core/pytests
		  $ ./build/bin/run_tests.py --dev eth0_rxe
		- blktest:
			2026-06-09	9.8

		$ TIMEOUT=30 QUICK_RUN=1 USE_RXE=1 NVMET_TRTYPES=rdma ./check nvme srp rnbd [1] https://lore.kernel.org/all/CAHj4cs9XRqE25jyVw9rj9YugffLn5+f=1znaBEnu1usLOciD+g@mail.gmail.com/T/		
CVE-2026-25089	fortinet - multiple products	A improper neutralization of special elements used in an os command ('os command injection') 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 through 5.0.5, FortiSandbox PaaS 5.0.4 through 5.0.5 may allow an unauthenticated attacker to execute unauthorized commands via specifically crafted HTTP requests	2026-06-09	9.8
CVE-2026-26142	microsoft - multiple products	Deserialization of untrusted data in Nuance PowerScribe allows an unauthorized attacker to execute code over a network.	2026-06-09	9.8
CVE-2026-44815	microsoft - multiple products	Stack-based buffer overflow in Windows DHCP Client allows an unauthorized attacker to execute code over a network.	2026-06-09	9.8
CVE-2026-45657	microsoft - multiple products	Use after free in Windows Kernel allows an unauthorized attacker to execute code over a network.	2026-06-09	9.8
CVE-2026-47291	microsoft - multiple products	Integer overflow or wraparound in Windows HTTP.sys allows an unauthorized attacker to execute code over a network.	2026-06-09	9.8
CVE-2026-47643	microsoft - azure_stack_edge	External control of file name or path in Azure Stack Edge allows an unauthorized attacker to execute code over a network.	2026-06-09	9.8
CVE-2026-35273	oracle - multiple products	Vulnerability in the PeopleSoft Enterprise PeopleTools product of Oracle PeopleSoft (component: Updates Environment Management). Supported versions that are affected are 8.61 and 8.62. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise PeopleSoft Enterprise PeopleTools. Successful attacks of this vulnerability can result in takeover of PeopleSoft Enterprise PeopleTools. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).	2026-06-11	9.8
CVE-2026-49875	apache - multiple products	Apache CXF's EndpointReferenceUtils and W3CMultiSchemaFactory classes construct a SAXParserFactory without the necessary JAXP hardening configurations, enabling out-of-band (OOB) external entity resolution. Users are recommended to upgrade to versions 4.2.2 or 4.1.7, which fix this issue.	2026-06-12	9.8
CVE-2026-50628	apache - multiple products	A logic error in OAuthRequestFilter rejects legitimate requests originating from the bound IP address, while blindly allowing requests from any other IP address. Enabling this security feature inadvertently creates an inverse security check. Users are recommended to upgrade to versions 4.2.2 or 4.1.7, which fixes this issue.	2026-06-12	9.8
CVE-2026-11634	google - chrome	Use after free in Gamepad in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-09	9.6
CVE-2026-11638	google - chrome	Use after free in Printing in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-09	9.6
CVE-2026-11651	google - chrome	Use after free in Network in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-09	9.6
CVE-2026-11654	google - chrome	Use after free in CameraCapture in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-09	9.6
CVE-2026-11659	google - chrome	Integer overflow in UI in Google Chrome on Linux prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-09	9.6
CVE-2026-11671	google - chrome	Use after free in Navigation in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-09	9.6
CVE-2026-11697	google - chrome	Insufficient validation of untrusted input in UI in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-09	9.6
CVE-2026-42904	microsoft - multiple products	Heap-based buffer overflow in Windows TCP/IP allows an unauthorized attacker to elevate privileges over an adjacent network.	2026-06-09	9.6
CVE-2026-47281	microsoft - visual_studio_code	Improper input validation in Visual Studio Code allows an unauthorized attacker to elevate privileges over a network.	2026-06-09	9.6
CVE-2026-47928	adobe - multiple products	ColdFusion versions 2023.19, 2025.8 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. Scope is changed.	2026-06-09	9.6
CVE-2026-12027	google - chrome	Inappropriate implementation in Headless in Google Chrome prior to 149.0.7827.115 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)	2026-06-11	9.6
CVE-2026-47430	apache software foundation - Cordova Plugin InAppBrowser	## Summary The iOS implementation of `cordova-plugin-inappbrowser` passes the `id` field from a `WKScriptMessage` body to `commandDelegate sendPluginResult:callbackId:` with no format validation (`CDVWKInAppBrowser.m:560–574`). Any web content loaded inside the InAppBrowser can fire any pending Cordova callback in the host app by posting a message whose `id` field is a guessable or enumerated callback identifier. An attack abusing this weakness must be tailored to the specific plugins and callback IDs the host app uses. Though an attacker with knowledge of common Cordova plugin configurations could craft reusable payloads targeting widely-adopted plugins.	2026-06-08	9.5

		## Impact An unauthenticated remote attacker who controls content displayed in the InAppBrowser — via a URL the app opens (OAuth redirect, marketing link, deep-link target) or a network interception — can call `window.webkit.messageHandlers.cordova_iab.postMessage({id: '<victim-callback-id>', d: '...'})` to fire callbacks belonging to any other installed Cordova plugin (Camera, Contacts, File, Geolocation). Cordova callback IDs follow the predictable format `<PluginName><sequential-integer>`, making enumeration feasible. Successful exploitation allows the attacker to spoof plugin results across trust boundaries — for example, injecting a forged camera approval, a fabricated contacts list, or a crafted file-read response. This issue affects Cordova Plugin InAppBrowser: from 3.1.0 through 6.0.0. Users are recommended to upgrade to version 6.0.1, which fixes the issue.		
CVE-2026-44963	veeam - Backup and Replication	A vulnerability allowing remote code execution (RCE) on the Backup Server by an authenticated domain user.	2026-06-09	9.4
CVE-2026-11624	google - MCP Toolbox for Databases	The Model Context Protocol has a security warning advising servers to validate the "Origin" header on all incoming connections to prevent DNS rebinding attacks. Prior to the v0.25.0 release, users had no way to validate the origin's host. In v0.25.0, a new "--allowed-hosts" flag was introduced alongside the existing "--allowed-origins" flag, enabling users to specify permitted hosts at server startup. Both flags default to "*", allowing users to implement strict access controls as needed without breaking existing setups. If either flag is set to "*", the server will output a startup warning about potential vulnerabilities. Documentation has also been updated to highlight these security considerations.	2026-06-13	9.4
CVE-2026-46316	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: vgic-its: Drop the translation cache reference only for the erased entry vgic_its_invalidate_cache() walks the per-ITS translation cache with xa_for_each() and drops the cache's reference on each entry with vgic_put_irq(). It puts the iterated pointer, though, rather than the value returned by xa_erase(). The function is called from contexts that do not exclude one another: the ITS command handlers hold its_lock, the GITS_CTLR write path holds cmd_lock, and the path that clears EnableLPIs in a redistributor's GICR_CTLR holds neither. Two or more of them can drain the same cache concurrently, and if each one observes the same entry, erases it and then puts it, the single reference the cache holds on that entry is dropped more than once. The entry can then be freed while an ITE still maps it. xa_erase() is atomic and returns the previous entry, so put only the entry that this context actually removed. The cache reference is then dropped exactly once per entry even when the invalidations run concurrently, and the behavior is unchanged when only one context runs.	2026-06-09	9.3
CVE-2026-34691	adobe - multiple products	Adobe Experience Manager Forms JEE versions LTS SP1, 6.5.24.0 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field, potentially gaining elevated access or control over the victim's account or session. Scope is changed.	2026-06-09	9.3
CVE-2025-66276	qnap - qts	QuTS hero is not affected. We have already fixed the vulnerability in the following version: QTS 5.2.7.3256 build 20250913 and later	2026-06-10	9.2
CVE-2026-42535	apache - http_server	A path handling issue in mod_dav_fs in Apache 2.4.67 and earlier allows a WebDAV content author to directly manipulate trusted DAV property databases, potentially causing child process crashes. Users are recommended to upgrade to version 2.4.68, which fixes this issue.	2026-06-08	9.1
CVE-2026-34182	openssl - multiple products	Issue Summary: Cryptographic Message Services (CMS) processing fails to perform sufficient input validation on the cipher and tag length fields of AuthEnvelopedData containers, leading to various potential compromises. Impact Summary: Attackers making use of these vulnerabilities may achieve key-equivalent functionality for a given CMS recipient and/or bypass integrity validation for a given message. In one use case, an attacker may send a CMS message containing AuthEnvelopedData with the cipher specified as a non-AEAD cipher. OpenSSL erroneously allows this selection, and attempts to decrypt and validate the message. An on-path attacker who captures one legitimate AES-GCM AuthEnvelopedData addressed to the victim can re-emit it with the recipientInfos set left byte-for-byte intact, so the victim's private key still unwraps the genuine CEK (the content-encryption key), but with the inner OID rewritten to AES-256-OFB (Output Feedback Mode, an unauthenticated keystream mode) and with an attacker-chosen IV and ciphertext. The victim initializes AES-256-OFB under the real CEK, never consults the MAC field, and CMS_decrypt() returns success. If the application under attack responds to the attacker with any indicator	2026-06-09	9.1

		showing success or failure of the decryption effort, it is possible for the attacker to use this as an oracle to obtain key equivalent functionality for the CEK used for the chosen recipient of the message. In another use case, an attacker can reduce the tag length of the chosen AEAD cipher for a given AuthEnvelopedData container to be a single byte long, allowing an attacker to brute force CMS decryption, producing an integrity bypass for applications that trust CMS_decrypt() to reject modified content. The FIPS modules are not affected by this issue.		
CVE-2026-45602	microsoft - multiple products	No cwe for this issue in Windows DHCP Server allows an unauthorized attacker to perform tampering over a network.	2026-06-09	9.1
CVE-2026-50627	apache - multiple products	The JwtAccessTokenValidator class in Apache CXF fails to validate the 'aud' (Audience) claims of incoming JWT access tokens. This allows a JWT issued for one Resource Server to be successfully replayed against a completely different Resource Server, leading to Token Confusion/Routing attacks. Users are recommended to upgrade to versions 4.2.2 or 4.1.7, which fixes this issue.	2026-06-12	9.1
CVE-2026-11629	google - chrome	Use after free in Ozone in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2026-06-09	8.8
CVE-2026-11630	google - chrome	Use after free in File Input in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2026-06-09	8.8
CVE-2026-11633	google - chrome	Use after free in Bluetooth in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code via a malicious peripheral. (Chromium security severity: Critical)	2026-06-09	8.8
CVE-2026-11637	google - chrome	Use after free in Views in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-06-09	8.8
CVE-2026-11645	google - chrome	Out of bounds read and write in V8 in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11646	google - chrome	Use after free in ViewTransitions in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11648	google - chrome	Use after free in FullScreen in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11649	google - chrome	Use after free in V8 in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11650	google - chrome	Use after free in V8 in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11657	google - chrome	Use after free in Payments in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11662	google - chrome	Type Confusion in Bindings in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11664	google - chrome	Use after free in Payments in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11670	google - chrome	Use after free in PDF in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11673	google - chrome	Use after free in InterestGroups in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11674	google - chrome	Use after free in Guest View in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11680	google - chrome	Use after free in Media in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11681	google - chrome	Use after free in Ozone in Google Chrome on Linux prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11683	google - chrome	Use after free in WebCodecs in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11687	google - chrome	Use after free in Dawn in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11688	google - chrome	Inappropriate implementation in SVG in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11698	google - chrome	Use after free in Bluetooth in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-11699	google - chrome	Use after free in Bluetooth in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.8
CVE-2026-46317	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: Reassign nested_mmus array behind mmu_lock kvm->arch.nested_mmus[] is walked under kvm->mmu_lock, including from the MMU notifier path (kvm_unmap_gfn_range() -> kvm_nested_s2_unmap()), which can run at any time. kvm_vcpu_init_nested() reallocates the array and frees	2026-06-09	8.8

		the old buffer while holding only kvm->arch.config_lock, so such a walker can reference the freed array. Allocate the new array outside of mmu_lock, as the allocation can sleep. Under the lock, copy the existing entries, fix up the back pointers and reassign the array. Free the old buffer after dropping the lock, as kvfree() can sleep as well.		
CVE-2026-32193	microsoft - azure_kubernetes_service	Improper limitation of a pathname to a restricted directory ('path traversal') in Microsoft Azure Kubernetes Service allows an authorized attacker to execute code locally.	2026-06-09	8.8
CVE-2026-40371	microsoft - dynamics_365	Improper handling of insufficient permissions or privileges in Microsoft Dynamics 365 (on-premises) allows an authorized attacker to elevate privileges over a network.	2026-06-09	8.8
CVE-2026-42985	microsoft - multiple products	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	8.8
CVE-2026-45447	openssl - multiple products	Issue summary: A specially crafted PKCS#7 or S/MIME signed message could trigger a use-after-free during PKCS#7 signature verification. Impact summary: A use-after-free may result in process crashes, heap corruption, or potentially remote code execution. When processing a PKCS#7 or S/MIME signed message, if the SignedData digestAlgorithms field is present as an empty ASN.1 SET, OpenSSL may incorrectly free a caller-owned BIO during PKCS7_verify(). A subsequent use of the BIO by the calling application results in a use-after-free condition. In the common case this occurs when the application later calls BIO_free() on the BIO originally passed to PKCS7_verify(). Depending on allocator behavior and application-specific BIO usage patterns, this may result in a crash or other memory corruption. In some application contexts this may potentially be exploitable for remote code execution. Applications that process PKCS#7 or S/MIME signed messages using OpenSSL PKCS#7 APIs may be affected. Applications using the CMS APIs for this processing are not affected. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	2026-06-09	8.8
CVE-2026-45484	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to elevate privileges over a network.	2026-06-09	8.8
CVE-2026-45504	microsoft - multiple products	Server-side request forgery (ssrf) in Microsoft Exchange Server allows an authorized attacker to elevate privileges over a network.	2026-06-09	8.8
CVE-2026-45648	microsoft - multiple products	Stack-based buffer overflow in Active Directory Domain Services allows an authorized attacker to execute code over a network.	2026-06-09	8.8
CVE-2026-47289	microsoft - multiple products	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	8.8
CVE-2026-47653	microsoft - multiple products	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	8.8
CVE-2026-47932	adobe - multiple products	ColdFusion versions 2023.19, 2025.8 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 requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	8.8
CVE-2026-53435	jenkins - multiple products	In Jenkins 2.567 and earlier, LTS 2.555.2 and earlier, it is possible for attackers to have Jenkins deserialize arbitrary types defined in Jenkins core or plugins from an attacker-controlled `config.xml` submission in a way that allows them to handle HTTP requests afterwards. This can be used to impersonate any user and send HTTP requests on their behalf, up to and including use of the Script Console to run arbitrary code, or to read arbitrary files from the Jenkins controller.	2026-06-10	8.8
CVE-2026-44693	pi-hole - FTL	Pi-hole FTL is the core engine of the Pi-hole network-level advertisement and tracker blocker. Prior to version 6.6.1, Pi-hole FTL contains a race condition vulnerability in the HTTP session management subsystem, introduced with the v6.0 rewrite of the embedded CivetWeb-based web server. This issue has been patched in version 6.6.1.	2026-06-10	8.8
CVE-2026-47342	apache - ofbiz	A privilege escalation vulnerability in Apache OFBiz allows a low-privileged authenticated user to obtain higher privileges This issue affects Apache OFBiz: before 24.09.07. Users are recommended to upgrade to version 24.09.07, which fixes the issue.	2026-06-10	8.8
CVE-2026-50223	apache - ofbiz	Improper Control of Generation of Code ('Code Injection') vulnerability in Apache OFBiz allows a low-privileged authenticated user with Content/DataResource editing privileges to perform template injection attacks that could lead to Remote Code Execution. This issue affects Apache OFBiz: before 24.09.07. Users are recommended to upgrade to version 24.09.07, which fixes the issue.	2026-06-10	8.8

CVE-2026-7870	ibm - multiple products	IBM i 7.6, 7.5, 7.4, and 7.3 could allow a user to gain elevated privileges due to an unqualified library call. A malicious actor could cause user-controlled code to run with administrator privilege.	2026-06-11	8.8
CVE-2025-24284	apple - macos	This issue was addressed with improved checks to prevent unauthorized actions. This issue is fixed in macOS Sequoia 15.4. An app may be able to break out of its sandbox.	2026-06-11	8.8
CVE-2026-12007	google - chrome	Use after free in Core in Google Chrome on Windows prior to 149.0.7827.115 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-06-11	8.8
CVE-2026-12018	google - chrome	Inappropriate implementation in Mojo in Google Chrome on Windows prior to 149.0.7827.115 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: High)	2026-06-11	8.8
CVE-2026-12020	google - chrome	Use after free in Autofill in Google Chrome on Mac prior to 149.0.7827.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-11	8.8
CVE-2026-12035	google - chrome	Use after free in Views in Google Chrome on Windows prior to 149.0.7827.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-11	8.8
CVE-2026-41539	qnap - multiple products	A cross-site scripting (XSS) vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerability to bypass security mechanisms or read application data. We have already fixed the vulnerability in the following versions: QTS 5.2.9.3492 build 20260507 and later QuTS hero h5.2.9.3499 build 20260514 and later QuTS hero h5.3.4.3500 build 20260520 and later QuTS hero h6.0.0.3500 build 20260520 and later	2026-06-09	8.7
CVE-2026-44083	qnap - qumagie	An authorization bypass through user-controlled key vulnerability has been reported to affect QuMagie. The remote attackers can then exploit the vulnerability to gain unintended privileges. We have already fixed the vulnerability in the following version: QuMagie 2.9.1 and later	2026-06-09	8.7
CVE-2026-46746	siemens - multiple products	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 6). The application does not properly sanitize user input in the /api/sftp/uploadFiles endpoint, allowing the injection of shell command payloads via crafted directory names. These payloads are stored and executed when directory listings are retrieved. This could allow an authenticated remote attacker to execute arbitrary commands on the underlying operating system with the privileges of the affected service user (sinecins).	2026-06-09	8.7
CVE-2026-46748	siemens - multiple products	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 6). The affected system includes a binary that is configured with the cap_dac_override capability. This capability allows the process to bypass file system permission checks, resulting in unrestricted file system access. This could allow a local attacker to escalate privileges leading to arbitrary file modification and gaining root privileges on the system.	2026-06-09	8.7
CVE-2026-9740	mongodb - multiple products	A vulnerability in MongoDB Server's BSON validation logic allows an unauthenticated user to crash the mongod process by sending a specially crafted message. The BSON validator's handling of certain nested binary data structures permits uncontrolled mutual recursion between validation functions, where each re-entry resets internal depth tracking.	2026-06-09	8.7
CVE-2026-11933	mongodb - MongoDB	A use-after-free vulnerability exists in MongoDB Server's server-side JavaScript engine when converting BSON documents to JavaScript arrays. An authenticated user with read privileges who is able to run server-side JavaScript (for example, via $where or $function) can cause the server to access memory that has already been freed. This may result in disclosure of information from the mongod process memory or a denial of service through a server crash.	2026-06-12	8.7
CVE-2026-47906	adobe - dreamweaver	Dreamweaver Desktop versions 21.7 and earlier are affected by a Dependency on Vulnerable Third-Party Component vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	8.6
CVE-2025-66273	qnap - multiple products	A command injection vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to execute arbitrary commands. We have already fixed the vulnerability in the following versions: QTS 5.2.9.3410 build 20260214 and later QuTS hero h5.2.9.3410 build 20260214 and later QuTS hero h5.3.4.3500 build 20260520 and later QuTS hero h6.0.0.3397 build 20260206 and later	2026-06-10	8.6
CVE-2025-66279	qnap - multiple products	A command injection vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to execute arbitrary commands. We have already fixed the vulnerability in the following versions: QTS 5.2.9.3410 build 20260214 and later QuTS hero h5.2.9.3410 build 20260214 and later QuTS hero h5.3.4.3500 build 20260520 and later QuTS hero h6.0.0.3397 build 20260206 and later	2026-06-10	8.6
CVE-2026-22893	qnap - multiple products	A command injection vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to execute arbitrary commands. We have already fixed the vulnerability in the following versions: QTS 5.2.9.3410 build 20260214 and later QuTS hero h5.2.9.3410 build 20260214 and later	2026-06-10	8.6

		QuTS hero h5.3.4.3500 build 20260520 and later QuTS hero h6.0.0.3459 build 20260409 and later		
CVE-2026-24719	qnap - multiple products	A command injection vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to execute arbitrary commands. We have already fixed the vulnerability in the following versions: QTS 5.2.9.3492 build 20260507 and later QuTS hero h5.2.9.3499 build 20260514 and later	2026-06-10	8.6
CVE-2026-8637	lenovo - LanSchool Classic	A potential uncontrolled search path vulnerability was reported in the LanSchool Classic client application that could allow a local authenticated user to execute arbitrary code with elevated privileges.	2026-06-10	8.5
CVE-2026-9045	lenovo - Accessories and Display Manager for Enterprise	During an internal security assessment, a potential vulnerability was discovered in Lenovo Accessories and Display Manager for Enterprise for Windows that could allow a local authenticated user to execute arbitrary code with elevated privileges.	2026-06-10	8.5
CVE-2026-46288	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: of: unittest: fix use-after-free in of_unittest_changeset() The variable 'parent' is assigned the value of 'nchangeset' earlier in the function, meaning both point to the same struct device_node. The call to of_node_put(nchangeset) can decrement the reference count to zero and free the node if there are no other holders. After that, the code still uses 'parent' to check for the presence of a property and to read a string property, leading to a use-after-free. Fix this by moving the of_node_put() call after the last access to 'parent', avoiding the UAF.	2026-06-08	8.4
CVE-2026-46326	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: iio: pressure: mprls0025pa: fix spi_transfer struct initialisation Make sure that the spi_transfer struct is zeroed out before use.	2026-06-09	8.4
CVE-2026-41098	microsoft - azure_stack_edge	Improper neutralization of input during web page generation ('cross-site scripting') in Azure Stack Edge allows an authorized attacker to perform spoofing over a network.	2026-06-09	8.4
CVE-2026-44810	microsoft - multiple products	Improper authentication in Windows Cryptographic Services allows an unauthorized attacker to elevate privileges locally.	2026-06-09	8.4
CVE-2026-45456	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4
CVE-2026-45458	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4
CVE-2026-45461	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4
CVE-2026-45463	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4
CVE-2026-45472	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4
CVE-2026-45474	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4
CVE-2026-45482	microsoft - Microsoft Visual Studio Code CoPilot Chat Extension	Initialization of a resource with an insecure default in GitHub Copilot and Visual Studio Code allows an unauthorized attacker to disclose information over a network.	2026-06-09	8.4
CVE-2026-45607	microsoft - multiple products	Out-of-bounds read in Windows Hyper-V allows an unauthorized attacker to execute code locally.	2026-06-09	8.4
CVE-2026-45641	microsoft - multiple products	Out-of-bounds read in Windows Hyper-V allows an unauthorized attacker to execute code locally.	2026-06-09	8.4
CVE-2026-47635	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	8.4
CVE-2026-47929	adobe - multiple products	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. A high-privileged attacker could exploit this vulnerability to gain elevated access or control over the victim's account or session. Exploitation of this issue does not require user interaction. Scope is changed.	2026-06-09	8.4
CVE-2026-47931	adobe - multiple products	ColdFusion versions 2023.19, 2025.8 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. Scope is changed.	2026-06-09	8.4
CVE-2025-10237	lenovo - multiple products	During an internal security assessment, a potential vulnerability was discovered in some ThinkPad embedded controller firmware that could allow a privileged local user to perform arbitrary reads or writes to privileged memory regions.	2026-06-10	8.4
CVE-2025-10238	lenovo - multiple products	During an internal security assessment, a potential out-of-bounds write vulnerability was discovered in the BIOS of some ThinkPad products could allow a privileged local user to execute code in System Management Mode (SMM).	2026-06-10	8.4
CVE-2026-46307	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: wifi: ath5k: do not access array OOB	2026-06-08	8.3

		Vincent reports:
		> The ath5k driver seems to do an array-index-out-of-bounds access as
		> shown by the UBSAN kernel message:
		> UBSAN: array-index-out-of-bounds in drivers/net/wireless/ath/ath5k/base.c:1741:20
		> index 4 is out of range for type 'ieee80211_tx_rate [4]'
		> ...
		> Call Trace:
		> <TASK>
		> dump_stack_lvl+0x5d/0x80
		> ubsan_epilogue+0x5/0x2b
		> __ubsan_handle_out_of_bounds.cold+0x46/0x4b
		> ath5k_tasklet_tx+0x4e0/0x560 [ath5k]
		> tasklet_action_common+0xb5/0x1c0
		
		It is real. 'ts->ts_final_idx' can be 3 on 5212, so:
		info->status.rates[ts->ts_final_idx + 1].idx = -1;
		with the array defined as:
		struct ieee80211_tx_rate rates[IEEE80211_TX_MAX_RATES];
		while the size is:
		#define IEEE80211_TX_MAX_RATES 4
		is indeed bogus.
		
		Set this 'idx = -1' sentinel only if the array index is less than the
		array size. As mac80211 will not look at rates beyond the size
		(IEEE80211_TX_MAX_RATES).
		
		Note: The effect of the OOB write is negligible. It just overwrites the
		next member of info->status, i.e. ack_signal.		

CVE-2026-11631	google - chrome	Use after free in Aura in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-09	8.3
CVE-2026-11635	google - chrome	Use after free in Bluetooth in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-09	8.3
CVE-2026-11640	google - chrome	Integer overflow in libyuv in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-09	8.3
CVE-2026-11642	google - chrome	Use after free in Web Apps in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-09	8.3
CVE-2026-11647	google - chrome	Use after free in Printing in Google Chrome on Android prior to 149.0.7827.103 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)	2026-06-09	8.3
CVE-2026-11652	google - chrome	Use after free in Extensions in Google Chrome prior to 149.0.7827.103 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)	2026-06-09	8.3
CVE-2026-11655	google - chrome	Integer overflow in Media in Google Chrome on Mac prior to 149.0.7827.103 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)	2026-06-09	8.3
CVE-2026-11656	google - chrome	Use after free in ServiceWorker in Google Chrome prior to 149.0.7827.103 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. (Chromium security severity: High)	2026-06-09	8.3
CVE-2026-11660	google - chrome	Insufficient validation of untrusted input in New Tab Page in Google Chrome prior to 149.0.7827.103 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)	2026-06-09	8.3
CVE-2026-11661	google - chrome	Use after free in Views in Google Chrome on Windows prior to 149.0.7827.103 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)	2026-06-09	8.3
CVE-2026-11663	google - chrome	Use after free in Skia in Google Chrome prior to 149.0.7827.103 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)	2026-06-09	8.3
CVE-2026-11672	google - chrome	Heap buffer overflow in GPU in Google Chrome on Android prior to 149.0.7827.103 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)	2026-06-09	8.3
CVE-2026-11676	google - chrome	Insufficient validation of untrusted input in Dawn in Google Chrome on Linux and ChromeOS prior to 149.0.7827.103 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)	2026-06-09	8.3
CVE-2026-11677	google - chrome	Race in Network in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker who had compromised the network process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.3
CVE-2026-11679	google - chrome	Use after free in Codecs in Google Chrome on Windows prior to 149.0.7827.103 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)	2026-06-09	8.3
CVE-2026-11682	google - chrome	Inappropriate implementation in Views in Google Chrome on Linux prior to 149.0.7827.103 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)	2026-06-09	8.3
CVE-2026-11692	google - chrome	Use after free in Read Anything in Google Chrome prior to 149.0.7827.103 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)	2026-06-09	8.3

CVE-2026-11700	google - chrome	Use after free in Tracing in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-09	8.3
CVE-2026-12008	google - chrome	Use after free in DigitalCredentials in Google Chrome prior to 149.0.7827.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-11	8.3
CVE-2026-12009	google - chrome	Insufficient validation of untrusted input in Accessibility in Google Chrome on Mac prior to 149.0.7827.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-11	8.3
CVE-2026-12010	google - chrome	Heap buffer overflow in GPU in Google Chrome on Android prior to 149.0.7827.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-11	8.3
CVE-2026-12011	google - chrome	Use after free in WebMIDI in Google Chrome on Windows prior to 149.0.7827.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-11	8.3
CVE-2026-12014	google - chrome	Use after free in Cast in Google Chrome prior to 149.0.7827.115 allowed an attacker on the local network segment to potentially perform a sandbox escape via malicious network traffic. (Chromium security severity: High)	2026-06-11	8.3
CVE-2026-12016	google - chrome	Inappropriate implementation in DevTools in Google Chrome prior to 149.0.7827.115 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)	2026-06-11	8.3
CVE-2026-12019	google - chrome	Heap buffer overflow in Codecs in Google Chrome on Linux and ChromeOS prior to 149.0.7827.115 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)	2026-06-11	8.3
CVE-2026-12022	google - chrome	Race in Safe Browsing in Google Chrome on Mac prior to 149.0.7827.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a malicious file. (Chromium security severity: High)	2026-06-11	8.3
CVE-2026-12023	google - chrome	Use after free in GPU in Google Chrome on Mac prior to 149.0.7827.115 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)	2026-06-11	8.3
CVE-2026-12028	google - chrome	Use after free in GPU in Google Chrome on Android prior to 149.0.7827.115 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)	2026-06-11	8.3
CVE-2026-12029	google - chrome	Use after free in Video in Google Chrome on Windows prior to 149.0.7827.115 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)	2026-06-11	8.3
CVE-2026-12030	google - chrome	Out of bounds write in GPU in Google Chrome on Android prior to 149.0.7827.115 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)	2026-06-11	8.3
CVE-2026-12031	google - chrome	Inappropriate implementation in Views in Google Chrome on Windows prior to 149.0.7827.115 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)	2026-06-11	8.3
CVE-2026-12034	google - chrome	Insufficient validation of untrusted input in Linux Toolkit Theming in Google Chrome on Linux prior to 149.0.7827.115 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a malicious file. (Chromium security severity: High)	2026-06-11	8.3
CVE-2026-46303	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: isofs: validate Rock Ridge CE continuation extent against volume size rock_continue() reads rs->cont_extent verbatim from the Rock Ridge CE record and passes it to sb_bread() without checking that the block number is within the mounted ISO 9660 volume. commit e595447e177b ("[PATCH] rock.c: handle corrupted directories") added cont_offset and cont_size rejection for the CE continuation but did not validate the extent block number itself. commit f54e18f1b831 ("isofs: Fix infinite looping over CE entries") later capped the CE chain length at RR_MAX_CE_ENTRIES = 32 but again left the block number unchecked. With a crafted ISO mounted via udisks2 (desktop optical auto-mount) or via CAP_SYS_ADMIN mount, rs->cont_extent can therefore point at an out-of-range block or at blocks belonging to an adjacent filesystem on the same block device. sb_bread() on an out-of-range block returns NULL cleanly via the block layer EIO path, so there is no memory-safety violation. For in-range reads of adjacent-filesystem data, the CE buffer is parsed as Rock Ridge records and only the text of SL sub-records reaches userspace through readlink(), which makes the info-leak channel narrow and difficult to exploit; still, rejecting the malformed CE outright matches the rejection shape already present in the same function for cont_offset and cont_size. Add an ISOFS_SB(sb)->s_nzones bounds check to rock_continue() next to the existing offset/size rejection, printing the same corrupted-directory-entry notice.	2026-06-08	8.2
CVE-2026-24349	siemens - multiple products	A vulnerability has been identified in SIMATIC WinCC Unified PC Runtime V16 (All versions), SIMATIC WinCC Unified PC Runtime V17 (All versions), SIMATIC WinCC Unified PC Runtime V18 (All versions), SIMATIC WinCC Unified PC Runtime V19 (All versions), SIMATIC WinCC Unified PC Runtime V20 (All versions), SIMATIC WinCC Unified PC Runtime V21 (All versions < V21 Update 2). Insufficient	2026-06-09	8.2

		protection of key material in WinCC Certificate Manager that could allow an attacker to extract sensitive information.		
CVE-2026-44822	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information over a network.	2026-06-09	8.2
CVE-2026-45476	microsoft - Linux kernel - Microsoft MANA Network Driver	Use after free in Linux MANA Driver allows an authorized attacker to elevate privileges locally.	2026-06-09	8.2
CVE-2026-47652	microsoft - multiple products	Out-of-bounds read in Windows Hyper-V allows an unauthorized attacker to execute code locally.	2026-06-09	8.2
CVE-2026-47907	adobe - dreamweaver	Dreamweaver Desktop versions 21.7 and earlier are affected by an Improper Access Control vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	8.2
CVE-2026-9742	mongodb - multiple products	When OIDC authentication is enabled in configuration, clients may set specific values in the "mechanism" parameter of the "authenticate" command that lead to server crash. The authenticate command is accessible to unauthenticated clients, leading to pre-auth denial-of-service in affected product configurations.	2026-06-09	8.2
CVE-2026-11643	google - chrome	Use after free in Proxy in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: Critical)	2026-06-09	8.1
CVE-2026-11689	google - chrome	Insufficient policy enforcement in Passwords in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.1
CVE-2026-11693	google - chrome	Inappropriate implementation in Plugins in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	2026-06-09	8.1
CVE-2026-42835	microsoft - teams	Improper neutralization of special elements in output used by a downstream component ('injection') in Microsoft Teams for Android allows an authorized attacker to disclose information over a network.	2026-06-09	8.1
CVE-2026-42974	microsoft - multiple products	Integer underflow (wrap or wraparound) in Windows Performance Monitor allows an unauthorized attacker to execute code over a network.	2026-06-09	8.1
CVE-2026-42981	microsoft - multiple products	Integer underflow (wrap or wraparound) in Windows Performance Monitor allows an unauthorized attacker to execute code over a network.	2026-06-09	8.1
CVE-2026-42987	microsoft - multiple products	Use after free in Windows Deployment Services allows an unauthorized attacker to execute code over a network.	2026-06-09	8.1
CVE-2026-45503	microsoft - multiple products	Server-side request forgery (ssrf) in Microsoft Exchange Server allows an authorized attacker to disclose information over a network.	2026-06-09	8.1
CVE-2026-45599	microsoft - multiple products	Use after free in Universal Plug and Play (upnp.dll) allows an unauthorized attacker to execute code over a network.	2026-06-09	8.1
CVE-2026-45635	microsoft - multiple products	Use after free in Universal Plug and Play (upnp.dll) allows an unauthorized attacker to execute code over a network.	2026-06-09	8.1
CVE-2026-47631	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	2026-06-09	8.1
CVE-2026-7383	openssl - multiple products	Issue summary: A signed integer overflow when sizing the destination buffer for Unicode output in ASN1_mbstring_ncopy() can lead to a heap buffer overflow. Impact summary: A heap buffer overflow may lead to a crash or possibly attacker controlled code execution or other undefined behaviour. In ASN1_mbstring_copy() and ASN1_mbstring_ncopy() the destination size for Unicode output is computed in a signed int: by left shift of the input character count for BMPSTRING (UTF-16) and UNIVERSALSTRING (UTF-32), and by summing per-character byte counts for UTF8STRING. The calculation overflows when the input reaches around 2^30 characters. In the worst case (UNIVERSALSTRING at 2^30 characters) the size wraps to zero, OPENSSL_malloc(1) is called, and the subsequent character copy writes several gigabytes past the one-byte allocation. X.509 certificate processing routes through ASN1_STRING_set_by_NID(), whose DIRSTRING_TYPE mask excludes UNIVERSALSTRING and whose per-NID size limits cap the input length; no network protocol or certificate-handling path in OpenSSL exercises the overflow. Triggering the bug requires an application that calls ASN1_mbstring_copy() or ASN1_mbstring_ncopy() directly, or registers a custom string type via ASN1_STRING_TABLE_add(), with attacker-controlled input on the order of half a gigabyte or more. For these reasons this issue was assigned Low severity. The FIPS modules in 4.0, 3.6, 3.5, 3.4 and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	2026-06-09	8.1
CVE-2026-47930	adobe - multiple products	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized read and write access. Exploitation of this issue does not require user interaction.	2026-06-09	8.1
CVE-2026-45062	php - frankenphp	FrankenPHP is a modern application server for PHP. From version 1.11.2 to before version 1.12.3, the splitPos() function in cgi.go misuses golang.org/x/text/search with search.IgnoreCase when the	2026-06-10	8.1

		request path contains a non-ASCII byte. Two distinct flaws in that fallback let an attacker mislead FrankenPHP into treating a non-.php file as a .php script. In any deployment where the attacker can place content into a file served by FrankenPHP (uploads, file storage, etc.), this can be escalated to remote code execution by crafting a URL whose path triggers either flaw. This issue has been patched in version 1.12.3.		
CVE-2026-41699	vmware - multiple products	Spring for GraphQL applications are vulnerable to Unsafe Deserialization when processing paginated GraphQL queries. An attacker can craft a malicious GraphQL request that can lead to Remote Code Execution when the application exposes a paginated (Connection) field and the classpath contains specific classes that can be leveraged during deserialization. Affected versions: Spring for GraphQL 2.0.0 through 2.0.3; 1.4.0 through 1.4.5; 1.3.0 through 1.3.8.	2026-06-11	8.1
CVE-2026-41700	vmware - multiple products	Spring for GraphQL applications that have enabled the WebSocket transport are vulnerable to Cross-Site WebSocket Hijacking. An attacker can trick an authenticated user into visiting a malicious page, allowing the attacker to execute arbitrary GraphQL operations with the victim's credentials. Affected versions: Spring for GraphQL 2.0.0 through 2.0.3; 1.4.0 through 1.4.5; 1.3.0 through 1.3.8; 1.0.0 through 1.0.6.	2026-06-11	8.1
CVE-2026-12012	google - chrome	Use after free in Network in Google Chrome prior to 149.0.7827.115 allowed an attacker in a privileged network position to potentially exploit heap corruption via malicious network traffic. (Chromium security severity: High)	2026-06-11	8.1
CVE-2026-50632	apache - multiple products	A further incomplete fix for a previous advisory CVE-2026-44417 (Untrusted JMS configuration can lead to RCE) for Apache CXF has been identified, which can allow code execution capabilities, if untrusted users are allowed to configure JMS for Apache CXF. Users are recommended to upgrade to versions 4.2.2 or 4.1.7, which fixes this issue.	2026-06-12	8.1
CVE-2026-50633	apache - multiple products	A JNDI Injection vulnerability has been discovered in Apache CXF's JCA integration module, which can allow for code execution, if an attacker is able to manipulate the JCA deployment descriptor (ra.xml) or runtime activation parameters. Users are recommended to upgrade to versions 4.2.2 or 4.1.7, which fixes this issue.	2026-06-12	8.1
CVE-2026-53408	zoom - multiple products	Improper Authorization in Handler for Custom URL Scheme in Zoom Workplace before version 7.0.4 for Android and before 7.0.3 for iOS may allow an unauthenticated user to conduct an escalation of privilege via network access.	2026-06-12	8.1
CVE-2026-41722	vmware - multiple products	VMware Cloud Foundation Operations contains multiple stored cross-site scripting vulnerabilities.A malicious actor with privileges to create policies, views or text-widgets may be able to inject scripts to perform administrative actions in VMware Cloud Foundation Operations.	2026-06-08	8
CVE-2026-41723	vmware - multiple products	VMware Cloud Foundation Operations contains multiple stored cross-site scripting vulnerabilities.A malicious actor with privileges to create policies, views or text-widgets may be able to inject scripts to perform administrative actions in VMware Cloud Foundation Operations.	2026-06-08	8
CVE-2026-41724	vmware - multiple products	VMware Cloud Foundation Operations contains multiple stored cross-site scripting vulnerabilities.A malicious actor with privileges to create policies, views or text-widgets may be able to inject scripts to perform administrative actions in VMware Cloud Foundation Operations.	2026-06-08	8
CVE-2026-46332	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: greybus: gb-beagleplay: bound bootloader receive buffering cc1352_bootloader_rx() appends each serdev chunk into the fixed rx_buffer before parsing bootloader packets. The helper can keep leftover bytes between callbacks and may receive multiple packets in one callback, so a single count value is not constrained by one packet length. Check that the incoming chunk fits in the remaining receive buffer space before memcpy(). If it does not, drop the staged data and consume the bytes instead of overflowing rx_buffer.	2026-06-09	8
CVE-2026-45644	microsoft - live_share_canvas	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Live Share Canvas SDK allows an authorized attacker to elevate privileges over a network.	2026-06-09	8
CVE-2026-47298	microsoft - multiple products	Improper authorization in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-06-09	8
CVE-2026-34693	adobe - multiple products	Adobe Experience Manager Forms JEE versions LTS SP1, 6.5.24.0 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. Exploit depends on conditions beyond the attacker's control. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page. Scope is changed.	2026-06-09	8
CVE-2026-45588	microsoft - multiple products	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9
CVE-2026-45654	microsoft - multiple products	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9
CVE-2026-47656	microsoft - multiple products	Protection mechanism failure in Windows Boot Manager allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9
CVE-2026-48568	microsoft - multiple products	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9
CVE-2026-48570	microsoft - multiple products	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9
CVE-2026-48573	microsoft - multiple products	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9
CVE-2026-48575	microsoft - multiple products	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9

CVE-2026-48576	microsoft - multiple products	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9
CVE-2026-48578	microsoft - multiple products	Protection mechanism failure in Windows Secure Boot allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.9
CVE-2026-46274	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: io-wq: check that the predecessor is hashed in io_wq_remove_pending() io_wq_remove_pending() needs to fix up wq->hash_tail[] if the cancelled work was the tail of its hash bucket. When doing this, it checks whether the preceding entry in acct->work_list has the same hash value, but never checks that the predecessor is hashed at all. io_get_work_hash() is simply atomic_read(&work->flags) >> IO_WQ_HASH_SHIFT, and the hash bits are never set for non-hashed work, so it returns 0. Thus, when a hashed bucket-0 work is cancelled while a non-hashed work is its list predecessor, the check spuriously passes and a pointer to the non-hashed io_kiocb is stored in wq->hash_tail[0]. Because non-hashed work is dequeued via the fast path in io_get_next_work(), which never touches hash_tail[], the stale pointer is never cleared. Therefore, after the non-hashed io_kiocb completes and is freed back to req_cachep, wq->hash_tail[0] is a dangling pointer. The io_wq is per-task (tctx->io_wq) and survives ring open/close, so the dangling pointer persists for the lifetime of the task; the next hashed bucket-0 enqueue dereferences it in io_wq_insert_work() and wq_list_add_after() writes through freed memory. Add the missing io_wq_is_hashed() check so a non-hashed predecessor never inherits a hash_tail[] slot.	2026-06-08	7.8
CVE-2026-46275	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: hci_uart: fix UAFs and race conditions in close and init paths Vulnerabilities leading to Use-After-Free (UAF) and Null Pointer Dereference (NPD) conditions were observed in the lifecycle management of hci_uart. The primary issue arises because the workqueues (init_ready and write_work) are only flushed/cancelled if the HCI_UART_PROTO_READY flag is set during TTY close. If a hangup occurs before setup completes, hci_uart_tty_close() skips the teardown of these workqueues and proceeds to free the `hu` struct. When the scheduled work executes later, it blindly dereferences the freed `hu` struct. Furthermore, several data races and UAFs were identified in the teardown sequence: 1. Calling hci_uart_flush() from hci_uart_close() without effectively disabling write_work causes a race condition where both can concurrently double-free hu->tx_skb. This happens because protocol timers can concurrently invoke hci_uart_tx_wakeup() and requeue write_work. 2. Calling hci_free_dev(hdev) before hu->proto->close(hu) causes a UAF when vendor specific protocol close callbacks dereference hu->hdev. 3. In the initialization error paths, failing to take the proto_lock write lock before clearing PROTO_READY leads to races with active readers. Additionally, hci_uart_tty_receive() accesses hu->hdev outside the read lock, leading to UAFs if the initialization error path frees hdev concurrently. Fix these synchronization and lifecycle issues by: 1. Re-ordering hci_uart_tty_close() to clear HCI_UART_PROTO_READY first, followed immediately by a cancel_work_sync(&hu->write_work). Clearing the flag locks out concurrent protocol timers from successfully invoking hci_uart_tx_wakeup(), effectively rendering the cancellation permanent and preventing the tx_skb double-free. 2. Note: Clearing PROTO_READY early causes hci_uart_close() to skip hu->proto->flush(). This is perfectly safe in the tty_close path because hu->proto->close() executes shortly after, which intrinsically purges all protocol SKB queues and tears down the state. 3. Relocating hu->proto->close(hu) strictly prior to hci_free_dev(hdev) across all close and error paths to prevent vendor-level UAFs. 4. Moving the hdev->stat.byte_rx increment in hci_uart_tty_receive() inside the proto_lock read-side critical section to safely synchronize with device unregistration. 5. Adding cancel_work_sync(&hu->write_work) to hci_uart_close() to safely flush the workqueue before hci_uart_flush() is invoked via the HCI core. 6. Utilizing cancel_work_sync() instead of disable_work_sync() across all paths to prevent permanently breaking user-space retry capabilities.	2026-06-08	7.8
CVE-2026-46277	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: mm/zone_device: do not touch device folio after calling ->folio_free()	2026-06-08	7.8

		The contents of a device folio can immediately change after calling ->folio_free(), as the folio may be reallocated by a driver with a different order. Instead of touching the folio again to extract the pgmap, use the local stack variable when calling percpu_ref_put_many().		
CVE-2026-46280	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: lib: test_hmm: evict device pages on file close to avoid use-after-free Patch series "Minor hmm_test fixes and cleanups". Two bugfixes a cleanup for the HMM kernel selftests. These were mostly reported by Zenghui Yu with special thanks to Lorenzo for analysing and pointing out the problems. This patch (of 3): When dmirror_fops_release() is called it frees the dmirror struct but doesn't migrate device private pages back to system memory first. This leaves those pages with a dangling zone_device_data pointer to the freed dmirror. If a subsequent fault occurs on those pages (eg. during coredump) the dmirror_devmem_fault() callback dereferences the stale pointer causing a kernel panic. This was reported [1] when running mm/ksft_hmm.sh on arm64, where a test failure triggered SIGABRT and the resulting coredump walked the VMAs faulting in the stale device private pages. Fix this by calling dmirror_device_evict_chunk() for each devmem chunk in dmirror_fops_release() to migrate all device private pages back to system memory before freeing the dmirror struct. The function is moved earlier in the file to avoid a forward declaration.	2026-06-08	7.8
CVE-2026-46311	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/amdgpu/userq: fix access to stale wptr mapping Use drm_exec to take both locks i.e vm root bo and wptr_obj bo to access the mapping data properly. This fixes the security issue of unmap the wptr_obj while a queue creation is in progress and passing other bo at same address. (cherry picked from commit 1fc6c8ab45dbee096469c08c13f6099d57a52d6c)	2026-06-08	7.8

CVE-2026-46319	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved:
		
		net/sched: act_ct: Only release RCU read lock after ct_ft
		
		When looking up a flow table in act_ct in tcf_ct_flow_table_get(), rhashtable_lookup_fast() internally opens and closes an RCU read critical section before returning ct_ft.
		The tcf_ct_flow_table_cleanup_work() can complete before refcount_inc_not_zero() is invoked on the returned ct_ft resulting in a UAF on the already freed ct_ft object. This vulnerability can lead to privilege escalation.
		
		Analysis from zdi-disclosures@trendmicro.com:
		When initializing act_ct, tcf_ct_init() is called, which internally triggers tcf_ct_flow_table_get().
		
		static int tcf_ct_flow_table_get(struct net *net, struct tcf_ct_params *params)
		
		{
		struct zones_ht_key key = { .net = net, .zone = params->zone };
		struct tcf_ct_flow_table *ct_ft;
		int err = -ENOMEM;
		
		mutex_lock(&zones_mutex);
		ct_ft = rhashtable_lookup_fast(&zones_ht, &key, zones_params); // [1]
		if (ct_ft && refcount_inc_not_zero(&ct_ft->ref)) // [2]
		goto out_unlock;
		...
		}
		
		static __always_inline void *rhashtable_lookup_fast(
		struct rhashtable *ht, const void *key,
		const struct rhashtable_params params)
		{
		void *obj;
			2026-06-09	7.8

		rcu_read_lock();
		obj = rhashtable_lookup(ht, key, params);
		rcu_read_unlock();
		
		return obj;
		}
		
		At [1], rhashtable_lookup_fast() looks up and returns the corresponding ct_ft from zones_ht . The lookup is performed within an RCU read critical section through rcu_read_lock() / rcu_read_unlock(), which prevents the object from being freed. However, at the point of function return, rcu_read_unlock() has already been called, and there is nothing preventing ct_ft from being freed before reaching refcount_inc_not_zero(&ct_ft->ref) at [2]. This interval becomes the race window, during which ct_ft can be freed.
		
		Free Process:
		
		tcf_ct_flow_table_put() is executed through the path tcf_ct_cleanup() call_rcu() tcf_ct_params_free_rcu() tcf_ct_params_free() tcf_ct_flow_table_put().
		
		static void tcf_ct_flow_table_put(struct tcf_ct_flow_table *ct_ft)
		{
		if (refcount_dec_and_test(&ct_ft->ref)) {
		rhashtable_remove_fast(&zones_ht, &ct_ft->node, zones_params);
		INIT_RCU_WORK(&ct_ft->rwork, tcf_ct_flow_table_cleanup_work); // [3]
		queue_rcu_work(act_ct_wq, &ct_ft->rwork);
		}
		}
		
		At [3], tcf_ct_flow_table_cleanup_work() is scheduled as RCU work
		
		static void tcf_ct_flow_table_cleanup_work(struct work_struct *work)
		
		{
		struct tcf_ct_flow_table *ct_ft;
		struct flow_block *block;
		
		ct_ft = container_of(to_rcu_work(work), struct tcf_ct_flow_table,
		rwork);
		nf_flow_table_free(&ct_ft->nf_ft);
		block = &ct_ft->nf_ft.flow_block;
		down_write(&ct_ft->nf_ft.flow_block_lock);
		WARN_ON(!list_empty(&block->cb_list));
		up_write(&ct_ft->nf_ft.flow_block_lock);
		kfree(ct_ft); // [4]
		
		module_put(THIS_MODULE);
		}
		
		tcf_ct_flow_table_cleanup_work() frees ct_ft at [4]. When this function executes between [1] and [2], UAF occurs.
		
		This race condition has a very short race window, making it generally difficult to trigger. Therefore, to trigger the vulnerability an msleep(100) was inserted after[1]		

CVE-2026-46323	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: gro: don't merge zcopy skbs skb_gro_receive() can currently copy frags between the source and GRO skb, without checking the zerocopy status, and in particular the SKBFL_MANAGED_FRAG_REFS flag. When SKBFL_MANAGED_FRAG_REFS is set, the skb doesn't hold a reference on the pages in shinfo->frags. Appending those frags to another skb's frags without fixing up the page refcount can lead to UAF. When either the last skb in the GRO chain (the one we would append frags to) or the source skb is zerocopy, don't merge the skbs.	2026-06-09	7.8
CVE-2026-46324	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_tables: use list_del_rcu for netlink hooks nft_netdev_unregister_hooks and __nft_unregister_flowtable_net_hooks need to use list_del_rcu(), this list can be walked by concurrent dumpers. Add a new helper and use it consistently.	2026-06-09	7.8
CVE-2026-46327	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: dm: fix unlocked test for dm_suspended_md	2026-06-09	7.8

		The function dm_blk_report_zones tests if the device is suspended with the "dm_suspended_md" call. However, this function is called without holding any locks, so the device may be suspended just after it. Move the call to dm_suspended_md after dm_get_live_table, so that the device can't be suspended after the suspended state was tested.		
CVE-2026-46330	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: Revert "net/smc: Introduce TCP ULP support" This reverts commit d7cd421da9da2cc7b4d25b8537f66db5c8331c40. As reported by Al Viro, the TCP ULP support for SMC is fundamentally broken. The implementation attempts to convert an active TCP socket into an SMC socket by modifying the underlying `struct file`, dentry, and inode in-place, which violates core VFS invariants that assume these structures are immutable for an open file, creating a risk of use after free errors and general system instability. Given the severity of this design flaw and the fact that cleaner alternatives (e.g., LD_PRELOAD, BPF) exist for legacy application transparency, the correct course of action is to remove this feature entirely.	2026-06-09	7.8
CVE-2026-52907	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: media: rockchip: rkcif: fix off by one bugs Change these comparisons from > vs >= to avoid accessing one element beyond the end of the arrays. While at it, use ARRAY_SIZE instead of the _MAX enum values. [fix cosmetic issues]	2026-06-09	7.8
CVE-2026-33828	microsoft - multiple products	Trust boundary violation in Windows Attestation allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-40404	microsoft - multiple products	Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability	2026-06-09	7.8
CVE-2026-40409	microsoft - multiple products	Windows Universal Disk Format File System Driver (UDFS) Elevation of Privilege Vulnerability	2026-06-09	7.8
CVE-2026-41092	microsoft - multiple products	Improper access control in Microsoft Kinect allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-42828	microsoft - multiple products	Buffer over-read in Windows Projected File System Filter Driver allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-42829	microsoft - multiple products	Improper access control in Windows Administrator Protection allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.8
CVE-2026-42837	microsoft - multiple products	Buffer over-read in Windows Projected File System Filter Driver allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-42902	microsoft - powertoys	Improper authorization in Microsoft PowerToys allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-42905	microsoft - multiple products	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-42910	microsoft - multiple products	Out-of-bounds write in Windows Hotpatch Monitoring Service allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-42916	microsoft - multiple products	Integer underflow (wrap or wraparound) in Windows NT OS Kernel allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-42977	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.	2026-06-09	7.8
CVE-2026-42978	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.	2026-06-09	7.8
CVE-2026-42979	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.	2026-06-09	7.8
CVE-2026-42980	microsoft - multiple products	Integer underflow (wrap or wraparound) in Windows NT OS Kernel allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-42983	microsoft - multiple products	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-42986	microsoft - multiple products	Use after free in Microsoft Graphics Component allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-42989	microsoft - multiple products	Improper link resolution before file access ('link following') in Winlogon allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-42991	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.	2026-06-09	7.8
CVE-2026-44802	microsoft - multiple products	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-44803	microsoft - multiple products	Integer overflow or wraparound in Windows Win32K - GRFX allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-44804	microsoft - multiple products	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-44807	microsoft - multiple products	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8

CVE-2026-44808	microsoft - multiple products	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-44809	microsoft - multiple products	Use after free in Windows Common Log File System Driver allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-44811	microsoft - multiple products	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-44812	microsoft - multiple products	Integer overflow or wraparound in Windows Win32K - GRFX allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-44813	microsoft - multiple products	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-44817	microsoft - multiple products	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-44819	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-44820	microsoft - multiple products	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-44823	microsoft - multiple products	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-44824	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-45457	microsoft - multiple products	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-45469	microsoft - multiple products	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-45471	microsoft - multiple products	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-45475	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-45486	microsoft - multiple products	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-45487	microsoft - multiple products	Time-of-check time-of-use (TOCTOU) race condition in Program Compatibility Assistant Service allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-45490	microsoft - multiple products	Improper authorization in .NET allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-45586	microsoft - multiple products	Improper link resolution before file access ('link following') in Windows Collaborative Translation Framework allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-45592	microsoft - multiple products	Integer overflow or wraparound in Windows Internet (wininet.dll) allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-45593	microsoft - multiple products	Use after free in Windows SDK allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-45600	microsoft - multiple products	Access of resource using incompatible type ('type confusion') in Windows Kernel-Mode Drivers allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-45605	microsoft - multiple products	Use after free in Windows Bluetooth Service allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-45636	microsoft - multiple products	Heap-based buffer overflow in Windows NTFS allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-45637	microsoft - multiple products	Use after free in Windows DWM Core Library allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-45638	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-45643	microsoft - multiple products	Untrusted pointer dereference in Microsoft Office Word allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-45645	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-45656	microsoft - multiple products	Protection mechanism failure in Windows UEFI allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.8
CVE-2026-45658	microsoft - multiple products	Protection mechanism failure in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2026-06-09	7.8
CVE-2026-47292	microsoft - visual_studio_code	Inclusion of functionality from untrusted control sphere in Visual Studio Code allows an unauthorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-48565	microsoft - windows_narrator_braille	Untrusted search path in Windows Narrator Braille allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-48574	microsoft - multiple products	Heap-based buffer overflow in Windows Media allows an unauthorized attacker to execute code locally.	2026-06-09	7.8
CVE-2026-48583	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-49161	microsoft - pc_manager	Improper access control in Microsoft PC Manager allows an authorized attacker to bypass a security feature locally.	2026-06-09	7.8
CVE-2026-34695	adobe - multiple products	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-34696	adobe - multiple products	InDesign Desktop versions 21.3, 20.5.3 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.	2026-06-09	7.8
CVE-2026-34697	adobe - multiple products	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8

CVE-2026-34698	adobe - multiple products	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-34699	adobe - multiple products	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-34700	adobe - multiple products	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-34701	adobe - multiple products	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-34702	adobe - multiple products	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-34706	adobe - multiple products	InCopy versions 21.3, 20.5.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-34707	adobe - multiple products	InCopy versions 21.3, 20.5.3 and earlier are affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-34708	adobe - multiple products	InCopy versions 21.3, 20.5.3 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-48293	adobe - multiple products	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-50511	microsoft - pc_manager	Improper link resolution before file access ('link following') in Microsoft PC Manager allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-50512	microsoft - pc_manager	Improper link resolution before file access ('link following') in Microsoft PC Manager allows an authorized attacker to elevate privileges locally.	2026-06-09	7.8
CVE-2026-34709	adobe - substance_3d_sampler	Substance3D - Sampler versions 6.0.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-34710	adobe - substance_3d_sampler	Substance3D - Sampler versions 6.0.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-47908	adobe - dreamweaver	Dreamweaver Desktop versions 21.7 and earlier are affected by an Access of Uninitialized Pointer 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.	2026-06-09	7.8
CVE-2026-48305	adobe - substance_3d_sampler	Substance3D - Sampler versions 6.0.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-48306	adobe - substance_3d_sampler	Substance3D - Sampler versions 6.0.0 and earlier are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-47911	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-09	7.8
CVE-2026-47912	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-09	7.8
CVE-2026-47913	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-09	7.8
CVE-2026-47914	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-09	7.8
CVE-2026-47915	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-09	7.8
CVE-2026-47916	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-09	7.8
CVE-2026-47917	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-09	7.8
CVE-2026-47918	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-09	7.8
CVE-2026-47919	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-09	7.8
CVE-2026-47920	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-09	7.8
CVE-2026-47921	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-09	7.8

CVE-2026-47952	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-09	7.8
CVE-2026-47955	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-09	7.8
CVE-2026-47959	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Stack-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	7.8
CVE-2026-48291	adobe - format_plugins	Format Plugins versions 1.1.2 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.	2026-06-09	7.8
CVE-2026-48292	adobe - format_plugins	Format Plugins versions 1.1.2 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.	2026-06-09	7.8
CVE-2025-31272	apple - macos	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4. An app may be able to bypass launch constraint protections and execute malicious code with elevated privileges.	2026-06-11	7.8
CVE-2026-47965	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 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.	2026-06-12	7.8
CVE-2026-54228	red hat - multiple products	A time-of-check time-of-use (TOCTOU) race condition was found in the abrt-dbus D-Bus service's SetElement method. Between dump directory creation and post-create event execution, any local user can call SetElement to write arbitrary text files into the root-owned dump directory, bypassing package validation and allowing crashes of unpackaged binaries to survive post-create processing.	2026-06-13	7.8
CVE-2026-52906	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: 9p: fix access mode flags being ORed instead of replaced Since commit 1f3e4142c0eb ("9p: convert to the new mount API"), v9fs_apply_options() applies parsed mount flags with |= onto flags already set by v9fs_session_init(). For 9P2000.L, session_init sets V9FS_ACCESS_CLIENT as the default, so when the user mounts with "access=user", both bits end up set. Access mode checks compare against exact values, so having both bits set matches neither mode. This causes v9fs_fid_lookup() to fall through to the default switch case, using INVALID_UID (nobody/65534) instead of current_fsuid() for all fid lookups. Root is then unable to chown or perform other privileged operations. Fix by clearing the access mask before applying the user's choice.	2026-06-09	7.7
CVE-2026-41003	vmware - multiple products	An attacker able to influence values in RelyingPartyRegistration may be able to run arbitrary code on HTML forms generated by Spring Security filters. Affected versions: Spring Security 5.7.0 through 5.7.23; 5.8.0 through 5.8.25; 6.3.0 through 6.3.16; 6.4.0 through 6.4.16; 6.5.0 through 6.5.10; 7.0.0 through 7.0.5.	2026-06-10	7.6
CVE-2026-11774	red hat - multiple products	An integer overflow flaw was found in the SASL I/O layer of 389 Directory Server (389-ds-base). In sasl_io_start_packet(), adding sizeof(uint32_t) to a crafted SASL packet length prefix of 0xFFFFFFFC causes unsigned wraparound to zero, bypassing the nsslapd-maxsasliosize limit and leading to a heap buffer overflow of up to approximately 2 megabytes of attacker-controlled data. After a successful SASL bind with integrity protection (SSF > 0), a remote attacker can cause a Denial of Service (DoS) or achieve Remote Code Execution (RCE). In FreeIPA and Red Hat Identity Management deployments, any domain user with a valid Kerberos ticket, enrolled host, or service account can trigger this vulnerability over the network. This flaw is independent of CVE-2025-14905, which patched schema.c only and did not modify sasl_io.c.	2026-06-11	7.6
CVE-2026-3238	red hat - multiple products	A flaw was found in Samba's WINS server component when running as an Active Directory Domain Controller. The WINS protocol handlers for certain request types did not properly validate incoming packets, allowing an unauthenticated remote attacker to trigger a NULL pointer dereference and crash the WINS service using specially crafted UDP packets.	2026-06-08	7.5
CVE-2026-34355	apache - http_server	A buffer overflow in mod_proxy_html in Apache HTTP Server 2.4.67 and earlier allows an attack by an untrusted backend. Users are recommended to upgrade to version 2.4.68, which fixes this issue.	2026-06-08	7.5
CVE-2026-34356	apache - http_server	Heap-based Buffer Overflow vulnerability in Apache HTTP Server with malicious backend servers and ProxyPassReverseCookie* This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	2026-06-08	7.5
CVE-2026-42536	apache - http_server	Heap-based Buffer Overflow vulnerability in Apache HTTP Server with mod_xml2enc, xml2StartParse, and untrusted content This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	2026-06-08	7.5

CVE-2026-49975	apache - multiple products	Memory Allocation with Excessive Size Value vulnerability in Apache HTTP Server's mod_http leads to denial of service via malicious HTTP requests. This issue affects Apache HTTP Server: from 2.4.17 through 2.4.67.	2026-06-08	7.5
CVE-2026-46304	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: nvmet: avoid recursive nvmet-wq flush in nvmet_ctrl_free nvmet_tcp_release_queue_work() runs on nvmet-wq and can drop the final controller reference through nvmet_cq_put(). If that triggers nvmet_ctrl_free(), the teardown path flushes ctrl->async_event_work on the same nvmet-wq. Call chain: nvmet_tcp_schedule_release_queue() kref_put(&queue->kref, nvmet_tcp_release_queue) nvmet_tcp_release_queue() queue_work(nvmet_wq, &queue->release_work) <--- nvmet_wq process_one_work() nvmet_tcp_release_queue_work() nvmet_cq_put(&queue->nvme_cq) nvmet_cq_destroy() nvmet_ctrl_put(cq->ctrl) nvmet_ctrl_free() flush_work(&ctrl->async_event_work) <--- nvmet_wq Previously Scheduled by :- nvmet_add_async_event queue_work(nvmet_wq, &ctrl->async_event_work); This trips lockdep with a possible recursive locking warning. [5223.015876] run blktests nvme/003 at 2026-04-07 20:53:55 [5223.061801] loop0: detected capacity change from 0 to 2097152 [5223.072206] nvmet: adding nsid 1 to subsystem blktests-subsystem-1 [5223.088368] nvmet_tcp: enabling port 0 (127.0.0.1:4420) [5223.126086] nvmet: Created discovery controller 1 for subsystem nqn.2014-08.org.nvmexpress.discovery for NQN nqn.2014-08.org.nvmexpress:uuid:0f01fb42-9f7f-4856-b0b3-51e60b8de349. [5223.128453] nvme nvme1: new ctrl: NQN "nqn.2014-08.org.nvmexpress.discovery", addr 127.0.0.1:4420, hostnqn: nqn.2014-08.org.nvmexpress:uuid:0f01fb42-9f7f-4856-b0b3-51e60b8de349 [5233.199447] nvme nvme1: Removing ctrl: NQN "nqn.2014-08.org.nvmexpress.discovery" [5233.227718] == [5233.231283] WARNING: possible recursive locking detected [5233.234696] 7.0.0-rc3nvme+ #20 Tainted: G O N [5233.238434] -- [5233.241852] kworker/u192:6/2413 is trying to acquire lock: [5233.245429] ffff888111632548 ((wq_completion)nvmet-wq){+.+.}-{0:0}, at: touch_wq_lockdep_map+0x26/0x90 [5233.251438] but task is already holding lock: [5233.255254] ffff888111632548 ((wq_completion)nvmet-wq){+.+.}-{0:0}, at: process_one_work+0x5cc/0x6e0 [5233.261125] other info that might help us debug this: [5233.265333] Possible unsafe locking scenario: [5233.269217] CPU0 [5233.270795] ---- [5233.272436] lock((wq_completion)nvmet-wq); [5233.275241] lock((wq_completion)nvmet-wq); [5233.278020] *** DEADLOCK *** [5233.281793] May be due to missing lock nesting notation [5233.286195] 3 locks held by kworker/u192:6/2413: [5233.289192] #0: ffff888111632548 ((wq_completion)nvmet-wq){+.+.}-{0:0}, at: process_one_work+0x5cc/0x6e0 [5233.294569] #1: ffffc9000e2a7e40 ((work_completion)(&queue->release_work)){+.+.}-{0:0}, at: process_one_work+0x1c5/0x6e0 [5233.300128] #2: ffffffff82d7dc40 (rcu_read_lock){....}-{1:3}, at: __flush_work+0x62/0x530 [5233.304290] stack backtrace: [5233.306520] CPU: 4 UID: 0 PID: 2413 Comm: kworker/u192:6 Tainted: G O N 7.0.0-rc3nvme+ #20 PREEMPT(full) [5233.306524] Tainted: [O]=OOT_MODULE, [N]=TEST	2026-06-08	7.5

		[5233.306525] Hardware name: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.17.0-0-gb52ca86e094d-prebuilt.qemu.org 04/01/2014 [5233.306527] Workqueue: nvmet-wq nvmet_tcp_release_queue_work [nvmet_tcp] [5233.306532] Call Trace: [5233.306534] <TASK> [5233.306536] dump_stack_lvl+0x73/0xb0 [5233.306552] print_deadlock_bug+0x225/0x2f0 [5233.306556] __lock_acquire+0x13f0/0x2290 [5233.306563] lock_acquire+0xd0/0x300 [5233.306565] ? touch_wq_lockdep_map+0x26/0x90 [5233.306571] ? __flush_work+0x20b/0x530 [5233.306573] ? touch_wq_lockdep_map+0x26/0x90 [5233.306577] touch_wq_lockdep_map+0x3b/0x90 [5233.306580] ? touch_wq_lockdep_map+0x26/0x90 [52 ---truncated---		
CVE-2026-46306	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: flow_dissector: do not dissect PPPoE PFC frames RFC 2516 Section 7 states that Protocol Field Compression (PFC) is NOT RECOMMENDED for PPPoE. In practice, pppd does not support negotiating PFC for PPPoE sessions, and the flow dissector driver has assumed an uncompressed frame until the blamed commit. During the review process of that commit [1], support for PFC is suggested. However, having a compressed (1-byte) protocol field means the subsequent PPP payload is shifted by one byte, causing 4-byte misalignment for the network header and an unaligned access exception on some architectures. The exception can be reproduced by sending a PPPoE PFC frame to an ethernet interface of a MIPS board, with RPS enabled, even if no PPPoE session is active on that interface: $ 0 : 00000000 80c40000 00000000 85144817 $ 4 : 00000008 00000100 80a75758 81dc9bb8 $ 8 : 00000010 8087ae2c 0000003d 00000000 $12 : 000000e0 00000039 00000000 00000000 $16 : 85043240 80a75758 81dc9bb8 00006488 $20 : 0000002f 00000007 85144810 80a70000 $24 : 81d1bda0 00000000 $28 : 81dc8000 81dc9aa8 00000000 805ead08 Hi : 00009d51 Lo : 2163358a epc : 805e91f0 __skb_flow_dissect+0x1b0/0x1b50 ra : 805ead08 __skb_get_hash_net+0x74/0x12c Status: 11000403 KERNEL EXL IE Cause : 40800010 (ExcCode 04) BadVA : 85144817 PrId : 0001992f (MIPS 1004Kc) Call Trace: [<805e91f0>] __skb_flow_dissect+0x1b0/0x1b50 [<805ead08>] __skb_get_hash_net+0x74/0x12c [<805ef330>] get_rps_cpu+0x1b8/0x3fc [<805fca70>] netif_receive_skb_list_internal+0x324/0x364 [<805fd120>] napi_complete_done+0x68/0x2a4 [<8058de5c>] mtk_napi_rx+0x228/0xfec [<805fd398>] __napi_poll+0x3c/0x1c4 [<805fd754>] napi_threaded_poll_loop+0x234/0x29c [<805fd848>] napi_threaded_poll+0x8c/0xb0 [<80053544>] kthread+0x104/0x12c [<80002bd8>] ret_from_kernel_thread+0x14/0x1c Code: 02d51821 1060045b 00000000 <8c640000> 3084000f 2c820005 144001a2 00042080 8e220000 To reduce the attack surface and maintain performance, do not process PPPoE PFC frames. [1] https://lore.kernel.org/r/20220630231016.GA392@debian.home	2026-06-08	7.5
CVE-2026-11632	google - chrome	Use after free in TabStrip in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-06-09	7.5
CVE-2026-11636	google - chrome	Use after free in Autofill in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2026-06-09	7.5
CVE-2026-11639	google - chrome	Use after free in Compositing in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-06-09	7.5

CVE-2026-11641	google - chrome	Use after free in Bluetooth in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-06-09	7.5
CVE-2026-11644	google - chrome	Use after free in Views in Google Chrome on Linux prior to 149.0.7827.103 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. (Chromium security severity: Critical)	2026-06-09	7.5
CVE-2026-11667	google - chrome	Out of bounds read in WebRTC in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the GPU process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-09	7.5
CVE-2026-11690	google - chrome	Out of bounds read and write in Media in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-09	7.5
CVE-2026-11694	google - chrome	Use after free in ServiceWorker in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-09	7.5
CVE-2026-41006	vmware - multiple products	Spring HATEOAS's internal PropertyUtils.createObjectFromProperties method, used by the Collection+JSON and UBER media type deserializers, performs bean property binding via reflection without consulting Jackson access-control annotations. Affected versions: Spring HATEOAS 1.5.0 through 1.5.6; 2.3.0 through 2.3.4; 2.4.0 through 2.4.1; 2.5.0 through 2.5.2; 3.0.0 through 3.0.3.	2026-06-09	7.5
CVE-2026-41007	vmware - multiple products	Spring HATEOAS maintains an unbounded static cache of StringLinkRelation instances keyed on attacker-supplied strings. Affected versions: Spring HATEOAS 1.5.0 through 1.5.6; 2.3.0 through 2.3.4; 2.4.0 through 2.4.1; 2.5.0 through 2.5.2; 3.0.0 through 3.0.3.	2026-06-09	7.5
CVE-2026-41842	vmware - multiple products	Spring MVC and WebFlux applications are vulnerable to Denial of Service (DoS) attacks when resolving static resources. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	7.5
CVE-2026-41849	vmware - spring_framework	An integer overflow vulnerability exists in the evaluation logic of the Spring Expression Language (SpEL). An attacker can exploit this by supplying a specially crafted SpEL expression that triggers excessive resource consumption, resulting in a Denial of Service (DoS). Affected versions: Spring Framework 5.3.0 through 5.3.48.	2026-06-09	7.5
CVE-2026-41850	vmware - multiple products	Applications that evaluate user-supplied Spring Expression Language (SpEL) expressions are vulnerable to an Algorithmic Denial of Service (DoS). By providing a specially crafted expression, an attacker can trigger excessive resource consumption during evaluation, leading to application degradation or unavailability. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	7.5
CVE-2026-34180	openssl - multiple products	Issue summary: Parsing a crafted DER-encoded ASN.1 structure with a primitive element whose content exceeds 2 gigabytes in length may cause a heap buffer over-read on 64-bit Unix and Unix-like platforms. Impact summary: The heap buffer over-read may crash the application (Denial of Service) or to load into the decoded ASN.1 object contents of memory beyond the end of the input buffer. More typically such ASN.1 elements would instead be truncated. An integer truncation in OpenSSL's ASN.1 decoder causes the content length of an ASN.1 primitive element to be mishandled when it exceeds 2 gigabytes. In the worst case the truncated length is treated as a request to scan the binary content for a terminating zero byte, possibly causing OpenSSL to read either less than or beyond the end of the allocated buffer. Applications that pass attacker-supplied data to d2i_X509(), d2i_PKCS7(), or any other d2i_* decoding function are affected. OpenSSL's own command-line tools are not vulnerable, as data read through the BIO layer is checked before it reaches the affected code. The issue only affects 64-bit Unix and Unix-like platforms; 32-bit platforms and 64-bit Windows are not affected. The FIPS modules in 4.0, 3.6, 3.5, 3.4 and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	2026-06-09	7.5
CVE-2026-34183	openssl - multiple products	Issue summary: Remote peer may exhaust heap memory of the QUIC server or client by flooding it with packets containing PATH_CHALLENGE frames. Impact summary: A malicious remote peer can cause an unbounded memory allocation which can lead to an abnormal termination of the application acting as a QUIC client or server and a Denial of Service.	2026-06-09	7.5

		A remote peer may exhaust heap memory by flooding the local QUIC stack with PATH_CHALLENGE frames. The local QUIC stack allocates a PATH_RESPONSE frame for every PATH_CHALLENGE it receives. The allocated PATH_RESPONSE frame gets freed only when the remote peer acknowledges reception of the PATH_RESPONSE frame which will not be done by a malicious peer. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are not affected by this issue. The QUIC stack is outside of OpenSSL FIPS module boundary.		
CVE-2026-40376	microsoft - visual_studio_code	Improper input validation in Visual Studio Code allows an unauthorized attacker to elevate privileges over a network.	2026-06-09	7.5
CVE-2026-42764	openssl - multiple products	Issue summary: Receiving a QUIC initial packet with an invalid token may trigger a NULL pointer dereference in the OpenSSL QUIC server with address validation disabled. Impact summary: NULL pointer dereference typically causes abnormal termination of the affected QUIC server process and a Denial of Service. If the address validation is disabled in the OpenSSL QUIC server implementation, an attacker can crash the server by sending an initial packet with an invalid or expired token. By default, the client address validation is enabled in the OpenSSL QUIC server implementation, which makes the default configuration not vulnerable to this issue. However if the SSL_LISTENER_FLAG_NO_VALIDATE is used with the SSL_new_listener() call, the address validation is disabled making the vulnerable code reachable. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	2026-06-09	7.5
CVE-2026-42765	openssl - multiple products	Issue summary: When a partial-chain certificate verification is enabled together with OCSP response checking for the whole chain, a NULL dereference will happen if the verified chain does not have a self-signed trusted anchor, crashing the process. Impact summary: A NULL pointer dereference can trigger a crash which leads to a Denial of Service for an application. When performing OCSP response checking for certificates in the verification chain, the code always tries to access the next certificate as the issuer. There is a check for a self-signed certificate. However with the partial chain verification enabled when the chain does not have a self-signed trusted anchor, the issuer will be NULL for the last certificate in the chain. A NULL pointer dereference then happens. This issue affects only applications which enable both OCSP verification of the certificate chain (X509_V_FLAG_OCSP_RESP_CHECK_ALL) and partial chain verification (X509_V_FLAG_PARTIAL_CHAIN) in the certificate verification. Both flags are disabled by default. For that reason, we have assigned Low severity to the issue. No FIPS modules are affected by this issue as the affected code is outside the OpenSSL FIPS module boundary.	2026-06-09	7.5
CVE-2026-42908	microsoft - multiple products	Out-of-bounds read in Windows RDP allows an unauthorized attacker to disclose information over a network.	2026-06-09	7.5
CVE-2026-42909	microsoft - multiple products	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5
CVE-2026-42913	microsoft - multiple products	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5
CVE-2026-42992	microsoft - multiple products	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5
CVE-2026-42993	microsoft - multiple products	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5
CVE-2026-44799	microsoft - multiple products	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5
CVE-2026-44801	microsoft - multiple products	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5
CVE-2026-45445	openssl - multiple products	Issue summary: When an application drives an AES-OCB context through the public EVP_Cipher() one-shot interface, the application-supplied initialisation vector (IV) is silently discarded. Impact summary: Every message encrypted under the same key uses the same effective nonce regardless of the IV supplied by the caller, resulting in (key, nonce) reuse and loss of confidentiality. If the same code path is used to compute the authentication tag, the tag depends only on the (key, IV) pair and not on the plaintext or ciphertext, allowing universal forgery of arbitrary ciphertext from a	2026-06-09	7.5

		single captured message. OpenSSL provides two ways to drive a cipher: the documented streaming interface (EVP_CipherUpdate / EVP_CipherFinal_ex) and a lower-level one-shot, EVP_Cipher(), whose documentation explicitly recommends against use by applications in favour of EVP_CipherUpdate() and EVP_CipherFinal_ex(). The OCB provider's streaming handler flushes the application-supplied IV into the OCB context before processing data; the one-shot handler did not. Every call to EVP_Cipher() on an AES-OCB context therefore ran with the all-zero key-derived offset state left by cipher initialisation, regardless of the caller's IV. If EVP_EncryptFinal_ex() is subsequently used to obtain the authentication tag, the deferred IV setup runs at that point and clears the running checksum that should have been accumulated over the plaintext. The resulting tag is a function of (key, IV) only and verifies against any ciphertext produced under the same (key, IV) pair. The OpenSSL SSL/TLS implementation is not affected: AES-OCB is not a TLS cipher suite, and libssl does not call EVP_Cipher() in any case. Applications that drive AES-OCB through the documented streaming AEAD API (EVP_CipherUpdate / EVP_CipherFinal_ex) are not affected. Only applications that combine the AES-OCB cipher with the EVP_Cipher() one-shot API are vulnerable. The FIPS modules in 4.0, 3.6, 3.5, 3.4 and 3.0 are not affected by this issue, as AES-OCB is outside the OpenSSL FIPS module boundary.		
CVE-2026-45583	microsoft - multiple products	Improper control of generation of code ('code injection') in Microsoft Exchange Server allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5
CVE-2026-45591	microsoft - multiple products	Uncontrolled resource consumption in ASP.NET Core allows an unauthorized attacker to deny service over a network.	2026-06-09	7.5
CVE-2026-45639	microsoft - multiple products	Out-of-bounds read in Windows RDP allows an unauthorized attacker to disclose information over a network.	2026-06-09	7.5
CVE-2026-47654	microsoft - multiple products	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5
CVE-2026-48563	microsoft - multiple products	Heap-based buffer overflow in Remote Desktop Client allows an unauthorized attacker to execute code over a network.	2026-06-09	7.5
CVE-2026-49160	microsoft - multiple products	Uncontrolled resource consumption in HTTP/2 allows an unauthorized attacker to deny service over a network.	2026-06-09	7.5
CVE-2026-9076	openssl - multiple products	Issue summary: When CMS password-based decryption (RFC 3211 / PWRI key unwrap) processes attacker-supplied CMS data, an attacker-chosen stream-mode KEK cipher can trigger a heap out-of-bounds read in kek_unwrap_key(). Impact summary: A heap buffer over-read may trigger a crash which leads to Denial of Service for an application if the input buffer ends at a memory page boundary and the following page is unmapped. There is no information disclosure as the over-read bytes are not revealed to the attacker. The key unwrapping function performs a check-byte test as specified in the RFC that reads 7 bytes from a heap allocation that is based on the wrapped key length from the message. There is a minimum length check based on the block length of the wrapping cipher. However the cipher is selected from an OID carried in the attacker's PWRI keyEncryptionAlgorithm with no requirement that the cipher be a block cipher. When an attacker selects a stream-mode cipher the guard will be ineffective and the allocated buffer containing the unwrapped key can be too small to fit the check-bytes specified in the RFC and a buffer over-read can happen. Applications calling CMS_decrypt() or CMS_decrypt_set1_password() (equivalently openssl cms -decrypt -pwri_password ...) on untrusted CMS data are vulnerable to this issue. No password knowledge is required: the over-read happens during the unwrap attempt before any authentication succeeds. The over-read is limited to a few bytes and is not written to output, so there is no information disclosure. Triggering a crash requires the allocation to border unmapped memory, which is unlikely with the normal allocator. The FIPS modules are not affected by this issue.	2026-06-09	7.5
CVE-2026-11799	mozilla - multiple products	UXSS in Focus for iOS / Klar Webkit navigation. This vulnerability was fixed in Focus for iOS 151.3.1 and Klar for iOS 151.3.1.	2026-06-09	7.5
CVE-2026-34711	adobe - multiple products	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Integer Overflow or Wraparound vulnerability. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-06-09	7.5
CVE-2026-34712	adobe - multiple products	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Improper Input Validation vulnerability. An attacker could exploit this vulnerability to crash the	2026-06-09	7.5

		application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.		
CVE-2026-34713	adobe - multiple products	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Uncontrolled Resource Consumption vulnerability. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-06-09	7.5
CVE-2026-40988	vmware - multiple products	An application using spring-security-saml2-service-provider and the REDIRECT binding for SAML 2.0 Login or Logout may be vulnerable to a denial of service by way of an unbounded writer that inflates the compressed SAML payload into memory. Affected versions: Spring Security 5.7.0 through 5.7.23; 5.8.0 through 5.8.25; 6.3.0 through 6.3.16; 6.4.0 through 6.4.16; 6.5.0 through 6.5.10; 7.0.0 through 7.0.5.	2026-06-10	7.5
CVE-2026-1220	google - chrome	Race in V8 in Google Chrome prior to 144.0.7559.99 allowed a remote attacker to potentially exploit type confusion via a crafted HTML page. (Chromium security severity: High)	2026-06-10	7.5
CVE-2026-6893	red hat - multiple products	A flaw was found in dracut. A remote attacker on the adjacent network can exploit this vulnerability by providing specially crafted DHCP (Dynamic Host Configuration Protocol) options, such as a malicious hostname, to a system using dracut's legacy DHCP path. These options are improperly handled and written into temporary shell scripts without proper escaping, leading to command injection. This allows the attacker to achieve root code execution within the initramfs, potentially compromising the system's boot and network behavior.	2026-06-10	7.5
CVE-2026-41856	vmware - multiple products	The Spring GraphQL annotation detection mechanism for @Controller data fetchers may not correctly resolve annotations on methods within type hierarchies. This can be an issue if such annotations are used for authorization decisions. When all conditions are met, security annotations can be ignored at runtime. Affected versions: Spring for GraphQL 2.0.0 through 2.0.3; 1.4.0 through 1.4.5; 1.3.0 through 1.3.8; 1.0.0 through 1.0.6.	2026-06-11	7.5
CVE-2025-46315	apple - macos	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Tahoe 26.1. An app may be able to access protected user data.	2026-06-11	7.5
CVE-2026-50645	apache - multiple products	There is no restriction on the amount of attachment headers that a message can contain when being deserialized by Apache CXF, which can lead to uncontrolled resource consumption or a denial of service attack. Users are recommended to upgrade to versions 4.2.2 or 4.1.7, which fix this issue by imposing a maximum default of 500 attachments per message.	2026-06-12	7.5
CVE-2026-4870	ibm - multiple products	IBM Qiskit SDK 0.43.0 through 2.5.0 could allow an attacker to trigger a segmentation fault leading to a denial of service due to uncontrolled recursion in the parser.	2026-06-12	7.5
CVE-2026-46320	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: tap: free page on error paths in tap_get_user_xdp() tap_get_user_xdp() rejects a frame shorter than ETH_HLEN with -EINVAL, and returns -ENOMEM when build_skb() fails. Both paths jump to the err label without freeing the page that vhost_net_build_xdp() allocated for the frame. tap_sendmsg() discards the per-buffer return value and always returns 0, so vhost_tx_batch() takes the success path and never frees the page; each rejected frame in a batch leaks one page-frag chunk. Free the page on both error paths, before the skb is built. This is the tap counterpart of the same leak in tun_xdp_one().	2026-06-09	7.4
CVE-2026-34181	openssl - multiple products	Issue Summary: The PKCS#12 file processing fails to perform sufficient input validation for files that use Password-Based Message Authentication Code 1 (PBMAC1) integrity mechanism allowing a certificate and private key forgery. Impact Summary: An attacker impersonating a user can cause a service reading PKCS#12 files to accept forged certificates and private keys with a 1 in 256 probability. If a service accepting PKCS#12 files is using passwords for authenticating the received files, the attacker can create unencrypted PKCS#12 files that use PBMAC1 authentication that specifies an HMAC key of only one byte, allowing them to craft a file that will be accepted with a 1 in 256 probability. That would then cause the service to accept a certificate and private key controlled by the attacker. The FIPS modules are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	2026-06-09	7.4
CVE-2026-47937	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an Uncontrolled Search Path Element vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	7.4
CVE-2026-47960	adobe - multiple products	ColdFusion versions 2023.19, 2025.8 and earlier are affected by an Improper Restriction of XML External Entity Reference ('XXE') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	7.4
CVE-2026-50631	apache - multiple products	A race condition in AbstractOAuthDataProvider allows concurrent requests using the same Refresh Token to bypass single-use semantics and generate multiple valid Access Tokens, when 'recycleRefreshTokens' is set to false. A leaked refresh token can be replayed concurrently by	2026-06-12	7.4

		multiple attackers or threads. Users are recommended to upgrade to versions 4.2.2 or 4.1.7, which fixes this issue.		
CVE-2026-44185	apache - http_server	Buffer Over-read vulnerability in Apache HTTP Server via outbound OCSP requests to an attacker controlled OCSP server This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	2026-06-08	7.3
CVE-2026-44186	apache - http_server	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in the mod_proxy_ftp module in Apache HTTP Server with an attacker controlled backend FTP server. This issue affects undefined: from 2.4.0 through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	2026-06-08	7.3
CVE-2026-48913	apache - http_server	Use After Free vulnerability in Apache HTTP Server module mod_http2 when file handles are already exhausted. This issue affects Apache HTTP Server: from 2.4.55 through 2.4.67.	2026-06-08	7.3
CVE-2026-46328	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: apparmor: fix rlimit for posix cpu timers Posix cpu timers requires an additional step beyond setting the rlimit. Refactor the code so its clear when what code is setting the limit and conditionally update the posix cpu timers when appropriate.	2026-06-09	7.3
CVE-2026-45481	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.	2026-06-09	7.3
CVE-2026-47634	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.	2026-06-09	7.3
CVE-2026-40993	vmware - spring_security	An attacker with write permissions to the database table managed by JdbcAssertingPartyMetadataRepository (saml2_asserting_party_metadata) may be able to store malicious serialized payloads in the columns containing the collection of verification or encryption credentials (verification_credentials and encryption_credentials, respectively). Affected versions: Spring Security 7.0.0 through 7.0.5.	2026-06-10	7.3
CVE-2026-11837	red hat - multiple products	A local privilege escalation vulnerability was found in the ansible.posix authorized_key module. The module's keyfile() function uses os.chown() instead of os.lchown() and opens files without O_NOFOLLOW when managing SSH authorized keys. An unprivileged local user can pre-stage symbolic links in their ~/.ssh directory to redirect file ownership changes to arbitrary system paths when an operator runs the authorized_key task as root, leading to local privilege escalation.	2026-06-10	7.3
CVE-2026-6090	lenovo - Smart Connect	A potential authentication bypass was reported in Lenovo Smart Connect for Windows that could allow a local authenticated user to execute arbitrary code with elevated privileges.	2026-06-10	7.3
CVE-2026-11577	red hat - multiple products	A flaw was found in Keycloak. A limited administrator can exploit an improper access control vulnerability in the POST /admin/realms/{realm}/partialImport endpoint. This allows them to bypass Fine-Grained Admin Permissions (FGAP) and escalate their privileges to a full realm administrator by importing users with realm-admin role mappings.	2026-06-08	7.2
CVE-2026-10727	ivanti - Endpoint Manager Mobile	An OS command injection vulnerability in Ivanti EPMM before 12.9.0.1, 12.8.0.3 and 12.7.0.2 versions allows a remote authenticated attacker to execute arbitrary commands as root	2026-06-09	7.2
CVE-2026-9753	mongodb - multiple products	The $_internalApplyOplogUpdate aggregation pipeline stage can be used to execute a document diff containing a malformed binary diff to return memory out-of-bounds or crash the server. $_internalApplyOplogUpdate can be executed by any authenticated user with access to the aggregate command.	2026-06-09	7.2
CVE-2026-25700	apache - answer	Improper Restriction of Security Token Assignment vulnerability in Apache Answer. This issue affects Apache Answer: through 2.0.0. Previously issued administrative tokens were not invalidated after an administrator account was suspended, deleted, or deactivated, allowing continued access to administrative APIs until the token expired. Users are recommended to upgrade to version 2.0.1, which fixes the issue.	2026-06-10	7.2
CVE-2026-42306	docker - multiple products	Moby is an open source container framework. In Docker Engine prior to version 29.5.1, Docker Daemon versions 28.5.2 and prior, and Moby Daemon prior to version 2.0.0-beta.14, a race condition during docker cp mount setup allows a malicious container to redirect a bind mount target to an arbitrary host path, potentially overwriting host files or causing denial of service. This issue has been patched in Docker Engine version 29.5.1 and Moby Daemon version 2.0.0-beta.14.	2026-06-12	7.2
CVE-2026-41845	vmware - multiple products	Due to incorrect escaping, the use of JavaScriptUtils.javaScriptEscape() may lead to JavaScript code injection in the browser, potentially resulting in a cross-site scripting (XSS) vulnerability. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	7.1
CVE-2026-46321	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: tun: free page on short-frame rejection in tun_xdp_one() tun_xdp_one() returns -EINVAL on a frame shorter than ETH_HLEN without freeing the page that vhost_net_build_xdp() allocated for it. tun_sendmsg() discards that -EINVAL and still returns total_len, so	2026-06-09	7.1

		vhost_tx_batch() takes the success path and never frees the page; each short frame in a batch leaks one page-frag chunk. A local process that can open /dev/net/tun and /dev/vhost-net can hit this path: it attaches a tun/tap device as the vhost-net backend and feeds TX descriptors whose length minus the virtio-net header is below ETH_HLEN. Each kick leaks the page-frag chunks for that batch, and a tight submission loop exhausts host memory and triggers an OOM panic. Free the page before returning -EINVAL, matching the XDP-program error path in the same function.		
CVE-2026-46322	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: tun: free page on build_skb failure in tun_xdp_one() When build_skb() fails in tun_xdp_one(), the function sets ret to -ENOMEM and jumps to the out label, which returns without freeing the page that vhost_net_build_xdp() allocated for the frame. As with the short-frame rejection path, tun_sendmsg() discards the per-buffer error and still returns total_len, so vhost_tx_batch() takes the success path and never frees the page. Each build_skb() failure in a batch leaks one page-frag chunk. Free the page before taking the error path, matching the put_page() the other error exits of tun_xdp_one() already perform.	2026-06-09	7.1
CVE-2026-45649	microsoft - multiple products	Improper access control in Office for Android allows an unauthorized attacker to perform spoofing locally.	2026-06-09	7.1
CVE-2026-47288	microsoft - multiple products	Integer overflow or wraparound in Windows Kerberos allows an authorized attacker to execute code over an adjacent network.	2026-06-09	7.1
CVE-2026-48569	microsoft - visual_studio_code	Improper input validation in Visual Studio Code allows an unauthorized attacker to bypass a security feature locally.	2026-06-09	7.1
CVE-2026-9741	mongodb - multiple products	A bug in query analysis processing of the $vectorSearch aggregation stage for Queryable Encryption (QE) or Client-Side Field Level Encryption (CSFLE) results in literal values for encrypted fields within the $vectorSearch stage filter expressions to be sent to the server as plaintext instead of ciphertext.	2026-06-09	7.1
CVE-2026-9743	mongodb - mongodb	In MongoDB Server 8.0, an aggregation stage can leave its _subPipeline field null during processing of certain pipelines. If a getMore is subsequently issued on the same cursor, the server may dereference this null sub-pipeline when reattaching to the operation context, accessing an invalid address and crashing the process. This issue allows an authenticated user who can run aggregation pipelines to cause a denial of service by issuing a specially crafted aggregation followed by getMore on affected versions.	2026-06-09	7.1
CVE-2026-9746	mongodb - multiple products	When using $changestreams and $_requestReshardingResumeToken with the exchange option the server hits an invariant which causes the server to crash. There are no special privileges needed. The user must be logged in to issue the statement.	2026-06-09	7.1
CVE-2026-9747	mongodb - multiple products	Adding fromRouter:true and runtimeConstants.userRoles could cause aggregations to crash mongodb server.	2026-06-09	7.1
CVE-2026-9748	mongodb - multiple products	The $_internalConvertBucketIndexStats stage used PauseExecution as a way to signal "skip this document" when an index stats conversion failed. But PauseExecution is not a general purpose skip mechanism, but rather a TeeBuffer-internal signal used solely by $facet to coordinate its sub-pipelines. When this stage is placed before $facet in a pipeline, TeeBuffer receives the unexpected PauseExecution from upstream and hits a hard invariant assertion, crashing mongod.	2026-06-09	7.1
CVE-2026-9749	mongodb - multiple products	This issue can occur when running an aggregation pipeline that uses the internal $exchange stage configured with key-range partitioning and order-preserving delivery. If a single key range produces enough documents to fill its exchange buffer (that is, many results are routed to the same consumer), the server reaches the code path where a full per-consumer buffer is detected but the internal "high watermark" for that key range is not updated as intended.	2026-06-09	7.1
CVE-2026-9750	mongodb - multiple products	An authenticated user can cause a MongoDB server to crash or return incorrect results by creating documents that interfere with internal metadata processing during query execution. This stems from insufficient separation between user-controlled document fields and internal metadata in certain execution paths.	2026-06-09	7.1
CVE-2026-9752	mongodb - multiple products	An authorized user could trigger a server crash by running a query with a 2dsphere index on a field that stores a GeoJSON GeometryCollection containing a Polygon with a strict-winding CRS. Strict-winding polygons are intentionally unsupported for indexing, but the guard that rejects them does not inspect members of a GeometryCollection, allowing the unsafe path to be reached which ends with an ensuing null-pointer dereference.	2026-06-09	7.1
CVE-2026-9754	mongodb - multiple products	An authenticated user with the read role may read limited amounts of uninitialized stack memory via specially-crafted issuances of the filemd5 command	2026-06-09	7.1
CVE-2022-26758	apple - macos	A malicious application may cause unexpected changes in memory shared between processes. A memory corruption issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.4.	2026-06-10	7.1
CVE-2026-46299	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: hfsplus: fix held lock freed on hfsplus_fill_super() hfsplus_fill_super() calls hfs_find_init() to initialize a search structure, which acquires tree->tree_lock. If the subsequent call to hfsplus_cat_build_key() fails, the function jumps to the out_put_root error label without releasing the lock. The later cleanup path then frees the tree data structure with the lock still held, triggering a	2026-06-08	7

held lock freed warning.

Fix this by adding the missing hfs_find_exit(&fd) call before jumping
to the out_put_root error label. This ensures that tree->tree_lock is
properly released on the error path.

The bug was originally detected on v6.13-rc1 using an experimental
static analysis tool we are developing, and we have verified that the
issue persists in the latest mainline kernel. The tool is specifically
designed to detect memory management issues. It is currently under active
development and not yet publicly available.

We confirmed the bug by runtime testing under QEMU with x86_64 defconfig,
lockdep enabled, and CONFIG_HFSPLUS_FS=y. To trigger the error path, we
used GDB to dynamically shrink the max_unistr_len parameter to 1 before
hfsplus_asc2uni() is called. This forces hfsplus_asc2uni() to naturally
return -ENAMETOOLONG, which propagates to hfsplus_cat_build_key() and
exercises the faulty error path. The following warning was observed
during mount:

```
        ==========================
        WARNING: held lock freed!
        7.0.0-rc3-00016-gb4f0dd314b39 #4 Not tainted
        -------------------------
        mount/174 is freeing memory ffff888103f92000-ffff888103f92fff, with a lock still held
there!
        ffff888103f920b0 (&tree->tree_lock){+.+.}-{4:4}, at: hfsplus_find_init+0x154/0x1e0
        2 locks held by mount/174:
        #0: ffff888103f960e0 (&type->s_umount_key#42/1){+.+.}-{4:4}, at:
alloc_super.constprop.0+0x167/0xa40
        #1: ffff888103f920b0 (&tree->tree_lock){+.+.}-{4:4}, at: hfsplus_find_init+0x154/0x1e0

        stack backtrace:
        CPU: 2 UID: 0 PID: 174 Comm: mount Not tainted 7.0.0-rc3-00016-gb4f0dd314b39 #4
PREEMPT(lazy)
        Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.15.0-1 04/01/2014
        Call Trace:
        <TASK>
        dump_stack_lvl+0x82/0xd0
        debug_check_no_locks_freed+0x13a/0x180
        kfree+0x16b/0x510
        ? hfsplus_fill_super+0xcb4/0x18a0
        hfsplus_fill_super+0xcb4/0x18a0
        ? __pfx_hfsplus_fill_super+0x10/0x10
        ? srso_return_thunk+0x5/0x5f
        ? bdev_open+0x65f/0xc30
        ? srso_return_thunk+0x5/0x5f
        ? pointer+0x4ce/0xbf0
        ? trace_contention_end+0x11c/0x150
        ? __pfx_pointer+0x10/0x10
        ? srso_return_thunk+0x5/0x5f
        ? bdev_open+0x79b/0xc30
        ? srso_return_thunk+0x5/0x5f
        ? srso_return_thunk+0x5/0x5f
        ? vsnprintf+0x6da/0x1270
        ? srso_return_thunk+0x5/0x5f
        ? vsnprintf+0x6da/0x1270
        ? srso_return_thunk+0x5/0x5f
        ? __mutex_unlock_slowpath+0x157/0x740
        ? __pfx_vsnprintf+0x10/0x10
        ? srso_return_thunk+0x5/0x5f
        ? srso_return_thunk+0x5/0x5f
        ? mark_held_locks+0x49/0x80
        ? srso_return_thunk+0x5/0x5f
        ? srso_return_thunk+0x5/0x5f
        ? irqentry_exit+0x17b/0x5e0
        ? trace_irq_disable.constprop.0+0x116/0x150
        ? __pfx_hfsplus_fill_super+0x10/0x10
        ? __pfx_hfsplus_fill_super+0x10/0x10
        get_tree_bdev_flags+0x302/0x580
        ? __pfx_get_tree_bdev_flags+0x10/0x10
        ? vfs_parse_fs_qstr+0x129/0x1a0
        ? __pfx_vfs_parse_fs_qstr+0x3/0x10
        vfs_get_tree+0x89/0x320
        fc_mount+0x10/0x1d0
        path_mount+0x5c5/0x21c0
        ? __pfx_path_mount+0x10/0x10
        ? trace_irq_enable.constprop.0+0x116/0x150
        ? trace_irq_enable.constprop.0+0x116/0x150
        ? srso_return_thunk+0x5/0x5f
        ? srso_return_thunk+0x5/0x5f
        ? kmem_cache_free+0x307/0x540
```

		? user_path_at+0x51/0x60 ? __x64_sys_mount+0x212/0x280 ? srso_return_thunk+0x5/0x5f __x64_sys_mount+0x212/0x280 ? __pfx___x64_sys_mount+0x10/0x10 ? srso_return_thunk+0x5/0x5f ? trace_irq_enable.constprop.0+0x116/0x150 ? srso_return_thunk+0x5/0x5f do_syscall_64+0x111/0x680 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7ffacad55eae Code: 48 8b 0d 85 1f 0f 00 f7 d8 64 89 01 48 83 c8 ff c3 66 2e 0f 1f 84 00 00 00 00 00 90 f3 0f 1e fa 49 89 ca b8 a5 00 00 8 RSP: 002b ---truncated---		
CVE-2026-34335	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-41108	microsoft - multiple products	Heap-based buffer overflow in Microsoft Windows DNS allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-42836	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.	2026-06-09	7
CVE-2026-42911	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-42912	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in Windows Telephony Service allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-42984	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-44818	microsoft - multiple products	Integer underflow (wrap or wraparound) in Microsoft Office Excel allows an unauthorized attacker to execute code locally.	2026-06-09	7
CVE-2026-45596	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-45597	microsoft - multiple products	Concurrent execution using shared resource with improper synchronization ('race condition') in UI Automation Manager (uiamanager.dll) allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-45598	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-45601	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-45603	microsoft - multiple products	Use after free in Windows Ancillary Function Driver for WinSock allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-45640	microsoft - multiple products	Use after free in Windows Bluetooth Port Driver allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-45653	microsoft - multiple products	Use after free in Windows Kernel allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-47293	microsoft - multiple products	Use after free in Microsoft Office Click-To-Run allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-47648	microsoft - multiple products	Untrusted search path in Windows Storage allows an authorized attacker to elevate privileges locally.	2026-06-09	7
CVE-2026-6250	tp-link - tapo_c110_firmware	An authenticated format string vulnerability exists in the ONVIF service of Tapo C110 v2 due to improper handling of user-controlled input. Externally controlled data is interpreted as a format string, which can be used to manipulate stack memory, including control flow data such as return addresses. A remote authenticated attacker may redirect execution flow to existing internal functions, triggering an unauthorized factory reset, leading to loss of configuration, deletion of stored credentials and service disruption.	2026-06-11	7
CVE-2026-54229	red hat - multiple products	A race condition was found in the abrt-dbus D-Bus service's ChownProblemDir method. ChownProblemDir opens the dump directory with DD_OPEN_READONLY and calls dd_chown to change ownership of all files to the caller's uid, succeeding even while post-create event handlers hold a write lock. This allows an attacker to gain filesystem-level control of the dump directory while privileged event scripts are still running.	2026-06-13	7
CVE-2026-54230	red hat - multiple products	A symlink following vulnerability was found in the ABRT post-create event handler scripts in libreport. Event scripts write output files using shell redirections without the O_NOFOLLOW flag. If the target file is replaced with a symlink, the shell process running as root follows the symlink and writes content to the symlink target, allowing arbitrary file overwrites on the system.	2026-06-13	7
CVE-2025-40808	siemens - multiple products	A vulnerability has been identified in SIPROTEC 5 6MD84 (CP300) (All versions), SIPROTEC 5 6MD85 (CP200) (All versions), SIPROTEC 5 6MD85 (CP300) (All versions), SIPROTEC 5 6MD86 (CP200) (All versions), SIPROTEC 5 6MD86 (CP300) (All versions), SIPROTEC 5 6MD89 (CP300) (All versions), SIPROTEC 5 6MU85 (CP300) (All versions), SIPROTEC 5 7KE85 (CP200) (All versions), SIPROTEC 5 7KE85 (CP300) (All versions), SIPROTEC 5 7SA82 (CP100) (All versions), SIPROTEC 5 7SA82 (CP150) (All versions), SIPROTEC 5 7SA86 (CP200) (All versions), SIPROTEC 5 7SA86 (CP300) (All versions), SIPROTEC 5 7SA87 (CP200) (All versions), SIPROTEC 5 7SA87 (CP300) (All versions), SIPROTEC 5 7SD82 (CP100) (All versions), SIPROTEC 5 7SD82 (CP150) (All versions), SIPROTEC 5 7SD86 (CP200)	2026-06-09	6.9

		(All versions), SIPROTEC 5 7SD86 (CP300) (All versions), SIPROTEC 5 7SD87 (CP200) (All versions), SIPROTEC 5 7SD87 (CP300) (All versions), SIPROTEC 5 7SJ81 (CP100) (All versions), SIPROTEC 5 7SJ81 (CP150) (All versions), SIPROTEC 5 7SJ82 (CP100) (All versions), SIPROTEC 5 7SJ82 (CP150) (All versions), SIPROTEC 5 7SJ85 (CP200) (All versions), SIPROTEC 5 7SJ85 (CP300) (All versions), SIPROTEC 5 7SJ86 (CP200) (All versions), SIPROTEC 5 7SJ86 (CP300) (All versions), SIPROTEC 5 7SK82 (CP100) (All versions), SIPROTEC 5 7SK82 (CP150) (All versions), SIPROTEC 5 7SK85 (CP200) (All versions), SIPROTEC 5 7SK85 (CP300) (All versions), SIPROTEC 5 7SL82 (CP100) (All versions), SIPROTEC 5 7SL82 (CP150) (All versions), SIPROTEC 5 7SL86 (CP200) (All versions), SIPROTEC 5 7SL86 (CP300) (All versions), SIPROTEC 5 7SL87 (CP200) (All versions), SIPROTEC 5 7SL87 (CP300) (All versions), SIPROTEC 5 7SS85 (CP200) (All versions), SIPROTEC 5 7SS85 (CP300) (All versions), SIPROTEC 5 7ST85 (CP200) (All versions), SIPROTEC 5 7ST85 (CP300) (All versions), SIPROTEC 5 7ST86 (CP300) (All versions), SIPROTEC 5 7SX82 (CP150) (All versions), SIPROTEC 5 7SX85 (CP300) (All versions), SIPROTEC 5 7SY82 (CP150) (All versions), SIPROTEC 5 7UM85 (CP300) (All versions), SIPROTEC 5 7UT82 (CP100) (All versions), SIPROTEC 5 7UT82 (CP150) (All versions), SIPROTEC 5 7UT85 (CP200) (All versions), SIPROTEC 5 7UT85 (CP300) (All versions), SIPROTEC 5 7UT86 (CP200) (All versions), SIPROTEC 5 7UT86 (CP300) (All versions), SIPROTEC 5 7UT87 (CP200) (All versions), SIPROTEC 5 7UT87 (CP300) (All versions), SIPROTEC 5 7VE85 (CP300) (All versions), SIPROTEC 5 7VK87 (CP200) (All versions), SIPROTEC 5 7VK87 (CP300) (All versions), SIPROTEC 5 7VU85 (CP300) (All versions), SIPROTEC 5 Compact 7SX800 (CP050) (All versions). The affected application allows authenticated users to upload arbitrary files using DIGSI 5 protocol. This could allow an attacker to upload malicious configuration files, that could cause denial of service condition and potentially lead to code execution.		
CVE-2026-9213	netgear - mr70_firmware	A vulnerability in the affected NETGEAR gaming routers allows attackers with the ability to intercept and tamper with traffic between the router and the Internet, to execute code on the device.	2026-06-09	6.9
CVE-2025-66281	qnap - multiple products	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. The remote attackers can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QTS 5.2.9.3410 build 20260214 and later QuTS hero h5.2.9.3410 build 20260214 and later QuTS hero h5.3.4.3500 build 20260520 and later QuTS hero h6.0.0.3397 build 20260206 and later	2026-06-10	6.9
CVE-2026-11628	google - chrome	Use after free in Ozone in Google Chrome prior to 149.0.7827.103 allowed a local attacker to potentially exploit heap corruption via physical access to the device. (Chromium security severity: Critical)	2026-06-09	6.8
CVE-2026-45608	microsoft - multiple products	Out-of-bounds read in Windows DHCP Server allows an authorized attacker to disclose information locally.	2026-06-09	6.8
CVE-2026-50507	microsoft - multiple products	Protection mechanism failure in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2026-06-09	6.8
CVE-2026-9735	mongodb - mongodb	MongoDB server may log authentication parameters, including credentials, to the server log during SASL authentication. When connection health metric logging is enabled, the full authentication parameters are written to the log without redaction.	2026-06-09	6.8
CVE-2026-9751	mongodb - multiple products	The ldapQueryPassword parameter, when set through the runtime setParameter command, will log the new password to the mongod.log file in plain text.	2026-06-09	6.8
CVE-2026-47838	vmware - multiple products	SubjectDnX509PrincipalExtractor does not correctly handle certain malformed X.509 certificate CN values, which can lead to reading the wrong value for the username. In a carefully crafted certificate, this can lead to an attacker impersonating another user. Affected versions: Spring Security 5.7.0 through 5.7.24; 5.8.0 through 5.8.26; 6.3.0 through 6.3.17; 6.4.0 through 6.4.17; 6.5.0 through 6.5.10.	2026-06-10	6.8
CVE-2025-67862	fortinet - multiple products	An Internal Asset Exposed to Unsafe Debug Access Level or State vulnerability [CWE-1244] vulnerability in Fortinet FortiOS 7.6.0 through 7.6.2, FortiOS 7.4.0 through 7.4.7, FortiOS 7.2.0 through 7.2.10, FortiOS 7.0.0 through 7.0.16, FortiOS 6.4 all versions, FortiProxy 7.6.0 through 7.6.3, FortiProxy 7.4.0 through 7.4.10, FortiProxy 7.2.0 through 7.2.14, FortiProxy 7.0 all versions may allow an authenticated admin to execute lua scripts via crafted CLI commands.	2026-06-09	6.7
CVE-2026-26236	qnap - qumagie	A missing authorization vulnerability has been reported to affect QuMagie. The remote attackers can then exploit the vulnerability to access unauthorized data or perform unauthorized actions. We have already fixed the vulnerability in the following version: QuMagie 2.9.0 and later	2026-06-09	6.6
CVE-2026-41976	huawei - multiple products	Permission control vulnerability in the audio framework. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-06-09	6.6
CVE-2026-26237	qnap - qumagie	A missing authorization vulnerability has been reported to affect QuMagie. The remote attackers can then exploit the vulnerability to access unauthorized data or perform unauthorized actions. We have already fixed the vulnerability in the following version: QuMagie 2.9.0 and later	2026-06-10	6.6
CVE-2026-43951	apache - http_server	Out-of-bounds Read vulnerability in Apache HTTP Server with mod_headers and mod_mime and multiple response languages. This issue affects Apache HTTP Server: from 2.4.0 through 2.4.67.	2026-06-08	6.5
CVE-2026-11611	redhat - multiple products	A flaw was found in 389 Directory Server. The Content Synchronization persistent search plugin allows unbounded memory growth when an authenticated client stops reading sync responses, enabling denial of service. Additional race conditions in plugin thread lifecycle can cause crashes during connection teardown or shutdown.	2026-06-08	6.5

CVE-2026-11653	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	2026-06-09	6.5
CVE-2026-11658	google - chrome	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	2026-06-09	6.5
CVE-2026-33582	apache - answer	Unrestricted Upload of File with Dangerous Type vulnerability in Apache Answer. This issue affects Apache Answer: through 2.0.0. A crafted TIFF image could trigger excessive memory allocation during image decoding, allowing an authenticated user to cause the server process to crash. Users are recommended to upgrade to version 2.0.1, which fixes the issue.	2026-06-09	6.5
CVE-2026-34031	apache - answer	Unrestricted Upload of File with Dangerous Type vulnerability in Apache Answer. This issue affects Apache Answer: through 2.0.0. The server did not sufficiently validate user-supplied image URLs, allowing arbitrary external content to be embedded as profile images, which could expose users to unintended external requests and tracking by third-party servers. Users are recommended to upgrade to version 2.0.1, which fixes the issue.	2026-06-09	6.5
CVE-2026-34905	apache - answer	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Answer. This issue affects Apache Answer: through 2.0.0. The unlisted question feature did not enforce access restrictions on direct API endpoints, allowing authenticated users to discover and access unlisted questions, their answers, comments, and revision history. Users are recommended to upgrade to version 2.0.1, which fixes the issue.	2026-06-09	6.5
CVE-2026-49818	apache - apache-airflow-providers-samba	The Apache Airflow Samba provider's `GCSToSambaOperator` joined GCS object names to the SMB destination path without a containment check, so an object named with `../` segments resolved a write path outside the configured `destination_path`. An attacker able to write objects into the source GCS bucket — typically an external data producer distinct from the trusted DAG author — could write files to arbitrary locations on the Samba target when the operator ran. Upgrade apache-airflow-providers-samba to 4.12.6 or later, which validates the resolved destination stays within `destination_path`.	2026-06-09	6.5
CVE-2026-49938	fortinet - multiple products	A improper access control vulnerability in Fortinet FortiPortal 7.4.0 through 7.4.7, FortiPortal 7.2.0 through 7.2.8, FortiPortal 7.0 all versions may allow attacker to improper access control via <insert attack vector here>	2026-06-09	6.5
CVE-2026-42903	microsoft - multiple products	Null pointer dereference in Windows Kerberos allows an authorized attacker to deny service over a network.	2026-06-09	6.5
CVE-2026-42907	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Shell allows an authorized attacker to disclose information locally.	2026-06-09	6.5
CVE-2026-45454	microsoft - multiple products	Improper limitation of a pathname to a restricted directory ('path traversal') in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-06-09	6.5
CVE-2026-45501	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	2026-06-09	6.5
CVE-2026-47284	microsoft - visual_studio_code	Exposure of sensitive information to an unauthorized actor in Visual Studio Code allows an unauthorized attacker to disclose information over a network.	2026-06-09	6.5
CVE-2026-47287	microsoft - visual_studio_code	Relative path traversal in Visual Studio Code allows an unauthorized attacker to perform tampering over a network.	2026-06-09	6.5
CVE-2026-50508	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows NTLM allows an unauthorized attacker to perform spoofing over a network.	2026-06-09	6.5
CVE-2026-11852	debian - debusine	Debusine is an integrated solution to build, distribute and maintain a Debian-based distribution. Files managed by debusine are organized into artifacts. The endpoints that create and delete relationships between artifacts enforced no permissions checks beyond being able to see the artifacts in question.	2026-06-10	6.5
CVE-2026-11853	debian - debusine	Debusine is an integrated solution to build, distribute and maintain a Debian-based distribution. Debian source packages (.dsc) and upload artifacts (.changes) are manifest files that name the files that make up the artifact. The parser used to read these files in Debusine accepted arbitrary fully user-controlled paths. The mergeuploads task could be abused to create arbitrary symbolic links on a worker, overwriting any file that the worker user has access to.	2026-06-10	6.5
CVE-2026-11884	red hat - multiple products	A heap buffer overflow flaw was found in 389 Directory Server. When serializing objectclass definitions, the oc_superior (SUP) field length is omitted from buffer size calculations in read_schema_dse() and schema_oc_to_string(), but the field is still written via strcat(). An attacker with Directory Manager privileges, or a compromised replication supplier, can trigger a server crash by creating objectclasses with long SUP values. This is an incomplete fix variant of CVE-2025-14905.	2026-06-10	6.5
CVE-2026-4096	ibm - devops_plan	IBM DevOps Plan 3.0.0 through 3.0.6 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking	2026-06-11	6.5
CVE-2026-53701	red hat - multiple products	An out-of-bounds write vulnerability was found in GStreamer's H.266/VVC PPS picture partition parser in gst-plugins-bad. In the multi-slice-in-tile processing of gst_h266_parser_parse_picture_partition() (gsth266parser.c), the loop iterates without checking that the slice index stays within bounds, writing past three fixed-size arrays (slice_height_in_ctus, slice_top_left_ctu_x, slice_top_left_ctu_y) in the GstH266PPS structure. While the initial proof-of-concept demonstrated a 4-byte out-of-bounds write, the code permits larger writes across multiple iterations. A crafted H.266/VVC media file can trigger this vulnerability.	2026-06-11	6.5

CVE-2026-53702	red hat - multiple products	A stack buffer overflow flaw was found in the GStreamer H.265 codec parser library (gst-plugins-bad). When parsing a buffering period SEI message, the parser uses an incorrect loop bound derived from cpb_cnt_minus1[i] (the loop index) instead of the sub-layer 0 CPB count cpb_cnt_minus1[0] from the referenced Sequence Parameter Set. A crafted H.265 video file or stream can cause the parser to write beyond the bounds of stack-allocated CPB delay arrays, resulting in a crash or potential stack memory corruption.	2026-06-11	6.5
CVE-2026-12024	google - chrome	Insufficient policy enforcement in DevTools in Google Chrome prior to 149.0.7827.115 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	2026-06-11	6.5
CVE-2026-12026	google - chrome	Out of bounds read in Video in Google Chrome on ChromeOS prior to 149.0.7827.115 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-06-11	6.5
CVE-2026-50630	apache - multiple products	A CRLF injection vulnerability exists in the OAuth2 AuthorizationUtils class. When constructing the WWW-Authenticate response header, the 'realm' parameter is concatenated without sanitizing Carriage Return (CR) and Line Feed (LF) characters. If an attacker can control the realm value, they can inject arbitrary HTTP headers or split the HTTP response entirely. Users are recommended to upgrade to versions 4.2.2 or 4.1.7, which fixes this issue.	2026-06-12	6.5
CVE-2026-50634	apache - multiple products	A vulnerability in Apache CXF's JwsJsonContainerRequestFilter can be exploited to cause CXF to process metadata that was not authenticated by the accepted signature. This can bypass the application's assumption that accepted `Content-Type` or protected HTTP-header metadata came from a verified signature entry, and may steer downstream JAX-RS entity parsing or signed-header consistency checks. Users are recommended to upgrade to versions 4.2.2 or 4.1.7, which fix this issue.	2026-06-12	6.5
CVE-2026-41982	huawei - HarmonyOS	Race condition vulnerability in the IPC module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	6.4
CVE-2026-11769	grafana - Grafana Operator	We have released version 5.24.0 of the Grafana Operator. This patch includes a CRITICAL severity security fix for a path traversal/privilege escalation vulnerability in the Grafana Operator. ### Summary The Grafana Operator supports loading dashboards & library panels using the jsonnet data templating language. The jsonnet expression is evaluated in the context of the operator manager pod. ### Impact It is possible for a malicious user who can create Dashboard or LibraryPanel resources for a Grafana instance to obtain the Kubernetes service account token of the Grafana Operator manager. ### Affected versions All Grafana Operator versions <= 5.23 ### Solutions and mitigations All installations should be upgraded as soon as possible. As a workaround, the following ValidatingAdmissionPolicy prevent the creation or modification of jsonnet based resources: apiVersion: admissionregistration.k8s.io/v1 kind: ValidatingAdmissionPolicy metadata:	2026-06-13	6.4

		name: "prevent-jsonnet-dashboards" spec: failurePolicy: Fail matchConstraints: resourceRules: - apiGroups: ["grafana.integreatly.org"] apiVersions: ["v1beta1"] operations: ["CREATE", "UPDATE"] resources: ["grafanadashboards", "grafanalibrarypanels"] validations: - expression: "!has(object.spec.jsonnetLib)" --- apiVersion: admissionregistration.k8s.io/v1 kind: ValidatingAdmissionPolicyBinding metadata: name: "prevent-jsonnet-dashboards-clusterwide" spec: policyName: "prevent-jsonnet-dashboards" validationActions: [Deny] ### Acknowledgement We would like to thank Artem Cherezov for responsibly disclosing the vulnerability.		
CVE-2026-41975	huawei - HarmonyOS	Permission management vulnerability in the network management module. Impact: Successful exploitation of this vulnerability may affect service integrity.	2026-06-09	6.3
CVE-2026-41116	dell - Inventory Collector Client	Dell Inventory Collector Client, versions prior to 13.8.0, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Arbitrary File Write.	2026-06-09	6.3
CVE-2026-44275	dell - Dell/Alienware Purchased Apps	Dell/Alienware Purchased Apps, versions prior to 1.1.32.0, contain an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Arbitrary File Write	2026-06-09	6.3
CVE-2026-47909	adobe - dreamweaver	Dreamweaver Desktop versions 21.7 and earlier are affected by an Improper Input Validation vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	6.3
CVE-2026-47910	adobe - dreamweaver	Dreamweaver Desktop versions 21.7 and earlier are affected by an Incorrect Authorization vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-06-09	6.3
CVE-2026-26239	qnap - file_station	A buffer overflow vulnerability has been reported to affect File Station 5. If a remote attacker gains a user account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5208 and later	2026-06-10	6.3
CVE-2026-42771	openssl - openssl	Issue summary: When the X509_VERIFY_PARAM_set1_email is called by an application to validate a crafted e-mail address, such as during S/MIME message validation, an out of bounds read can happen. Impact summary: This out of bounds read will not directly exfiltrate the data read to the attacker so the most likely result is a crash and a Denial of Service. An internal helper function called from X509_VERIFY_PARAM_[set|add]_email() used a wrong length when validating the local part of an email address. This could cause the 64 octet limit on the local part of an email address to be not enforced, or cause an out of bound read and potentially a crash. The bug is reachable via S-MIME validation with a crafted From: address	2026-06-09	6.2

		supplied in an email message that can potentially cause a crash. No FIPS modules are affected by this issue as the affected code is outside the OpenSSL FIPS module boundary.		
CVE-2026-45491	microsoft - multiple products	Improper link resolution before file access ('link following') in .NET allows an unauthorized attacker to perform tampering locally.	2026-06-09	6.2
CVE-2026-47902	adobe - multiple products	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Uncontrolled Resource Consumption vulnerability. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-06-09	6.2
CVE-2026-47903	adobe - multiple products	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Improper Input Validation vulnerability. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-06-09	6.2
CVE-2026-47904	adobe - multiple products	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Uncontrolled Resource Consumption vulnerability. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-06-09	6.2
CVE-2026-47905	adobe - multiple products	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Uncontrolled Resource Consumption vulnerability. An attacker could exploit this vulnerability to exhaust system resources, resulting in an application denial-of-service condition. Exploitation of this issue does not require user interaction.	2026-06-09	6.2
CVE-2026-24724	qnap - file_station	An incorrect authorization vulnerability has been reported to affect File Station 6. If a remote attacker gains a user account, they can then exploit the vulnerability to bypass intended access restrictions. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5243 and later	2026-06-10	6.2
CVE-2026-29170	apache - http_server	A cross-site scripting vulnerability exists in mod_proxy_ftp's HTML directory list generation in Apache HTTP Server 2.4.67 and earlier when listing FTP directory contents either via forward or reverse proxy configuration. Users are recommended to upgrade to version 2.4.68, which fixes this issue.	2026-06-08	6.1
CVE-2026-25688	apache - answer	Improper Neutralization of Alternate XSS Syntax vulnerability in Apache Answer. This issue affects Apache Answer: through 2.0.0. AI-generated response content was rendered in the browser without proper sanitization, allowing malicious scripts to be executed when the content was viewed. Users are recommended to upgrade to version 2.0.1, which fixes the issue.	2026-06-09	6.1
CVE-2026-25699	apache - answer	Exposure of Private Personal Information to an Unauthorized Actor vulnerability in Apache Answer. This issue affects Apache Answer: through 2.0.0. Timeline-related APIs lacked proper authorization checks, allowing regular authenticated users to access deleted, private, or unapproved content and its revision history. Users are recommended to upgrade to version 2.0.1, which fixes the issue.	2026-06-09	6.1
CVE-2026-45500	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Exchange Server allows an unauthorized attacker to perform spoofing over a network.	2026-06-09	6.1
CVE-2026-41706	vmware - multiple products	Spring Security's CookieRequestCache and CookieServerRequestCache store the pre-authentication request URL in a browser cookie so that users can be redirected back to their intended destination after a successful login. In affected versions, the full absolute URL is stored in the cookie and is used without validation as the post-login redirect target. Affected versions: Spring Security 5.7.0 through 5.7.23; 5.8.0 through 5.8.25; 6.3.0 through 6.3.16; 6.4.0 through 6.4.16; 6.5.0 through 6.5.10; 7.0.0 through 7.0.5.	2026-06-10	6.1
CVE-2026-41568	docker - multiple products	Moby is an open source container framework. In Docker Engine prior to version 29.5.1, Docker Daemon versions 28.5.2 and prior, and Moby Daemon prior to version 2.0.0-beta.14, a race condition during docker cp mount setup allows a malicious container to create empty files or directories at arbitrary absolute paths on the host filesystem. This issue has been patched in Docker Engine version 29.5.1 and Moby Daemon version 2.0.0-beta.14.	2026-06-12	6.1
CVE-2026-28262	dell - iDRAC Tools	Dell iDRAC Tools, versions prior to 11.4.1.0, contains an Improper Link Resolution Before File Access ('Link Following') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Information tampering.	2026-06-09	6
CVE-2026-41840	vmware - multiple products	Spring WebFlux applications are vulnerable to Denial of Service (DoS) attacks when processing multipart requests. Affected versions: Spring Framework 7.0.0 through 7.0.7, 6.2.0 through 6.2.18, 6.1.0 through 6.1.27, 5.3.0 through 5.3.48.	2026-06-09	5.9
CVE-2026-41841	vmware - multiple products	Spring MVC and WebFlux applications are vulnerable to Information Disclosure attacks when resolving static resources. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	5.9
CVE-2026-41843	vmware - multiple products	Spring MVC and WebFlux applications are vulnerable to Path Traversal attacks when resolving static resources. Affected versions:	2026-06-09	5.9

		Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.		
CVE-2026-41846	vmware - multiple products	Spring MVC applications which accept user-supplied values in the cssClass, cssErrorClass, or cssStyle attributes of JSP form tags allow arbitrary HTML/JavaScript code injection, potentially resulting in a cross-site scripting (XSS) vulnerability. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	5.9
CVE-2026-41973	huawei - multiple products	Permission control vulnerability in calls. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	5.9
CVE-2026-11788	redhat - multiple products	A flaw was found in 389 Directory Server. The dereference control plugin does not check for allocation failure before using a BER structure, allowing an unauthenticated remote attacker to crash the LDAP server when the system is under memory pressure.	2026-06-09	5.9
CVE-2026-42766	openssl - multiple products	Issue summary: A specially crafted password-encrypted CMS message can trigger a NULL pointer dereference during CMS decryption. Impact summary: This NULL pointer dereference leads to an application crash and a Denial of Service. The CMS PasswordRecipientInfo.keyDerivationAlgorithm field is defined as OPTIONAL in the ASN.1 specification and may therefore be absent in specially crafted inputs. During the password-based CMS decryption the OpenSSL CMS implementation dereferences this field without first checking whether it was present. An attacker who supplies such a CMS message to an application performing password-based CMS decryption can trigger an application crash, leading to a Denial of Service. Applications that process password-encrypted CMS messages may be affected. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	2026-06-09	5.9
CVE-2026-42767	openssl - multiple products	Issue summary: An attacker-controlled CMP (Certificate Management Protocol) server could trigger a NULL pointer dereference in a CMP client application. Impact summary: A NULL pointer dereference causes a crash of the application and a Denial of Service. An attacker controlling a CMP server (or acting as a man-in-the-middle) could craft a CMP response containing a CRMF (Certificate Request Message Format) CertRepMessage with an EncryptedValue structure where the symmAlg field has an algorithm OID but no parameters field. When the OpenSSL CMP client processes this response, the NULL dereference occurs, causing a crash of the CMP client. Applications that process untrusted CMP/CRMF messages may be affected. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	2026-06-09	5.9
CVE-2026-34694	adobe - multiple products	Adobe Experience Manager Forms JEE versions LTS SP1, 6.5.24.0 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a high-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.9
CVE-2026-40639	dell - multiple products	Dell Client Platform BIOS contains a Weak Encoding for Password vulnerability. An unauthenticated attacker with physical access could potentially exploit this vulnerability, leading to Elevation of Privileges.	2026-06-09	5.7
CVE-2026-9212	netgear - lbr1020_firmware	Insufficient authentication and input validation in the listed NETGEAR models allow users connected to the local network to execute commands impacting the product's confidentiality or change certain configurations.	2026-06-09	5.6
CVE-2026-44119	apache - http_server	Improper Privilege Management vulnerability in Apache HTTP Server 2.4.67 and earlier allows local .htaccess authors to read files with the privileges of the httpd user. This issue affects Apache HTTP Server: from through 2.4.67. Users are recommended to upgrade to version 2.4.68, which fixes the issue.	2026-06-08	5.5
CVE-2026-41979	huawei - HarmonyOS	Permission control vulnerability in the print module. Impact: Successful exploitation of this vulnerability may affect integrity and confidentiality.	2026-06-09	5.5
CVE-2026-41980	huawei - HarmonyOS	Permission control vulnerability in the file preview module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-06-09	5.5
CVE-2026-42906	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Shell allows an authorized attacker to disclose information locally.	2026-06-09	5.5
CVE-2026-42915	microsoft - multiple products	Incorrect calculation of buffer size in Windows VMSwitch allows an authorized attacker to deny service locally.	2026-06-09	5.5
CVE-2026-42968	microsoft - multiple products	Out-of-bounds read in Windows Telephony Service allows an authorized attacker to disclose information locally.	2026-06-09	5.5
CVE-2026-42969	microsoft - multiple products	Use of uninitialized resource in Windows Push Notifications allows an authorized attacker to disclose information locally.	2026-06-09	5.5

CVE-2026-42970	microsoft - multiple products	Use of uninitialized resource in Windows Push Notifications allows an authorized attacker to disclose information locally.	2026-06-09	5.5
CVE-2026-42971	microsoft - multiple products	Use of uninitialized resource in Windows Push Notifications allows an authorized attacker to disclose information locally.	2026-06-09	5.5
CVE-2026-42972	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Hyper-V allows an authorized attacker to disclose information locally.	2026-06-09	5.5
CVE-2026-42973	microsoft - multiple products	Use of uninitialized resource in Windows Push Notifications allows an authorized attacker to disclose information locally.	2026-06-09	5.5
CVE-2026-44805	microsoft - multiple products	Use after free in Windows Network Controller (NC) Host Agent allows an authorized attacker to deny service locally.	2026-06-09	5.5
CVE-2026-44814	microsoft - multiple products	Out-of-bounds read in Windows DWM Core Library allows an authorized attacker to disclose information locally.	2026-06-09	5.5
CVE-2026-44821	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-06-09	5.5
CVE-2026-45594	microsoft - multiple products	Exposure of sensitive information to an unauthorized actor in Windows Application Identity (AppID) Subsystem allows an authorized attacker to disclose information locally.	2026-06-09	5.5
CVE-2026-45604	microsoft - multiple products	Out-of-bounds read in Windows Application Identity (AppID) Subsystem allows an authorized attacker to disclose information locally.	2026-06-09	5.5
CVE-2026-45606	microsoft - multiple products	Out-of-bounds read in Microsoft UxTheme Library (uxtheme.dll) allows an authorized attacker to deny service locally.	2026-06-09	5.5
CVE-2026-45634	microsoft - multiple products	Out-of-bounds read in Windows DHCP Server allows an authorized attacker to disclose information locally.	2026-06-09	5.5
CVE-2026-45647	microsoft - defender_for_endpoint	Time-of-check time-of-use (toctou) race condition in Microsoft Defender for Endpoint allows an authorized attacker to elevate privileges locally.	2026-06-09	5.5
CVE-2026-48566	microsoft - multiple products	Out-of-bounds read in Windows DWM Core Library allows an authorized attacker to disclose information locally.	2026-06-09	5.5
CVE-2026-34703	adobe - multiple products	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5
CVE-2026-34704	adobe - multiple products	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by a NULL Pointer Dereference vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5
CVE-2026-34705	adobe - multiple products	InDesign Desktop versions 21.3, 20.5.3 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5
CVE-2026-47923	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5
CVE-2026-47924	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by a Use After Free vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5
CVE-2026-47925	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an Integer Overflow or Wraparound vulnerability that could result in an application denial-of-service. An attacker could exploit this vulnerability to crash the application, leading to a denial-of-service condition. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5
CVE-2026-47926	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5
CVE-2026-47961	adobe - multiple products	Acrobat Reader versions 24.001.30365, 26.001.21651 and earlier are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to disclose sensitive information. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-06-09	5.5
CVE-2026-34657	adobe - multiple products	CAI Content Credentials versions c2pa-web@0.7.1, c2pa-v0.80.1 and earlier are affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could result in an arbitrary file system write. An attacker could leverage this vulnerability to write to unauthorized files or directories outside of intended restrictions. Exploitation of this issue requires user interaction in that a victim must extract a maliciously crafted file.	2026-06-09	5.5
CVE-2025-24165	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.4, macOS Sonoma 14.7.5, macOS Ventura 13.7.5. An app may be able to cause unexpected system termination.	2026-06-11	5.5
CVE-2025-24268	apple - macos	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Sequoia 15.4. An app may be able to access sensitive user data.	2026-06-11	5.5
CVE-2025-30431	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.4, macOS Sonoma 14.7.5, macOS Ventura 13.7.5. A malicious app may be able to access private information.	2026-06-11	5.5
CVE-2025-30459	apple - macos	A privacy issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.4. An app may be able to access sensitive user data.	2026-06-11	5.5
CVE-2025-43278	apple - macos	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sequoia 15.4. An app may be able to access protected user data.	2026-06-11	5.5
CVE-2025-43339	apple - macos	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Tahoe 26.1. A malicious app may be able to access sensitive user data.	2026-06-11	5.5

CVE-2025-46293	apple - macos	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sequoia 15.4. An app may be able to access protected user data.	2026-06-11	5.5
CVE-2025-46313	apple - macos	A logging issue was addressed with improved data redaction. This issue is fixed in macOS Tahoe 26.1. An app may be able to access sensitive user data.	2026-06-11	5.5
CVE-2026-54231	red hat - multiple products	A content injection vulnerability was found in the ABRT post-create event handler scripts in libreport. The event script queries the systemd journal for log entries matching the crashed process and writes the results to files in the dump directory without sanitizing embedded control characters. A local user can inject arbitrary content into the journal output by embedding newline characters in syslog messages, controlling the content that root writes to dump directory files.	2026-06-13	5.5
CVE-2026-11569	red hat - multiple products	A flaw was found in Quay. The filedrop endpoint accepts any mime type without validation, allowing an authenticated user with repository write access to upload a malicious SVG file containing JavaScript. The file is stored and served inline through the CDN, enabling stored cross-site scripting when a victim visits the archive URL.	2026-06-08	5.4
CVE-2026-11666	google - chrome	Insufficient validation of untrusted input in Input in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: High)	2026-06-09	5.4
CVE-2026-11701	google - chrome	Inappropriate implementation in Guest View in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-06-09	5.4
CVE-2026-41972	huawei - HarmonyOS	Path traversal vulnerability in the SMS app. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	5.4
CVE-2026-34033	apache - answer	Improper Neutralization of Script-Related HTML Tags in a Web Page (Basic XSS) vulnerability in Apache Answer. This issue affects Apache Answer: through 2.0.0. User-supplied content was included in notification emails without proper escaping, allowing authenticated users to inject arbitrary HTML into emails sent to other users. Users are recommended to upgrade to version 2.0.1, which fixes the issue.	2026-06-09	5.4
CVE-2026-33113	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.	2026-06-09	5.4
CVE-2026-34692	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-45453	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.	2026-06-09	5.4
CVE-2026-45464	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.	2026-06-09	5.4
CVE-2026-45465	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.	2026-06-09	5.4
CVE-2026-45595	microsoft - multiple products	Protection mechanism failure in Windows Mark of the Web (MOTW) allows an unauthorized attacker to bypass a security feature over a network.	2026-06-09	5.4
CVE-2026-47636	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.	2026-06-09	5.4
CVE-2026-47639	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.	2026-06-09	5.4
CVE-2026-47935	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-47936	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47939	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47941	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47942	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47943	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47944	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47945	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject	2026-06-09	5.4

		malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.		
CVE-2026-47946	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-47947	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-47948	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47949	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47950	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47951	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47953	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47954	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47956	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47957	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47958	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47962	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47966	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47970	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47972	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47973	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47974	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47975	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47977	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject	2026-06-09	5.4

		malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.		
CVE-2026-47978	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47980	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47981	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47982	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-47983	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-47985	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-47986	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-47987	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-47989	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-47990	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-47993	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-48250	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-48251	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-48256	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-48258	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-48264	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4

CVE-2026-48265	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-48266	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-48268	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-48271	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-48280	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 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. Scope is changed.	2026-06-09	5.4
CVE-2026-48297	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-48299	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-48300	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-48301	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-48304	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	5.4
CVE-2026-48560	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.	2026-06-09	5.4
CVE-2026-53441	jenkins - multiple products	Jenkins 2.483 through 2.567 (both inclusive), LTS 2.492.1 through 2.555.2 (both inclusive) does not escape the user-provided description of a generic offline cause that could be set through the `POST config.xml` API, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Agent/Configure permission.	2026-06-10	5.4
CVE-2026-11669	google - chrome	Out of bounds read in Media in Google Chrome on ChromeOS prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-06-09	5.3
CVE-2026-11678	google - chrome	Integer overflow in libyuv in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-06-09	5.3
CVE-2026-11696	google - chrome	Uninitialized Use in Video in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-06-09	5.3
CVE-2026-41851	vmware - multiple products	Applications which accept user-supplied Spring Expression Language (SpEL) expressions may be vulnerable to a Denial of Service (DoS) attack if the evaluation of a SpEL expression triggers unbounded cache growth. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	5.3
CVE-2026-41853	vmware - multiple products	Spring MVC and WebFlux applications are vulnerable to Multipart request smuggling attacks. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	5.3
CVE-2026-41981	huawei - HarmonyOS	Out-of-bounds write vulnerability in the IPC module. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	5.3
CVE-2026-46747	siemens - multiple products	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 6). The affected application does not properly sanitize path input in the `GET /api/sftp/uploadFiles` endpoint used for directory listing. This allows path traversal through crafted input, enabling access to unintended file system locations.	2026-06-09	5.3

CVE-2026-42769	openssl - multiple products	Issue Summary: An error in the callback used to verify the certificate provided in a Root CA key update Certificate Management Protocol (CMP) message response rendered the certificate validation ineffectual, which could lead to escalation of credentials from the Registration Authority (RA) level to the root Certification Authority (root CA) level. Impact Summary: The Registration Autority could replace the root CA certificate for the CMP clients with an arbitrary root CA certificate. One of the parts of the Certificate Management Protocol (CMP), specified in RFC 9810, is Root Certification Authority (root CA) key Rollover, which is sent by the server in a message with type 'id-it-rootCaKeyUpdate'. As part of these messages, 'newWithOld' certificate, the new root CA certificate signed with the old root CA key, is provided, and verifying its signature is crucial for transferring the trust from the old CA key to the new one. The 'id-it-rootCaKeyUpdate' messages are expected to be processed with OSSL_CMP_get1_rootCaKeyUpdate(), that is expected to verify the 'newWithOld' certificate. A typo in the certificate chain building code led to adding an incorrect certificate ('newWithOld' instead of 'oldRoot') to the certificate chain, rendering the certificate verification process ineffectual (only the issuer name and the algorithm OIDs were verified by other parts of the verification code). An attacker who already has credentials that satisfy the CMP message protection checks can generate a new key pair and use a crafted self-signed certificate in its 'id-it-rootCaKeyUpdate' CMP messages which affected CMP clients would accept as a new trust anchor. Significant preconditions for the attack (having valid RA-level credentials) are the reason the issue was assigned Low severity. The FIPS modules are not affected by this issue, as the affected code is outside the OpenSSL FIPS module boundary.	2026-06-09	5.3
CVE-2026-42914	microsoft - multiple products	Windows Kerberos Denial of Service Vulnerability	2026-06-09	5.3
CVE-2026-45655	microsoft - multiple products	Protection mechanism failure in Windows BitLocker allows an unauthorized attacker to bypass a security feature with a physical attack.	2026-06-09	5.3
CVE-2026-53442	jenkins - multiple products	Jenkins 2.567 and earlier, LTS 2.555.2 and earlier does not encrypt secrets from POST config.xml submissions before storing them in job configurations unencrypted in job config.xml files on the Jenkins controller where they can be viewed by users with Item/Extended Read permission, or access to the Jenkins controller file system.	2026-06-10	5.3
CVE-2025-46308	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in iOS 18.4 and iPadOS 18.4, macOS Sequoia 15.4. An app may be able to leak sensitive user information.	2026-06-11	5.3
CVE-2026-12015	google - chrome	Use after free in Autofill in Google Chrome prior to 149.0.7827.115 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-06-11	5.3
CVE-2026-12025	google - chrome	Insufficient validation of untrusted input in Network in Google Chrome prior to 149.0.7827.115 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-11	5.3
CVE-2026-12033	google - chrome	Out of bounds read in VideoCapture in Google Chrome prior to 149.0.7827.115 allowed a remote attacker who had compromised the GPU process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-06-11	5.3
CVE-2026-50629	apache - multiple products	The 'clientId' parameter from incoming HTTP requests is directly concatenated into OAuth2 server log warning messages without sanitizing control characters. This allows an attacker to inject arbitrary content, including fake log entries, into the server's log files. Users are recommended to upgrade to versions 4.2.2 or 4.1.7, which fixes this issue.	2026-06-12	5.3
CVE-2026-41984	huawei - HarmonyOS	UAF vulnerability in the package management module. Impact: Successful exploitation of this vulnerability may affect service integrity.	2026-06-09	5.2
CVE-2026-9211	netgear - cax30_firmware	An unauthenticated user on the local network can gain control of the router and make unauthorized changes to its operation.	2026-06-09	5.2
CVE-2025-62858	qnap - multiple products	A buffer overflow vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following versions: QTS 5.2.9.3410 build 20260214 and later QuTS hero h5.2.9.3410 build 20260214 and later QuTS hero h5.3.4.3500 build 20260520 and later QuTS hero h6.0.0.3397 build 20260206 and later	2026-06-09	5.1
CVE-2026-41985	huawei - HarmonyOS	UAF vulnerability in the package management module. Impact: Successful exploitation of this vulnerability may affect service integrity.	2026-06-09	5.1
CVE-2025-62850	qnap - multiple products	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QuTS hero h5.2.9.3410 build 20260214 and later	2026-06-10	5.1

		QuTS hero h5.3.4.3500 build 20260520 and later QuTS hero h6.0.0.3459 build 20260409 and later		
CVE-2025-66280	qnap - multiple products	An integer overflow or wraparound vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to compromise the security of the system. We have already fixed the vulnerability in the following versions: QTS 5.2.9.3410 build 20260214 and later QuTS hero h5.2.9.3410 build 20260214 and later QuTS hero h5.3.4.3500 build 20260520 and later QuTS hero h6.0.0.3397 build 20260206 and later	2026-06-10	5.1
CVE-2026-24716	qnap - multiple products	A NULL pointer dereference vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following versions: QTS 5.2.9.3492 build 20260507 and later QuTS hero h5.2.9.3499 build 20260514 and later QuTS hero h5.3.4.3500 build 20260520 and later QuTS hero h6.0.0.3459 build 20260409 and later	2026-06-10	5.1
CVE-2026-24717	qnap - multiple products	A path traversal vulnerability has been reported to affect several QNAP operating system versions. If a remote attacker gains an administrator account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following versions: QTS 5.2.9.3492 build 20260507 and later QuTS hero h5.2.9.3499 build 20260514 and later QuTS hero h5.3.4.3500 build 20260520 and later QuTS hero h6.0.0.3459 build 20260409 and later	2026-06-10	5.1
CVE-2026-7516	lenovo - Application	A vulnerability was identified in the Lenovo Android Application, distributed exclusively on tablets in the Chinese market, that could allow a website visited by the built-in browser to overwrite system clipboard contents.	2026-06-10	5.1
CVE-2026-41977	huawei - multiple products	DoS vulnerability in the log service. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	5
CVE-2026-11787	redhat - multiple products	A flaw was found in 389 Directory Server. The ldap_utf8prev() function reads bytes before the start of a buffer without bounds checking, causing a heap buffer over-read in string filter parsing that may influence internal filter processing behavior.	2026-06-09	5
CVE-2026-35188	openssl - multiple products	Issue summary: A malicious server can exploit TLS OCSP stapling by delivering a crafted response through the status_request extension, triggering a double-free in the client's certificate verification path. Impact summary: Successful exploitation allows an attacker to corrupt heap memory via a double-free, potentially leading to a Denial of Service or possibly an attacker controlled code execution or other undefined behavior. If OCSP stapling is enabled and the TLS client connects to a malicious server, a crafted OCSP stapled response can trigger a double free in the TLS client when the stapled response is checked. The OCSP stapling is not enabled by default. Reliable code execution through a double-free is technically complex and highly environment-dependent but the Denial of Service impact is straightforward to achieve, warranting Moderate severity. No FIPS modules are affected by this issue as the affected code is outside the OpenSSL FIPS module boundary.	2026-06-09	5
CVE-2026-45502	microsoft - multiple products	Server-side request forgery (ssrf) in Microsoft Exchange Server allows an authorized attacker to disclose information over a network.	2026-06-09	5
CVE-2026-11850	red hat - multiple products	An integer underflow vulnerability was found in MIT krb5 in the berval2tl_data() function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c. The function performs an unsigned subtraction (bv_len - 2) without a prior bounds check. When bv_len is 0 or 1, the subtraction wraps to a large value which is then truncated to uint16_t, yielding 0xFFFE (65534) or 0xFFFF (65535). The subsequent malloc succeeds and memcpy reads up to 65534 bytes from a 0-1 byte buffer, resulting in a heap out-of-bounds read. The attack vector involves a malicious or compromised LDAP KDB backend returning a krbExtraData attribute with bv_len < 2, triggering the underflow when the KDC or kadmind reads principal data.	2026-06-11	5
CVE-2026-46749	siemens - multiple products	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 6). The affected application uses a password hashing implementation with a static, hardcoded salt shared across all users and installations, and is configured with an insufficient number of iterations. This could allow an attacker to efficiently recover user passwords using brute-force or precomputed attacks, potentially resulting in unauthorized access.	2026-06-09	4.9
CVE-2026-11789	redhat - multiple products	A flaw was found in 389 Directory Server. The SMD5 password storage plugin performs unsigned integer underflow when computing salt length from a crafted password hash shorter than 16 bytes, causing a buffer over-read that crashes the LDAP server during authentication.	2026-06-09	4.9
CVE-2026-11790	redhat - multiple products	A flaw was found in 389 Directory Server. The PBKDF2-SHA256 password storage plugin does not enforce an upper bound on the iteration count extracted from stored password hashes. A privileged attacker who can modify a user's password hash can cause excessive CPU consumption during authentication, resulting in denial of service.	2026-06-09	4.9
CVE-2026-11793	redhat - 389_directory_server	A stack buffer overflow flaw was found in 389 Directory Server. The checkPrefix() function in pw.c copies an attacker-controlled algorithm ID into a 256-byte stack buffer without bounds checking when parsing reversible-encrypted attribute values. An attacker with Directory Manager privileges can crash the LDAP server by storing a crafted credential with an oversized algorithm ID. FORTIFY_SOURCE mitigates this to denial of service only.	2026-06-09	4.9
CVE-2026-3088	netgear - rbe970_firmware	Unauthenticated users on the local network can cause the router to become unavailable by sending specially crafted requests.	2026-06-09	4.9

CVE-2026-9210	netgear - ex3700_firmware	Insufficient input validation vulnerability in the listed NETGEAR models allows authenticated administrators connected to the local network to make unauthorized modification of router software and functionality.	2026-06-09	4.9
CVE-2026-11986	red hat - multiple products	A flaw was found in the admin-ui-ext component of Keycloak, which provides extended administrative user interface capabilities. The issue occurs because certain bulk role-removal endpoints fail to perform granular permission checks when deleting role mappings. This allows a delegated administrator with limited permissions to remove highly privileged roles from other users or groups, potentially disrupting administrative access control.	2026-06-11	4.9
CVE-2026-41838	vmware - multiple products	IDs for WebSocket sessions in the spring-websocket module are not cryptographically unpredictable, which may be possible to exploit in combination with inadequate authorization rules. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	4.8
CVE-2026-41847	vmware - spring_framework	Spring WebFlux applications may be vulnerable to a security bypass when using the Kotlin Router DSL. Affected versions: Spring Framework 5.3.0 through 5.3.48.	2026-06-09	4.8
CVE-2026-0409	netgear - rbe370_firmware	A NETGEAR security issue that could allow an attacker with ability to intercept and tamper with traffic between the router and the Internet to run commands on your device when the device administrator performs certain specific management actions. This issue affects NETGEAR Orbi 370 series devices before V12.1.2.7.	2026-06-09	4.8
CVE-2026-28301	solarwinds - Observability Self-Hosted	A vulnerability in which an attacker can provide a crafted external URL that may redirect a user to an unintended website.	2026-06-09	4.8
CVE-2026-45446	openssl - multiple products	Issue summary: The implementations of AES-SIV (RFC 5297) and AES-GCM-SIV (RFC 8452) mishandle the authentication of AAD (Additional Authenticated Data) with an empty ciphertext allowing a forgery of such messages. Impact summary: An attacker can forge empty messages with arbitrary AAD to the victim's application using these ciphers. AES-SIV (RFC 5297) and AES-GCM-SIV (RFC 8452) are nonce-misuse-resistant AEAD modes: they accept a key, nonce, optional AAD (bytes that are authenticated but not encrypted), and plaintext, and produces ciphertext plus a 16-byte tag. On decrypt, `EVP_DecryptFinal_ex()` is documented to return success only if the tag is verified succesfully. In OpenSSL's provider implementation of these ciphers, the expected tag is computed only when decryption function is invoked with non-empty data. If the caller supplies AAD and then calls `EVP_DecryptFinal_ex()` without invocation of the ciphertext update, which can happen when the received ciphertext length is zero, the tag is never recalculated and still holds its all-zeros value. When AES-GCM-SIV is used, an attacker who sends arbitrary AAD, empty ciphertext, and all-zeros tag passes authentication under any key they do not know, single-shot. When AES-SIV is used, for mounting the attack it's necessary for the application to reuse the decryption context without resetting the key. AES-SIV is implemented since OpenSSL 3.0. AES-GCM-SIV is implemented since OpenSSL 3.2. No protocols implemented in OpenSSL itself (TLS/CMS/PKCS7/HPKE/QUIC) support either AES-GCM-SIV or AES-SIV. To mount an attack, the applications must implement their own protocol and use the EVP interface. Also they must skip the ciphertext update when a message with an empty ciphertext arrives. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are not affected by this issue, as these algorithms are not FIPS approved and the affected code is outside the OpenSSL FIPS module boundary.	2026-06-09	4.8
CVE-2026-47933	adobe - multiple products	ColdFusion versions 2023.19, 2025.8 and earlier are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by a low-privileged attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. Scope is changed.	2026-06-09	4.8
CVE-2026-50623	apache - multiple products	An authentication bypass vulnerability exists in the OAuth2 TokenIntrospectionService in Apache CXF. Due to a missing 'throw' keyword in the security context check, the introspection endpoint (/services/oauth2/introspect) can be accessed by any unauthenticated network attacker. However note that this is a safeguard only in the case that someone forgot to enable authentication on the service. Users are recommended to upgrade to version 4.2.2 or 4.1.7, which fixes this issue.	2026-06-12	4.8
CVE-2026-52902	red hat - multiple products	A path traversal vulnerability was found in awxkit, the CLI tool for AWX. The YAML !include directive does not sanitize file paths, allowing an attacker to craft a malicious YAML file that reads arbitrary YAML-formatted files from the local filesystem when a user imports it using "awx --conf.format yaml import". This is a client-side vulnerability requiring user interaction.	2026-06-09	4.7
CVE-2026-45460	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-06-09	4.7

CVE-2026-0420	netgear - rax120_firmware	An improper implementation of TLS certificate validation vulnerability found in NETGEAR's ReadyCloud client app which could allow an attacker to perform attacker-in-the-middle (MiTM) style attacks impacting the product's confidentiality. This vulnerability affects the listed NETGEAR models.	2026-06-09	4.6
CVE-2026-45462	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.	2026-06-09	4.6
CVE-2026-45467	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.	2026-06-09	4.6
CVE-2026-45468	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.	2026-06-09	4.6
CVE-2026-45479	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.	2026-06-09	4.6
CVE-2026-45483	microsoft - multiple products	Improper neutralization of input during web page generation ('cross-site scripting') in Microsoft Office Project Server allows an authorized attacker to perform spoofing over a network.	2026-06-09	4.6
CVE-2026-47637	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.	2026-06-09	4.6
CVE-2026-47638	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.	2026-06-09	4.6
CVE-2026-47640	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.	2026-06-09	4.6
CVE-2026-47641	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.	2026-06-09	4.6
CVE-2026-48562	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.	2026-06-09	4.6
CVE-2025-62851	qnap - license_center	A path traversal vulnerability has been reported to affect License Center. If a local attacker gains an administrator account, they can then exploit the vulnerability to read the contents of unexpected files or system data. We have already fixed the vulnerability in the following version: License Center 1.9.56 and later	2026-06-10	4.6
CVE-2026-41978	huawei - HarmonyOS	Permission control vulnerability in the clone module. Impact: Successful exploitation of this vulnerability may affect service confidentiality.	2026-06-09	4.4
CVE-2026-0419	netgear - jr6150_firmware	Insufficient input validation in NETGEAR JR6150 (AC750 WiFi Router 802.11ac Dual Band Gigabit released in 2014) allows users connected to the local WiFi Networks to execute operating system commands. NETGEAR JR6150 has reached End-of-Support phase as of 2018 , and no further security updates are planned. NETGEAR strongly recommends replacing these devices with newer NETGEAR models to ensure continued security support and updates. This vulnerability has been identified through firmware emulation in a controlled research environment and has not been verified on production hardware.	2026-06-09	4.4
CVE-2026-11665	google - chrome	Out of bounds read in Dawn in Google Chrome on Windows prior to 149.0.7827.103 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-09	4.3
CVE-2026-11668	google - chrome	Uninitialized Use in Codecs in Google Chrome on Linux, ChromeOS prior to 149.0.7827.103 allowed a remote attacker to leak cross-origin data via a crafted video file. (Chromium security severity: High)	2026-06-09	4.3
CVE-2026-11685	google - chrome	Inappropriate implementation in MediaCapture in Google Chrome on Mac prior to 149.0.7827.103 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-09	4.3
CVE-2026-11695	google - chrome	Inappropriate implementation in Passwords in Google Chrome prior to 149.0.7827.103 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-09	4.3
CVE-2026-41983	huawei - HarmonyOS	DoS vulnerability in the browser kernel. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	4.3
CVE-2026-11785	redhat - multiple products	A flaw was found in 389 Directory Server. A type confusion in the SSO token extended operation handler causes partial stack address information to be disclosed in LDAP responses to authenticated users.	2026-06-09	4.3
CVE-2026-0412	netgear - jr6150_firmware	Insufficient input validation vulnerability in NETGEAR JR6150 (AC750 WiFi Router 802.11ac Dual Band Gigabit released in 2014) allows administrators connected to the local network to make unauthorized modification of router software and functionality. NETGEAR JR6150 reached End-of-Support status in 2018 and is no longer receiving security updates. NETGEAR strongly recommends replacing these devices with newer NETGEAR models to ensure continued security support and updates. This vulnerability has been identified through firmware emulation in a controlled research environment and has not been verified on production hardware.	2026-06-09	4.3
CVE-2026-0413	netgear - rbe370_firmware	A buffer overflow vulnerability due to insufficient input validation in the listed NETGEAR models allows authenticated administrators connected to the local network to make unauthorized modification of router software and functionality.	2026-06-09	4.3
CVE-2026-0414	netgear - rbe970_firmware	Insufficient input validation vulnerability in the listed NETGEAR models allows authenticated administrators connected to the local network to make unauthorized modification of router software and functionality.	2026-06-09	4.3
CVE-2026-0415	netgear - rbe970_firmware	Insufficient input validation vulnerability in the listed NETGEAR models allows authenticated administrators connected to the local network to make unauthorized modification of router software and functionality.	2026-06-09	4.3

CVE-2026-0416	netgear - raxe450_firmware	An insufficient input validation vulnerability in certain NETGEAR router models as listed allows an authenticated administrator with local network access to submit crafted input that bypasses intended management interface restrictions, resulting in unauthorized modification of protected router software or functionality.	2026-06-09	4.3
CVE-2026-0417	netgear - mr60_firmware	Insufficient input validation vulnerability in the listed NETGEAR devices allows authenticated administrators connected to the local network to tamper with the router's integrity.	2026-06-09	4.3
CVE-2026-0418	netgear - cbr750_firmware	Insufficient configuration management in the listed devices allows authenticated administrators connected to the local network to tamper with the system.	2026-06-09	4.3
CVE-2026-45650	microsoft - bing	User interface (ui) misrepresentation of critical information in Microsoft Bing allows an unauthorized attacker to perform spoofing over a network.	2026-06-09	4.3
CVE-2026-47991	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by an Improper Redirect (Open Redirect) vulnerability that could lead to account takeover. An attacker could construct a malicious URL that redirects a victim to an attacker-controlled site. Exploitation of this issue requires user interaction in that a victim must click on a malicious link.	2026-06-09	4.3
CVE-2026-53436	jenkins - multiple products	Jenkins 2.567 and earlier, LTS 2.555.2 and earlier improperly determines that a redirect URL after login is legitimately pointing to Jenkins when it contains relative path segments (`./` or `../`), allowing attackers to perform phishing attacks.	2026-06-10	4.3
CVE-2026-53437	jenkins - multiple products	Jenkins 2.567 and earlier, LTS 2.555.2 and earlier improperly determines that a redirect URL after login is legitimately pointing to Jenkins when it contains tab or newline characters between `//`, allowing attackers to perform phishing attacks.	2026-06-10	4.3
CVE-2026-53438	jenkins - multiple products	A missing permission check in Jenkins 2.567 and earlier, LTS 2.555.2 and earlier allows attackers with Item/Cancel permission, but lacking Item/Read permission, to cancel queue items they do not have permission to view.	2026-06-10	4.3
CVE-2026-53439	jenkins - multiple products	Missing permission checks in Jenkins 2.567 and earlier, LTS 2.555.2 and earlier allow attackers with Overall/Read permission to determine other users' configured timezone and to enumerate view names of other users' "My Views".	2026-06-10	4.3
CVE-2026-53440	jenkins - multiple products	Jenkins 2.567 and earlier, LTS 2.555.2 and earlier does not ensure that the "from" parameter in the "Delegate to servlet container" security realm is safe to redirect to after login, allowing attackers to perform phishing attacks by redirecting users to an attacker-controlled domain.	2026-06-10	4.3
CVE-2026-41844	vmware - multiple products	A Spring MVC or Spring WebFlux application which configures a mapping for "/**" where the view name is not explicitly specified allows an attacker to craft a link resulting in a 302 redirect to an arbitrary external host via the redirect: prefix. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	4.2
CVE-2026-41854	vmware - multiple products	Due to incorrect host parsing, applications that rely on UriComponentsBuilder to parse and validate an externally provided URL string may be exposed to a server-side request forgery (SSRF) attack. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18.	2026-06-09	4.2
CVE-2026-0411	netgear - rbe970_firmware	An information disclosure vulnerability in the NETGEAR Orbi satellites (RBR/RBE/RBS Series) could allow a user connected to your network to gain administrator access to the Orbi router. The listed NETGEAR models are affected by this vulnerability. Orbi WiFi Systems without satellite devices are not impacted by this issue.	2026-06-09	4.2
CVE-2024-45636	ibm - security_qradar_edr	IBM Security QRadar EDR 3.12 through 3.12.24 stores user credentials in plain text which can be read by a local privileged user.	2026-06-11	4.1
CVE-2026-45642	microsoft - multiple products	Improper input validation in Microsoft Azure Attestation service and Device Health Attestation Service allows an authorized attacker to perform spoofing with a physical attack.	2026-06-09	3.9
CVE-2026-41848	vmware - multiple products	Applications may be vulnerable to a Regular Expression Denial of Service (ReDoS) attack if an attacker is able to provide a pattern which is then directly or indirectly supplied to one of the following methods in AntPathMatcher: match(String pattern, String path), matchStart(String pattern, String path), extractUriTemplateVariables(String pattern, String path). Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	3.7
CVE-2026-41852	vmware - multiple products	A vulnerability in Spring Expression Language (SpEL) evaluation logic allows for arbitrary zero-argument method invocation, even within restricted or read-only contexts, which may allow an attacker to invoke unintended application logic. Affected versions: Spring Framework 7.0.0 through 7.0.7; 6.2.0 through 6.2.18; 6.1.0 through 6.1.27; 5.3.0 through 5.3.48.	2026-06-09	3.7
CVE-2026-42768	openssl - multiple products	Issue summary: The CMS_decrypt and PKCS7_decrypt functions are vulnerable to Bleichenbacher-style attack when an attacker is able to provide the CMS or S/MIME messages and observe the error code and/or decryption output. Impact summary: The Bleichenbacher-style attack allows an attacker to use the victim's vulnerable application as a way to decrypt or sign messages with the victim's private RSA key. The attack is possible in 2 variants.	2026-06-09	3.7

		1. The decryption API (CMS_decrypt(), PKCS7_decrypt()) is used without providing the recipient certificate. In this case OpenSSL iterates over every KeyTransRecipientInfo (KTRI) without stopping at the first success. An attacker who authors a message with two KTRI entries — the first one wrapping a real CEK under the victim's public key, the second with an arbitrary probe ciphertext — obtains opportunity to iterate the 2nd KTRI to get a valid PKCS#1 v1.5 padding if the error code of the application is available. That is a Bleichenbacher oracle (Bleichenbacher, CRYPTO '98): an adaptive-chosen-ciphertext side channel from which the attacker decrypts any RSA ciphertext to the victim's key or forges any PKCS#1 v1.5 signature under it. 2. When the decryption API (CMS_decrypt(), PKCS7_decrypt()) is provided with the recipient certificate, and the recipient is not found, a random key is substituted. An attacker who authors a message and is able to compare both error code and the result of the decryption, can mount a Bleichenbacher oracle. We are not aware of any applications that provide a remote attacker an opportunity to mount an attack described in these scenarios. We consider the existence of such application very unlikely, and for this reason this CVE has been evaluated as Low severity. To avoid these attacks, when RSA PKCS#1 v1.5 Key Transport is in use, the invoked EVP_PKEY_decrypt() will use the implicit rejection mechanism described in draft-irtf-cfrg-rsa-guidance. In previous OpenSSL releases the implicit rejection was explicitly disabled. The implicit rejection mechanism always returns a plaintext value, the symmetric key. This result is deterministic for the ciphertext and the private key. The length of the decryption result can happen to match the length of the key of the symmetric cipher that was used for the content encryption. When a certificate is not provided, the last RecipientInfo producing a key that looks valid will be used. It may cause getting garbage content on decryption. As a proper way to deal with this a recipient certificate has to be provided to identify the particular RecipientInfo for decryption. The FIPS modules in 4.0, 3.6, 3.5, and 3.4 are not affected by this issue, as CMS and S/MIME processing happens outside the OpenSSL FIPS module boundary.		
CVE-2026-42770	openssl - multiple products	Issue summary: When EVP_PKEY_derive_set_peer() is called with a DHX (X9.42) peer key, the peer key is not properly checked for the subgroup membership. Impact summary: A malicious peer which presents an X9.42 key carrying the victim's p and g parameters, a forged q = r (a small prime factor of the cofactor (p−1)/q_local), and a public value Y of order r can recover the victim's private key after a small number of key exchange attempts. When EVP_PKEY_derive_set_peer() is called with a DHX (X9.42) peer key, the subgroup membership check Y^q ≡ 1 (mod p) is performed using the peer's own q parameter, not the local key's q. The peer's domain parameters are then matched against the domain parameters of the private key, but the value of q is not compared. A malicious peer who presents an X9.42 key carrying the victim's p, g, a forged q = r (a small prime factor of the cofactor), and a public value Y of order r passes all checks. The shared secret then takes only r distinct values, leaking priv mod r. Repeating for each small-prime factor of the cofactor and combining via CRT recovers the full private key (Lim–Lee / small-subgroup-confinement attack). The realistic attack surface is narrow: principally CMP deployments with long-lived RA/CA DHX keys and bespoke enterprise or government applications using X9.42 DHX static keys with interactive protocols and therefore this issue was assigned Low severity. The FIPS modules in 4.0, 3.6, 3.5, 3.4, and 3.0 are affected by this issue.	2026-06-09	3.7
CVE-2026-41694	vmware - multiple products	Since Spring Security SAML decrypts SAML Responses as well as elements of SAML LogoutRequests and LogoutResponses without requiring a valid signature, attackers may be able to craft these SAML payloads and use the Service Provider as a decryption oracle. Affected versions: Spring Security 5.7.0 through 5.7.23; 5.8.0 through 5.8.25; 6.3.0 through 6.3.16; 6.4.0 through 6.4.16; 6.5.0 through 6.5.10; 7.0.0 through 7.0.5.	2026-06-10	3.7

CVE-2026-41974	huawei - multiple products	Permission control vulnerability in service notifications. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	3.6
CVE-2026-48288	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page.	2026-06-09	3.5
CVE-2026-48289	adobe - multiple products	Adobe Experience Manager versions 6.5.24, LTS SP1, 2026.04 and earlier are affected by an Improper Input Validation vulnerability that could result in a Security feature bypass. A low-privileged attacker could leverage this vulnerability to bypass security measures and gain unauthorized write access. Exploitation of this issue requires user interaction in that a victim must visit a maliciously crafted URL or interact with a compromised web page.	2026-06-09	3.5
CVE-2022-48575	apple - macos	A person with access to a Mac may be able to bypass Login Window. A consistency issue was addressed with improved state handling. This issue is fixed in macOS Monterey 12.4.	2026-06-10	3.5
CVE-2026-11792	red hat - multiple products	A heap buffer overflow flaw was found in 389 Directory Server. When audit logging is enabled, the create_masked_entry_string() function in auditlog.c copies a fixed-length password mask into a precisely-sized heap buffer without checking available space. If a short cleartext password is logged (requiring non-default CLEAR password storage or a compromised replication peer), the copy overflows the buffer, corrupting heap memory and audit log output.	2026-06-09	3.3
CVE-2026-45455	microsoft - multiple products	Out-of-bounds read in Microsoft Office Excel allows an unauthorized attacker to disclose information over a network.	2026-06-09	3.3
CVE-2026-45459	microsoft - multiple products	Protection mechanism failure in Microsoft Office Excel allows an unauthorized attacker to bypass a security feature locally.	2026-06-09	3.3
CVE-2026-45466	microsoft - multiple products	Heap-based buffer overflow in Microsoft Office Word allows an unauthorized attacker to disclose information locally.	2026-06-09	3.3
CVE-2026-45485	microsoft - multiple products	Out-of-bounds read in Microsoft Office allows an unauthorized attacker to disclose information locally.	2026-06-09	3.3
CVE-2026-11675	google - chrome	Out of bounds read in Skia in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-09	3.1
CVE-2026-11684	google - chrome	Insufficient policy enforcement in Network in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the utility process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-09	3.1
CVE-2026-11686	google - chrome	Insufficient validation of untrusted input in Dawn in Google Chrome on macOS prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-09	3.1
CVE-2026-11691	google - chrome	Insufficient validation of untrusted input in New Tab Page in Google Chrome prior to 149.0.7827.103 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-09	3.1
CVE-2026-12017	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.115 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	2026-06-11	3.1
CVE-2026-12032	google - chrome	Inappropriate implementation in Passwords in Google Chrome on Android prior to 149.0.7827.115 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	2026-06-11	3.1
CVE-2026-41986	huawei - HarmonyOS	Logic bypass vulnerability in the file system. Impact: Successful exploitation of this vulnerability may affect availability.	2026-06-09	2.4
CVE-2026-11786	redhat - multiple products	A flaw was found in 389 Directory Server. The LDIF parser reads past the end of a heap buffer when processing attribute types with trailing semicolons during database import, causing an out-of-bounds read detectable under memory instrumentation.	2026-06-09	1.9
CVE-2026-0410	netgear - r7000_firmware	Authenticated administrators connected to the local network can gain elevated access to the router and make unauthorized changes to router software and functionality.	2026-06-09	1.9
CVE-2026-22899	qnap - file_station	A NULL pointer dereference vulnerability has been reported to affect File Station 6. If a remote attacker gains a user account, they can then exploit the vulnerability to launch a denial-of-service (DoS) attack. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5208 and later	2026-06-10	1.3
CVE-2026-24720	qnap - file_station	An allocation of resources without limits or throttling vulnerability has been reported to affect File Station 6. If a remote attacker gains a user account, they can then exploit the vulnerability to prevent other systems, applications, or processes from accessing the same type of resource. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5243 and later	2026-06-10	1.3
CVE-2026-26240	qnap - file_station	A buffer overflow vulnerability has been reported to affect File Station 5. The remote attackers can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5243 and later	2026-06-10	1.3
CVE-2026-26241	qnap - file_station	A buffer overflow vulnerability has been reported to affect File Station 5. The remote attackers can then exploit the vulnerability to modify memory or crash processes. We have already fixed the vulnerability in the following version: File Station 5 5.5.6.5243 and later	2026-06-10	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.