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 26 يوليو إلى 1 أغسطس. 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 26th of July to 1st of August. 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-2026-48449	adobe - multiple products	Adobe Campaign Classic (ACC) is affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-30	10
CVE-2026-66803	microsoft - azure_cosmos_db	Improper access control in Azure Cosmos DB allows an unauthorized attacker to execute code over a network.	2026-07-30	10
CVE-2026-64530	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net/sched: cls_api: Handle TC_ACT_CONSUMED in tcf_qevent_handle tcf_classify() can return TC_ACT_CONSUMED while the skb is held by the defragmentation engine (e.g. act_ct on out-of-order fragments). When that happens the skb is no longer owned by the caller and must not be touched again. tcf_qevent_handle() did not handle TC_ACT_CONSUMED: it fell through the switch and returned the skb to the caller as if classification had passed. The only qdisc that wires up qevents today is RED, via three call sites (qe_mark on RED_PROB_MARK/HARD_MARK, qe_early_drop on congestion_drop) red_enqueue() was continuing to operate on an skb it no longer owns in this case -- enqueueing it, dropping it, or updating statistics. Resulting in a UAF. tc qdisc add dev eth0 root handle 1: red ... qevent early_drop block 10 tc filter add block 10 ... action ct (with ct defrag enabled and traffic that produces out-of-order fragments, e.g. a fragmented UDP stream) Handle TC_ACT_CONSUMED in tcf_qevent_handle() the same way the ingress and egress fast paths do: treat it as stolen and return NULL without touching the skb. Unlike the TC_ACT_STOLEN case, the skb must not be dropped/freed here, as it is no longer owned by us.	2026-07-26	9.8
CVE-2026-64534	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: check INIT_FAILED before nvmet_req_uninit in digest error path In nvmet_tcp_try_recv_ddgst(), when a data digest mismatch is detected, nvmet_req_uninit() is called unconditionally. However, if the command arrived via the nvmet_tcp_handle_req_failure() path, nvmet_req_init() had returned false and percpu_ref_tryget_live() was never executed. The unconditional percpu_ref_put() inside nvmet_req_uninit() then causes a refcount underflow, leading to a WARNING in percpu_ref_switch_to_atomic_rcu, a use-after-free diagnostic, and eventually a permanent workqueue deadlock. Check cmd->flags & NVMET_TCP_F_INIT_FAILED before calling	2026-07-27	9.8

		nvmet_req_uninit(), matching the existing pattern in nvmet_tcp_execute_request().		
CVE-2026-64535	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: Fix potential UAF when ddgst mismatch Shivam Kumar found via vulnerability testing: When data digest is enabled on an NVMe/TCP connection and a digest mismatch occurs on a non-final H2C_DATA PDU during an R2T-based data transfer, the digest error handler in nvmet_tcp_try_recv_ddgst() calls nvmet_req_uninit() — which performs percpu_ref_put() on the submission queue — but does NOT mark the command as completed. It does not set cqe->status, does not modify rbytes_done, and does not clear any flag. When the subsequent fatal error triggers queue teardown, nvmet_tcp_uninit_data_in_cmds() iterates all commands, checks nvmet_tcp_need_data_in() for each one, and finds that the already-uninited command still appears to need data (because rbytes_done < transfer_len and cqe->status == 0). It therefore calls nvmet_req_uninit() a second time on the same command — a double percpu_ref_put against a single percpu_ref_get.	2026-07-27	9.8
CVE-2026-28911	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sonoma 14.8.8, macOS Tahoe 26.6. A malicious app may be able to corrupt memory of a system process.	2026-07-27	9.8
CVE-2026-28928	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-28982	apple - multiple products	A race condition was addressed with improved locking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A remote user may be able to cause unexpected system termination or corrupt kernel memory.	2026-07-27	9.8
CVE-2026-39873	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. Connecting to a malicious SMB server may lead to unexpected system termination.	2026-07-27	9.8
CVE-2026-43682	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A remote user may be able to cause unexpected system termination or corrupt kernel memory.	2026-07-27	9.8
CVE-2026-43694	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination or write kernel memory.	2026-07-27	9.8
CVE-2026-43710	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An attacker may be able to cause unexpected system termination or corrupt kernel memory.	2026-07-27	9.8
CVE-2026-43730	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to fingerprint the user.	2026-07-27	9.8
CVE-2026-43748	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-43750	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to execute arbitrary code out of its sandbox or with certain elevated privileges.	2026-07-27	9.8
CVE-2026-43757	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-43764	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-43769	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-43773	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. Mounting a maliciously crafted disk image may cause unexpected system termination or corrupt kernel memory.	2026-07-27	9.8
CVE-2026-43778	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination or corrupt kernel memory.	2026-07-27	9.8
CVE-2026-43779	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to intercept network connections intended for another process.	2026-07-27	9.8
CVE-2026-43793	apple - multiple products	An issue existed in the handling of environment variables. This issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-43799	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-43802	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-43803	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS	2026-07-27	9.8

		26.6, visionOS 26.6, watchOS 26.6. A remote attacker may be able to cause unexpected system termination.		
CVE-2026-43805	apple - multiple products	A race condition was addressed with improved state handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, watchOS 26.6. An app may be able to cause unexpected system termination or write kernel memory.	2026-07-27	9.8
CVE-2026-43807	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 26.5.2 and iPadOS 26.5.2, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.5.2, tvOS 26.6, visionOS 26.6, watchOS 26.6. A malicious accessory may be able to cause unexpected app termination.	2026-07-27	9.8
CVE-2026-43809	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-43810	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. A remote user may be able to cause unexpected system termination or corrupt kernel memory.	2026-07-27	9.8
CVE-2026-43812	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-43814	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-43822	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-64541	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net/smc: fix UAF in smc_cdc_rx_handler() by pinning the socket smc_cdc_rx_handler() looks up the connection by token under the link group's conns_lock, drops the lock, and then dereferences conn and the smc_sock derived from it, ending in sock_hold(&smc->sk) inside smc_cdc_msg_recv(). No reference is held across the lock release. The only reference pinning the socket while the connection is discoverable in the link group is taken in smc_lgr_register_conn() (sock_hold) and dropped in __smc_lgr_unregister_conn() (sock_put), both under conns_lock. Once the handler drops conns_lock, a concurrent close() -> smc_release() -> smc_conn_free() -> smc_lgr_unregister_conn() can drop that reference and free the smc_sock, so the handler's later sock_hold() runs on freed memory: WARNING: lib/refcount.c:25 at refcount_warn_saturate Workqueue: rxe_wq do_work refcount_warn_saturate (lib/refcount.c:25) smc_cdc_msg_recv (net/smc/smc_cdc.c:430) smc_cdc_rx_handler (net/smc/smc_cdc.c:502) smc_wr_rx_tasklet_fn (net/smc/smc_wr.c:445) tasklet_action_common (kernel/softirq.c:938) handle_softirqs (kernel/softirq.c:622) Kernel panic - not syncing: panic_on_warn set Only SMC-R is affected. The SMC-D receive tasklet is stopped by tasklet_kill(&conn->rx_tsklet) in smc_conn_free() before the connection is unregistered, so it cannot run concurrently with the free. Take the socket reference while still holding conns_lock, so the registration reference can no longer be the last one, and drop it once the handler is done.	2026-07-27	9.8
CVE-2026-64691	apple - macos	A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Tahoe 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-64694	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-64695	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A remote user may be able to cause unexpected system termination or corrupt kernel memory.	2026-07-27	9.8
CVE-2026-64696	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A remote user may be able to cause unexpected system termination or corrupt kernel memory.	2026-07-27	9.8
CVE-2026-64697	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination or corrupt kernel memory.	2026-07-27	9.8
CVE-2026-64698	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination or read kernel memory.	2026-07-27	9.8
CVE-2026-64700	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8

CVE-2026-64702	apple - multiple products	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to break out of its sandbox.	2026-07-27	9.8
CVE-2026-64703	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause a denial-of-service.	2026-07-27	9.8
CVE-2026-64704	apple - multiple products	A type confusion issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-64720	apple - multiple products	A race condition was addressed with improved state handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-64726	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An attacker in physical proximity may be able to corrupt process memory.	2026-07-27	9.8
CVE-2026-64727	apple - multiple products	A type confusion issue was addressed with improved memory handling. This issue is fixed in macOS Tahoe 26.6, tvOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-64729	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-64731	apple - multiple products	A path handling issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.7.8, macOS Tahoe 26.6. A malicious app may be able to break out of its sandbox.	2026-07-27	9.8
CVE-2026-64733	apple - multiple products	This issue was addressed with improved data protection. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to fingerprint the user.	2026-07-27	9.8
CVE-2026-64738	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A malicious app may be able to break out of its sandbox.	2026-07-27	9.8
CVE-2026-64746	apple - multiple products	An authorization issue was addressed with improved validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, visionOS 26.6, watchOS 26.6. An app may be able to add contacts without user authorization.	2026-07-27	9.8
CVE-2026-64751	apple - multiple products	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination or write kernel memory.	2026-07-27	9.8
CVE-2026-64762	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-64767	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A remote attacker may be able to cause unexpected system termination or corrupt kernel memory.	2026-07-27	9.8
CVE-2026-64769	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6. A remote attacker may be able to cause unexpected application termination or heap corruption.	2026-07-27	9.8
CVE-2026-64770	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6. A remote attacker may be able to cause unexpected application termination or heap corruption.	2026-07-27	9.8
CVE-2026-64771	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6. A remote attacker may be able to cause unexpected application termination or heap corruption.	2026-07-27	9.8
CVE-2026-64772	apple - multiple products	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6. A remote attacker may be able to cause unexpected application termination or heap corruption.	2026-07-27	9.8
CVE-2026-64774	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6. A remote attacker may be able to cause unexpected application termination or heap corruption.	2026-07-27	9.8
CVE-2026-64775	apple - multiple products	A memory initialization issue was addressed with improved memory handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	9.8
CVE-2026-66713	apache - axis2\/java	Deserialization of Untrusted Data (CWE-502) in the Tribes-based clustering component in Apache Software Foundation Apache Axis2/Java through 2.0.0 on Apache Tomcat (only when Tribes clustering is enabled, which is off by default) allows an unauthenticated remote attacker with network access to the clustering port to execute arbitrary code via a crafted serialized Java object delivered to the cluster channel and deserialized in org.apache.axis2.clustering.tribes.Axis2ChannelListener#messageReceived. Users are recommended to upgrade to version 2.0.1, which fixes this issue by removing the clustering feature entirely.	2026-07-28	9.8

CVE-2026-14446	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to broken access control/privilege escalation in the administrative console.	2026-07-28	9.8
CVE-2026-14512	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 traditional is vulnerable to pre-authentication unsafe deserialization which could allow a remote attacker to bypass authentication or execute arbitrary code.	2026-07-28	9.8
CVE-2026-59243	apache - apache-airflow-providers-fab	The FAB auth manager's Azure AD OAuth login defaulted `verify_signature=False` when decoding the ID token, so an attacker able to present a forged or unsigned (`alg:none`) ID token to the OAuth callback could bypass authentication and log in as an arbitrary user, including one holding the Admin role (CWE-347). Deployments running the FAB auth manager with the Azure AD OAuth login path under its default configuration are affected; the Authentik path already defaulted to `True`. This issue affects `apache-airflow-providers-fab` before 3.7.3. Users are advised to upgrade to `apache-airflow-providers-fab` 3.7.3, which defaults `verify_signature=True`.	2026-07-29	9.8
CVE-2026-59309	vmware - multiple products	VMware vCenter contains an authentication bypass vulnerability in the VMware Directory Service. A malicious actor with network access to vCenter may exploit this issue to bypass authentication and gain unauthorized access to the system.	2026-07-30	9.8
CVE-2026-59310	vmware - multiple products	VMware vCenter contains a directory traversal vulnerability in the Syslog server. A malicious actor with network access to vCenter may exploit this issue to execute arbitrary code.	2026-07-30	9.8
CVE-2026-15435	ibm - multiple products	IBM App Connect Enterprise 13.0.1.0 through 13.0.7.2, and 12.0.1.0 through 12.0.12.27 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to write arbitrary files on the system.	2026-07-30	9.8
CVE-2026-28323	solarwinds - Web Help Desk	SolarWinds Web Help Desk is found to be affected by a SAML authentication bypass vulnerability. This requires the SAML 2.0 authentication method to be enabled.	2026-07-30	9.8
CVE-2026-28812	apache - jspwiki	UserManager lack of checks allows impersonation in Apache JSPWiki up to 2.12.3 which may allow attackers to escalate privileges. Users are recommended to upgrade to version 2.12.4 or newer which fixes this issue.	2026-07-30	9.8
CVE-2026-52680	apache - kyuubi	Apache Kyuubi REST batch multipart upload handling uses the client-supplied multipart filename when creating a temporary uploaded resource. A remote attacker who can access the REST batch upload endpoint can provide path traversal sequences in the filename and cause the Kyuubi server process to write controlled content outside the intended upload directory, subject to filesystem permissions. This issue affects Apache Kyuubi: from 1.7.0 through 1.11.1. Users are recommended to upgrade to version 1.12.0, which fixes the issue.	2026-07-30	9.8
CVE-2026-12118	ibm - webMethods Integration (on prem)	IBM webMethods Integration (on prem) 10.15, 10.11 could allow an unauthenticated remote attacker to execute arbitrary code on the system due to the deserialization of untrusted data.	2026-07-30	9.8
CVE-2026-12943	ibm - multiple products	IBM HMC V10.3.1050.0 through 10.3.1064.0 and IBM HMC V11.1.1110.0 through 11.1.1112.0 Management systems in IBM Power environments (HMC and Novalink) could allow an unauthenticated user to execute arbitrary commands with elevated privileges on the system due to improper validation of user supplied input.	2026-07-30	9.8
CVE-2026-17651	google - chrome	Insufficient validation of untrusted input in Dawn in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-07-30	9.6
CVE-2026-17652	google - chrome	Use after free in Views in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	9.6
CVE-2026-17655	google - chrome	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-07-30	9.6
CVE-2026-17656	google - chrome	Use after free in Ozone in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-07-30	9.6
CVE-2026-17669	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17670	google - chrome	Use after free in Views in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17671	google - chrome	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17672	google - chrome	Insufficient validation of untrusted input in Chromecast in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17673	google - chrome	Integer overflow in QUIC in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17675	google - chrome	Out of bounds write in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17676	google - chrome	Inappropriate implementation in ANGLE in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17680	google - chrome	Heap buffer overflow in Color in Google Chrome on ChromeOS prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6

CVE-2026-17681	google - chrome	Insufficient validation of untrusted input in Web Authentication in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17682	google - chrome	Integer overflow in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17684	google - chrome	Insufficient validation of untrusted input in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17687	google - chrome	Type Confusion in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17688	google - chrome	Use after free in Input in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17691	google - chrome	Out of bounds write in ANGLE in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17692	google - chrome	Use after free in DataTransfer in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17695	google - chrome	Inappropriate implementation in ANGLE in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17697	google - chrome	Type Confusion in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17701	google - Chrome	Insufficient validation of untrusted input in ANGLE in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17704	google - chrome	Use after free in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17708	google - chrome	Use after free in Audio in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17709	google - chrome	Race in Downloads in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17710	google - chrome	Inappropriate implementation in MHTML in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17711	google - chrome	Race in Downloads in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17713	google - Chrome	Insufficient validation of untrusted input in Accessibility in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17717	google - chrome	Integer overflow in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17718	google - chrome	Use after free in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17721	google - chrome	Out of bounds write in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17726	google - chrome	Integer overflow in WebGL in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17727	google - chrome	Out of bounds write in WebGL in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	9.6
CVE-2026-17738	google - Chrome	Insufficient validation of untrusted input in Payments in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	9.6
CVE-2026-17749	google - Chrome	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 151.0.7922.72 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: Medium)	2026-07-30	9.6
CVE-2026-17758	google - chrome	Heap buffer overflow in Dawn in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	9.6
CVE-2026-17768	google - chrome	Insufficient validation of untrusted input in WebSockets in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	9.6
CVE-2026-17801	google - chrome	Out of bounds read and write in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	9.6
CVE-2026-17803	google - chrome	Insufficient validation of untrusted input in Save to Drive in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted PDF file. (Chromium security severity: Medium)	2026-07-30	9.6

CVE-2026-17804	google - chrome	Use after free in Media in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	9.6
CVE-2026-17832	google - chrome	Use after free in ANGLE in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	9.6
CVE-2026-17834	google - chrome	Insufficient validation of untrusted input in Passwords in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	9.6
CVE-2026-17837	google - chrome	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	9.6
CVE-2026-17847	google - chrome	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	9.6
CVE-2026-17848	google - chrome	Integer overflow in Codecs in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: Medium)	2026-07-30	9.6
CVE-2026-17855	google - chrome	Race in DevTools in Google Chrome on Mac prior to 151.0.7922.72 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)	2026-07-30	9.6
CVE-2026-17856	google - chrome	Inappropriate implementation in Network in Google Chrome on Mac prior to 151.0.7922.72 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)	2026-07-30	9.6
CVE-2026-17865	google - chrome	Inappropriate implementation in Crypto in Google Chrome on Mac prior to 151.0.7922.72 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)	2026-07-30	9.6
CVE-2026-17924	google - chrome	Use after free in DNS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	9.6
CVE-2026-17940	google - chrome	Insufficient validation of untrusted input in Picture-in-Picture in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	9.6
CVE-2026-17947	google - chrome	Use after free in WebSockets in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	9.6
CVE-2026-17987	google - chrome	Insufficient validation of untrusted input in Notifications in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted PDF file. (Chromium security severity: Low)	2026-07-30	9.6
CVE-2026-17990	google - chrome	Insufficient validation of untrusted input in WebAuthn in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted PDF file. (Chromium security severity: Low)	2026-07-30	9.6
CVE-2026-17991	google - chrome	Insufficient validation of untrusted input in AI in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	9.6
CVE-2026-18002	google - chrome	Insufficient validation of untrusted input in Google Lens in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	9.6
CVE-2026-18015	google - chrome	Inappropriate implementation in Tint in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	9.6
CVE-2026-14529	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 traditional is vulnerable to server-side request forgery (SSRF) when the SIP container feature (sipServlet-1.1) is enabled.	2026-07-29	9.4
CVE-2026-55971	apache - thrift	Heap-based Buffer Overflow vulnerability in Apache Thrift C++ bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	9.3
CVE-2026-64740	apple - multiple products	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6. A malicious app may be able to break out of its sandbox.	2026-07-27	9.3
CVE-2026-14973	ibm - Aspera Desktop App	IBM Aspera Desktop App 1.0.5 through 1.0.19 IBM Aspera for desktop can allow files to be written outside of the user's selected download destination.	2026-07-28	9.3
CVE-2026-18236	google - Google-ADK	A vulnerability in the Agent Development Kit (ADK) allows for continuation forgery in tool confirmations. An attacker who is able to manipulate or inject events into the session history can execute unauthorized tools by forging a tool confirmation response. This is possible because the framework did not verify if the target tool was registered to the executing agent, did not validate if the tool actually required confirmation, and did not match the confirmation arguments against the original tool call event in the history.	2026-07-29	9.3
CVE-2026-47876	vmware - multiple products	VMware ESX contains an out-of-bounds write vulnerability in the VMXNET3 virtual network adapter. A malicious actor with local administrative privileges on a virtual machine with VMXNET3 virtual network adapter may exploit this issue to execute code on the host. Non VMXNET3 virtual adapters are not affected by this issue.	2026-07-30	9.3
CVE-2026-11707	ibm - Tivoli System Automation Application Manager	IBM Tivoli System Automation Application Manager 4.1 and IBM WebSphere Application Server is affected by a cross-site scripting vulnerability in the administrative console login page.	2026-07-30	9.3
CVE-2026-58154	apache - multiple products	Apache Traffic Server can write out of bounds or overflow integers while parsing MIME and HTTP headers.	2026-07-29	9.2

		This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.		
CVE-2026-58155	apache - multiple products	Apache Traffic Server truncates over-long header names, allowing header aliasing, request smuggling, and policy bypass. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	9.2
CVE-2026-58161	apache - multiple products	Apache Traffic Server can crash from null dereferences and dangling references in TLS and SNI handling. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	9.2
CVE-2026-58179	apache - multiple products	The Apache Traffic Server regex_remap plugin overflows the stack and integers from substitution input. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	9.2
CVE-2026-48144	apache - thrift	Improper Validation of Certificate with Host Mismatch vulnerability in Apache Thrift c_glib bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	9.1

CVE-2026-64551	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved:
		
		sctp: validate STALE_COOKIE cause length before reading staleness
		
		When an ERROR chunk with a STALE_COOKIE cause is received in the COOKIE_ECHOED state, sctp_sf_do_5_2_6_stale() reads the 4-byte Measure of Staleness that follows the cause header:
		
		err = (struct sctp_errhdr *)(chunk->skb->data);
		stale = ntohl(*(__be32 *)((u8 *)err + sizeof(*err)));
		
		err is the first cause in the chunk, not the STALE_COOKIE cause that caused the dispatch, and nothing guarantees the staleness field is present. sctp_walk_errors() only requires a cause to be as long as the 4-byte header, so for a STALE_COOKIE cause of length 4 the read runs past the cause, and for a minimal ERROR chunk past skb->tail. The value is echoed to the peer in the Cookie Preservative of the reply INIT, leaking uninitialized memory.
		
		sctp_sf_cookie_echoed_err() already walks to the STALE_COOKIE cause, so check its length there and pass it to sctp_sf_do_5_2_6_stale(), which reads that cause instead of the first one. A STALE_COOKIE cause too short to hold the staleness field is discarded.
		
		The read is reachable by any peer that can drive an association into COOKIE_ECHOED, including an unprivileged process using a raw SCTP socket in a user and network namespace.
			2026-07-27	9.1

CVE-2026-14958	ibm - aspera_faspex	IBM Aspera Faspex 5 5.0.0 through 5.0.15.4 could allow a remote authenticated attacker to execute arbitrary code due to unquoted shell interpolation.	2026-07-28	9.1
CVE-2026-14959	ibm - aspera_faspex	IBM Aspera Faspex 5 5.0.0 through 5.0.15.4 could allow a remote authenticated attacker to execute arbitrary code due to shell command injection.	2026-07-28	9.1
CVE-2026-17666	google - chrome	Cryptographic Flaw in Enterprise in Google Chrome prior to 151.0.7922.72 allowed an attacker in a privileged network position to bypass discretionary access control via malicious network traffic. (Chromium security severity: High)	2026-07-30	9.1
CVE-2026-28931	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, watchOS 26.6. Connecting to a malicious NFS server may lead to kernel memory corruption.	2026-07-27	8.8
CVE-2026-43818	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. Processing a maliciously crafted image may lead to arbitrary code execution.	2026-07-27	8.8
CVE-2026-64554	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netfilter: bridge: fix stale prevhdr pointer in br_ip6_fragment() br_ip6_fragment() gets prevhdr, a pointer into the skb head, from ip6_find_1stfragopt(), then calls skb_checksum_help(). For a cloned skb skb_checksum_help() reallocates the head via pskb_expand_head(), leaving prevhdr dangling. It is later dereferenced in ip6_frag_next(), causing a	2026-07-27	8.8

		use-after-free write. Save prevhdr's offset before skb_checksum_help() and recompute it after, like commit ef0efcd3bd3f ("ipv6: Fix dangling pointer when ipv6 fragment"). BUG: KASAN: slab-use-after-free in ip6_frag_next (net/ipv6/ip6_output.c:857) Write of size 1 at addr ffff888013ff5016 by task exploit/141 Call Trace: ... kasan_report (mm/kasan/report.c:595) ip6_frag_next (net/ipv6/ip6_output.c:857) br_ip6_fragment (net/ipv6/netfilter.c:212) nf_ct_bridge_post (net/bridge/netfilter/nf_conntrack_bridge.c:407) nf_hook_slow (net/netfilter/core.c:619) br_forward_finish (net/bridge/br_forward.c:66) __br_forward (net/bridge/br_forward.c:115) maybe_deliver (net/bridge/br_forward.c:191) br_flood (net/bridge/br_forward.c:245) br_handle_frame_finish (net/bridge/br_input.c:229) br_handle_frame (net/bridge/br_input.c:442) ... packet_sendmsg (net/packet/af_packet.c:3114) ... do_syscall_64 (arch/x86/entry/syscall_64.c:94) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:121) Kernel panic - not syncing: Fatal exception in interrupt		
CVE-2026-64555	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: KVM: arm64: nv: Fix SPSR_EL2 restore in kvm_hyp_handle_mops() kvm_hyp_handle_mops() resets the single-step state machine as part of rewinding state for a MOPS exception by modifying vcpu_cpsr() and writing the result directly into hardware. In the case of nested virtualization, vcpu_cpsr() is a synthetic value such that the rest of KVM can deal with vEL2 cleanly. That means the value requires translation before being written into hardware, which is unfortunately missing from the MOPS handler. Fix it by directly modifying SPSR_EL2 and avoiding the synthetic state altogether, which will be resynchronized on the next 'full' exit back to KVM.	2026-07-27	8.8
CVE-2026-64739	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An attacker may be able to cause unexpected app termination.	2026-07-27	8.8
CVE-2026-64757	apple - multiple products	A memory corruption issue was addressed with improved state management. This issue is fixed in Safari 26.6, iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, visionOS 26.6, watchOS 26.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2026-07-27	8.8
CVE-2026-64783	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in Safari 26.6, iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, visionOS 26.6, watchOS 26.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2026-07-27	8.8
CVE-2026-64557	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: L2CAP: Fix use-after-free in l2cap_sock_new_connection_cb() l2cap_sock_new_connection_cb() returned l2cap_pi(sk)->chan after release_sock(parent). Once the parent lock is dropped the newly enqueued child socket sk is reachable via the accept queue, so another task can accept and free it before the callback dereferences sk, resulting in a use-after-free. Rework the ->new_connection() op so the core, rather than the callback, owns the child channel's lifetime. The op now receives a pre-allocated new_chan and returns an errno instead of allocating and returning a channel. l2cap_new_connection() allocates the child channel and links it into the conn list via __l2cap_chan_add() before invoking the callback, so the conn-list reference keeps the channel alive once release_sock(parent) exposes the socket to other tasks. Channel configuration that was duplicated in l2cap_sock_init() and the various new_connection callbacks is consolidated into l2cap_chan_set_defaults(), which now inherits from the parent channel when one is supplied.	2026-07-29	8.8
CVE-2026-50622	apache - atlas	Description: Missing Authorization in Apache Atlas. A missing authorization vulnerability in Apache Atlas's admin endpoints allows any authenticated user, regardless of their assigned role, to perform administrative operations.	2026-07-29	8.8

		Affect Version: This issue affects Apache Atlas: from 0.8 through 2.5.0. Mitigation: Users are recommended to upgrade to version 2.6.0, which fixes the issue.		
CVE-2026-17658	google - chrome	Use after free in V8 in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.8
CVE-2026-17661	google - Chrome	Use after free in Loader in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.8
CVE-2026-17665	google - chrome	Use after free in V8 in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.8
CVE-2026-17677	google - chrome	Inappropriate implementation in ANGLE in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.8
CVE-2026-17678	google - chrome	Out of bounds read in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.8
CVE-2026-17685	google - chrome	Use after free in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.8
CVE-2026-17694	google - chrome	Use after free in DOM in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.8
CVE-2026-17705	google - chrome	Integer overflow in libxml in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.8
CVE-2026-17712	google - chrome	Race in Skia in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.8
CVE-2026-17719	google - chrome	Use after free in Input in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.8
CVE-2026-17725	google - chrome	Type Confusion in V8 in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.8
CVE-2026-17729	google - Chrome	Use after free in V8 in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	8.8
CVE-2026-17751	google - chrome	Inappropriate implementation in AdFilter in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	8.8
CVE-2026-17752	google - chrome	Use after free in Views in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	8.8
CVE-2026-17778	google - chrome	Use after free in Extensions in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-07-30	8.8
CVE-2026-17784	google - chrome	Use after free in Audio in Google Chrome on Mac prior to 151.0.7922.72 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)	2026-07-30	8.8
CVE-2026-17786	google - chrome	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to perform privilege escalation via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-07-30	8.8
CVE-2026-17807	google - chrome	Use after free in V8 in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	8.8
CVE-2026-17836	google - chrome	Use after free in V8 in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	8.8
CVE-2026-17868	google - chrome	Insufficient policy enforcement in USB in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform privilege escalation via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	8.8
CVE-2026-17875	google - chrome	Use after free in PDFium in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: Medium)	2026-07-30	8.8
CVE-2026-17881	google - chrome	Integer overflow in WebXR in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	8.8
CVE-2026-17884	google - chrome	Object lifecycle issue in WebRTC in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	8.8
CVE-2026-17886	google - chrome	Use after free in Enterprise in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	8.8
CVE-2026-17894	google - chrome	Use after free in Views in Google Chrome on Linux prior to 151.0.7922.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	8.8

CVE-2026-17899	google - chrome	Insufficient policy enforcement in DevTools in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to perform privilege escalation via a crafted Chrome Extension. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-17918	google - chrome	Use after free in Sync in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-17920	google - chrome	Use after free in V8 in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-17922	google - chrome	Inappropriate implementation in Enterprise in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-17935	google - chrome	Heap buffer overflow in Codecs in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-17950	google - chrome	Inappropriate implementation in Safebrowsing in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code via a malicious file. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-17951	google - chrome	Heap buffer overflow in WebRTC in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-17956	google - chrome	Inappropriate implementation in Scheduling in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-17967	google - chrome	Use after free in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-17969	google - chrome	Inappropriate implementation in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-17971	google - chrome	Inappropriate implementation in Frame in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-17989	google - chrome	Type Confusion in V8 in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-18012	google - chrome	Use after free in PDFium in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-18017	google - chrome	Use after free in Dawn in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	8.8
CVE-2026-16526	red hat - multiple products	A flaw in the PCP linux_sockets module exposes an unsecured internal connection. An attacker with initial code execution can exploit this to escalate privileges and execute arbitrary commands as root.	2026-07-30	8.8
CVE-2026-14522	ibm - multiple products	IBM App Connect Enterprise 13.0.1.0 through 13.0.7.2, and 12.0.1.0 through 12.0.12.27 could allow a remote attacker to execute arbitrary commands due to improper neutralization of CRLF characters.	2026-07-30	8.8
CVE-2026-28813	apache - jspwiki	Apache JSPWiki, up to 2.12.3, is vulnerable to JSON Hijacking, which leads to csrf vulnerabilities. Users are recommended to upgrade to version 2.12.4, which fixes this issue.	2026-07-30	8.8
CVE-2026-58222	red hat - multiple products	A security flaw combining LDAP filter injection and improper authorization checks was found in Samba Active Directory Domain Controller (AD DC). When processing LDAP Compare requests, Samba fails to properly validate user-supplied attribute names and executes the resulting internal database search in a trusted context, bypassing normal Access Control List (ACL) enforcement. An authenticated low-privilege domain user can exploit these flaws to disclose confidential Active Directory attributes that would normally be inaccessible. The disclosed information may be leveraged to derive sensitive authentication material, potentially leading to privilege escalation and complete domain compromise. For example: In deployments configured with Group Managed Service Accounts (gMSAs), an attacker can extract the "msKds-RootKeyData" attribute and derive gMSA passwords offline, potentially leading to complete domain compromise if privileged gMSAs are present.	2026-07-30	8.8
CVE-2026-43871	apache - thrift	Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in Apache Thrift Python, Go, PHP and Java bindings.This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	8.7
CVE-2026-48586	apache - thrift	Improper Handling of Highly Compressed Data (Data Amplification) vulnerability in Apache Thrift C++, Java, Python, Go, D, C/GLib bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	8.7
CVE-2026-55968	apache - thrift	Inefficient Algorithmic Complexity, Allocation of Resources Without Limits or Throttling vulnerability in Apache Thrift Node.js bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	8.7
CVE-2026-55969	apache - thrift	Integer Overflow or Wraparound vulnerability in Apache Thrift C++, c_glib, Go, netstd, Delphi and Haxe bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	8.7

CVE-2026-58389	apache - thrift	Allocation of Resources Without Limits or Throttling vulnerability in Apache Thrift Rust bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	8.7
CVE-2026-58662	apache - thrift	Improper Validation of Specified Quantity in Input, Out-of-bounds Read vulnerability in Apache Thrift C++ bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	8.7
CVE-2026-16347	mikrotik - multiple products	MikroTik RouterOS contains a weakness in its API authentication handling that lacks effective safeguards against excessive login attempts. The system does not enforce meaningful rate-limiting, account lockout, or source-based restrictions, allowing repeated authentication failures to proceed without defensive response. In some versions, a fixed per-connection delay is present, but it can be bypassed through concurrent sessions, resulting in continued high-volume attempts. This deficiency increases the risk that an attacker could eventually obtain valid credentials and gain unauthorized access to administrative services.	2026-07-28	8.7
CVE-2026-15064	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 is vulnerable to HTTP Response Smuggling due to improper handling of non-standard HTTP version tokens.	2026-07-28	8.7
CVE-2026-15325	ibm - multiple products	IBM WebSphere Application Server and IBM WebSphere Application Server - Liberty is vulnerable to HTTP request smuggling due to improper handling of TRACE requests.	2026-07-28	8.7
CVE-2026-58151	apache - multiple products	Apache Traffic Server can be crashed or driven to resource exhaustion by abusive HTTP/2 framing and flow-control. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.7
CVE-2026-17735	google - Chrome	Insufficient validation of untrusted input in BFCache in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	8.7
CVE-2026-28973	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, watchOS 26.6. A malicious app may be able to break out of its sandbox.	2026-07-27	8.6
CVE-2026-43760	apple - multiple products	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to access user-sensitive data.	2026-07-27	8.6
CVE-2026-45293	wordpress - WordPress-Coding-Standards	WordPress Coding Standards is a set of PHP_CodeSniffer rules (sniffs) that enforce WordPress coding conventions. From 0.14.1 until 3.4.1, the WordPress.WP.EnqueuedResourceParameters sniff (active in the WordPress and WordPress-Extra rulesets) reconstructed the $ver argument passed to functions such as wp_enqueue_script() and ran it through eval() inside its is_falsy() method, so a maliciously crafted argument such as 'system'('id') would execute during a scan; as a result, running PHPCS with WordPressCS over untrusted PHP (for example a CI pipeline that lints pull requests, or a developer reviewing third-party code) could lead to arbitrary command execution on the scanning host. The WordPress-Core and WordPress-Docs rulesets are not affected. This issue is fixed in version 3.4.1.	2026-07-28	8.6
CVE-2026-48388	adobe - photoshop_installer	Adobe Photoshop Installer was affected by an Uncontrolled Search Path Element vulnerability that could have resulted in arbitrary code execution in the context of the current user. An attacker could have exploited this vulnerability by placing a malicious library in a directory searched by the installer. Exploitation of this issue required user interaction in that a victim must have been running the installer. Scope is changed.	2026-07-28	8.6
CVE-2026-48395	adobe - multiple products	Bridge is affected by an Untrusted Search Path vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-07-28	8.6
CVE-2026-48396	adobe - multiple products	Bridge is affected by an Incorrect Authorization vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-07-28	8.6
CVE-2026-17699	google - chrome	Use after free in Views in Google Chrome prior to 151.0.7922.72 allowed a local attacker to potentially perform a sandbox escape via a malicious file. (Chromium security severity: High)	2026-07-30	8.6
CVE-2026-48448	adobe - multiple products	Adobe Campaign Classic (ACC) is affected by an Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to gain file system read access. Exploitation of this issue does not require user interaction. Scope is changed.	2026-07-30	8.6
CVE-2026-49332	red hat - multiple products	A flaw was found in openshift/oauth-proxy. The proxy sets authenticated identity headers using only dash-variant keys (X-Forwarded-User) but does not strip underscore-variant keys (X_Forwarded_User) from incoming requests. WSGI and PHP frameworks normalize both variants to the same variable, allowing an authenticated low-privilege user to smuggle a forged identity that may override the legitimate authenticated identity in the upstream application.	2026-07-28	8.5
CVE-2026-11536	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 is affected by a remote code execution vulnerability in the SOAP/JMX connector.	2026-07-30	8.5
CVE-2026-10079	red hat - multiple products	A flaw was found in Red Hat Advanced Cluster Security for Kubernetes (RHACS). When processing Kubernetes Deployments, ACS replaces deployment identity metadata based on the openshift.io/encoded-deployment-config label. A user with permission to create Deployments can set this label to "null", causing ACS to treat the workload as having empty UID, name and labels and namespace "default". This bypasses deploy-time policy detection and enforcement visibility,	2026-07-31	8.5

		prevents correct persistence in Central and breaks violation reporting and compliance correlation for the affected deployment.		
CVE-2026-9044	tp-link - archer_axe75_firmware	An OS command injection vulnerability exists in the VPN module of TP-Link AXE75 V1 routers. This vulnerability allows an adjacent, authenticated attacker to execute arbitrary commands on the device by importing a specially crafted VPN client configuration file. The issue arises from improper filtering of special characters. Successful exploitation of this vulnerability may enable an attacker to gain full control of the affected device, potentially compromising configuration integrity, network security, and service availability.	2026-07-31	8.5
CVE-2026-16481	google - MCP Toolbox for Databases (googleapis/mcp-toolbox)	A Server-Side Request Forgery (SSRF) and credential exfiltration vulnerability exists in the cloud-healthcare-fhir-fetch-page tool of googleapis/mcp-toolbox. The tool takes an unvalidated pageURL parameter from the client and issues an HTTP GET request to it using an authenticated client. The underlying transport automatically attaches an Authorization: Bearer header to every outbound request regardless of the destination host. An attacker can supply an arbitrary external URL to the pageURL parameter (either directly via the tool execution payload or implicitly via data-driven pagination tracking loops), leading Toolbox into sending its OAuth/service-account access token to an attacker-controlled listener. Depending on the configuration, this leaks either the end-user's token or the broader service-account access token (ADC), potentially exposing Protected Health Information (PHI) and secondary Google Cloud Platform services.	2026-07-27	8.4
CVE-2026-64548	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: bpf, sockmap: reject overflowing copy + len in bpf_msg_push_data() When the scatterlist ring is full or nearly full, bpf_msg_push_data() enters a copy fallback path and computes copy + len for the page allocation size. Since len comes from BPF with arg3_type = ARG_ANYTHING and both are u32, a crafted len can wrap the sum to a small value, causing an undersized allocation followed by an out-of-bounds memcpy. BUG: unable to handle page fault for address: ffffed104089a402 Oops: Oops: 0000 [#1] SMP KASAN NOPTI Call Trace: __asan_memcpy (mm/kasan/shadow.c:105) bpf_msg_push_data (net/core/filter.c:2852 net/core/filter.c:2788) bpf_prog_9ed8b5711920a7d7+0x2e/0x36 sk_psock_msg_verdict (net/core/skmsg.c:934) tcp_bpf_sendmsg (net/ipv4/tcp_bpf.c:421 net/ipv4/tcp_bpf.c:584) __sys_sendto (net/socket.c:2206) do_syscall_64 (arch/x86/entry/syscall_64.c:94) entry_SYSCALL_64_after_hwframe (arch/x86/entry/entry_64.S:130) Add an overflow check before the allocation.	2026-07-27	8.4
CVE-2026-64552	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: virtio-net: fix len check in receive_big() receive_big() bounds the device-announced length by (big_packets_num_skbfrags + 1) * PAGE_SIZE. That is still too loose: add_recvbuf_big() sets sg[1] to start at offset sizeof(struct padded_vnet_hdr) into the first page, so the chain actually carries hdr_len + (PAGE_SIZE - sizeof(padded_vnet_hdr)) + big_packets_num_skbfrags * PAGE_SIZE bytes -- 20 bytes less than the check allows for the common hdr_len == 12 case. A malicious virtio backend can announce a len in that gap. page_to_skb() then walks one frag past the page chain, storing a NULL page->private into skb_shinfo()->frags[MAX_SKB_FRAGS], which is both an out-of-bounds write past the static frag array and a NULL frag handed up the rx path. Bound len by the size add_recvbuf_big() actually advertised.	2026-07-27	8.4
CVE-2026-58162	apache - multiple products	The Apache Traffic Server certifier plugin generates certificates based on attacker-controlled client SNI. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.4
CVE-2026-58188	apache - multiple products	Several Apache Traffic Server experimental plugins have memory-safety and limit-bypass errors. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.4
CVE-2026-17716	google - Chrome	Use after free in Updater in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to perform privilege escalation via malicious network traffic. (Chromium security severity: High)	2026-07-30	8.4

CVE-2026-17877	google - chrome	Inappropriate implementation in Chromoting in Google Chrome on Linux prior to 151.0.7922.72 allowed a local attacker to perform OS-level privilege escalation via malicious network traffic. (Chromium security severity: Medium)	2026-07-30	8.4
CVE-2026-11885	ibm - PowerVM Hypervisor	IBM PowerVM Hypervisor FW1110.00 through FW1110.20, FW1060.00 through FW1060.71, and FW950.00 through FW950.H1 A carefully crafted OS hypervisor call can cause the PowerVM hypervisor to crash or compromise OS memory integrity.	2026-07-30	8.4
CVE-2026-10535	ibm - multiple products	IBM Db2 11.5.0 through 11.5.9, and 12.1.0 through 12.1.4 is vulnerable to buffer overflow in setgid helper db2flacc.	2026-07-30	8.4
CVE-2026-58163	apache - multiple products	Apache Traffic Server mishandles on-disk cache fields and object lifetimes, corrupting state or crashing. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.3
CVE-2026-58164	apache - multiple products	Apache Traffic Server has use-after-free and time-of-check/time-of-use errors in remap configuration handling. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.3
CVE-2026-58177	apache - traffic_server	The Apache Traffic Server Cripts framework has out-of-bounds writes, path traversal, and use-after-free errors. This issue affects Apache Traffic Server: from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 10.1.4, which fix the issue.	2026-07-29	8.3
CVE-2026-58184	apache - multiple products	The Apache Traffic Server header_rewrite plugin can crash or corrupt memory during cookie operations and CIDR condition matching. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.3
CVE-2026-17650	google - chrome	Use after free in Compositing in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	8.3
CVE-2026-17653	google - chrome	Use after free in Skia in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	8.3
CVE-2026-17657	google - chrome	Use after free in Navigation in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.3
CVE-2026-17660	google - chrome	Insufficient validation of untrusted input in Network in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.3
CVE-2026-17663	google - chrome	Insufficient validation of untrusted input in GPU in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.3
CVE-2026-17722	google - chrome	Object lifecycle issue in WebView in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.3
CVE-2026-17723	google - Chrome	Use after free in Media in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.3
CVE-2026-14980	ibm - websphere_application_server	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 is vulnerable to cross-site request forgery which could allow an attacker to perform SSRF attacks with elevated privileges when the collectiveController-1.0 feature is enabled.	2026-07-30	8.3
CVE-2026-48145	apache - thrift	Improper Validation of Certificate with Host Mismatch vulnerability in Apache Thrift C++ bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	8.2
CVE-2026-43772	apple - multiple products	A path traversal issue was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to break out of its sandbox.	2026-07-27	8.2
CVE-2026-64737	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A malicious app may be able to break out of its sandbox.	2026-07-27	8.2
CVE-2026-48390	adobe - multiple products	Bridge is affected by an Incorrect Authorization vulnerability that could result in privilege escalation. An attacker could leverage this vulnerability to gain unauthorized read and write access. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-07-28	8.2
CVE-2026-48391	adobe - multiple products	Bridge is affected by an Untrusted Search Path vulnerability that could result in arbitrary code execution in the context of the current user. A low-privileged attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue requires user interaction in that a victim must open a malicious file. Scope is changed.	2026-07-28	8.2

CVE-2026-14996	ibm - aspera_faspex	IBM Aspera Faspex 5 5.0.0 through 5.0.15.4 has addressed a vulnerability related to session management.	2026-07-28	8.2
CVE-2026-33930	apache - multiple products	Apache Traffic Server copies the client Host header into a fixed-size stack buffer without a bound during redirect handling, so an over-long Host header overflows the stack when redirect following is enabled. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.2
CVE-2026-65324	apache - multiple products	Apache Traffic Server drops the per-stream buffer cap when dechunking HTTP/2 or HTTP/3 responses, letting a slow client exhaust server memory. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.2
CVE-2026-58158	apache - multiple products	Apache Traffic Server mishandles PROXY protocol input, truncating ports and overflowing the stack. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.2
CVE-2026-58175	apache - multiple products	Apache Traffic Server leaks memory when handling HostDB SRV records. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.2
CVE-2026-58178	apache - multiple products	The Apache Traffic Server ESI plugin can recurse without bound and fetch attacker-controlled URLs. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.2
CVE-2026-58180	apache - multiple products	The Apache Traffic Server txn_box plugin overflows the stack from attacker-controlled input. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.2
CVE-2026-58181	apache - multiple products	The Apache Traffic Server uri_signing and url_sig plugins can exhaust the stack or crash on attacker input. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.2
CVE-2026-58182	apache - multiple products	The Apache Traffic Server ts_lua plugin mishandles initialization, transform context, and per-instance state. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.2
CVE-2026-58183	apache - multiple products	The Apache Traffic Server prefetch plugin can crash when processing attacker-influenced input. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.2
CVE-2026-58185	apache - multiple products	The Apache Traffic Server intercept plugin has a use-after-free. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.2
CVE-2026-58186	apache - multiple products	The Apache Traffic Server webp_transform plugin can decode unsafely and serve mislabeled, cacheable responses. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	8.2
CVE-2026-58189	apache - multiple products	Apache Traffic Server allows redirect-limit bypass when plugins reset the retry counter, enabling SSRF amplification. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3.	2026-07-29	8.2

		Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.		
CVE-2026-18141	red hat - multiple products	A flaw was found in aap-gateway, a component of Ansible Automation Platform's Event-Driven Ansible (EDA). An unauthenticated remote attacker can bypass mutual Transport Layer Security (mTLS) authentication for event streams. This is achieved by manipulating the event stream URL and forging the HTTP Subject header. The system also inadvertently discloses the expected certificate subject in error messages, which simplifies the attack. This vulnerability allows an attacker to inject arbitrary events into EDA, potentially triggering automated workflows.	2026-07-31	8.2
CVE-2026-64536	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: staging: rtl8723bs: fix OOB reads in is_ap_in_tkip() IE loop The loop in is_ap_in_tkip() iterates over IEs without verifying that enough bytes remain before dereferencing the IE header or its payload: - pIE->element_id and pIE->length are read without checking that i + sizeof(*pIE) <= ie_length, so a truncated IE at the end of the buffer causes an OOB read. - For WLAN_EID_VENDOR_SPECIFIC the code compares pIE->data + 12, which requires pIE->length >= 16. For WLAN_EID_RSN it compares pIE->data + 8, requiring pIE->length >= 12. Neither requirement is checked. Add the missing IE header and payload bounds checks and guard each data access with an explicit pIE->length minimum, matching the pattern established in update_beacon_info().	2026-07-27	8.1
CVE-2026-64540	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: usbnet: gl620a: fix out-of-bounds read in genelink_rx_fixup() genelink_rx_fixup() splits an aggregated RX frame into its individual packets, using a per-packet length taken from device-supplied data. That length is only bounded by GL_MAX_PACKET_LEN (1514); it is never compared against how many bytes were actually received. A malicious GeneLink (GL620A) device can therefore send a short URB whose header claims packet_count > 1 and a first packet of up to 1514 bytes. skb_put_data(gl_skb, packet->packet_data, size); then copies past the end of the receive buffer and hands the adjacent slab contents up the network stack, an out-of-bounds read that leaks kernel heap. No privilege is required: the path runs in the usbnet RX softirq as soon as the interface is up. BUG: KASAN: slab-out-of-bounds in genelink_rx_fixup (drivers/net/usb/gl620a.c:112) Read of size 1514 at addr ffff888011309708 by task ksoftirqd/0/14 Call Trace: ... __asan_memcpy (mm/kasan/shadow.c:105) genelink_rx_fixup (include/linux/skbuff.h:2814 drivers/net/usb/gl620a.c:112) usbnet_bh (drivers/net/usb/usbnet.c:572 drivers/net/usb/usbnet.c:1589) process_one_work (kernel/workqueue.c:3322) bh_worker (kernel/workqueue.c:3405) tasklet_action (kernel/softirq.c:965) handle_softirqs (kernel/softirq.c:622) run_ksoftirqd (kernel/softirq.c:1076) ... skb_pull() already verifies that the requested length fits the buffer and returns NULL otherwise. Move it ahead of the copy and check its result, so a packet that overruns the received data is rejected before it is read. Well-formed frames, whose packets are fully present, are unaffected.	2026-07-27	8.1
CVE-2026-64547	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: usb: net1080: validate packet_len before pad-byte access in rx_fixup For an even packet_len, net1080_rx_fixup() reads the pad byte at skb->data[packet_len] before the skb->len != packet_len check further down, and packet_len is only bounded against NC_MAX_PACKET. A malicious NetChip 1080 device can send a short frame advertising a large even packet_len (e.g. 0x4000), so the pad-byte read lands past the end of the skb: BUG: KASAN: slab-out-of-bounds in net1080_rx_fixup Read of size 1 at addr ffff8880106c83c6 by task ksoftirqd/0/14 ... net1080_rx_fixup (drivers/net/usb/net1080.c:384) usbnet_bh (drivers/net/usb/usbnet.c:1589)	2026-07-27	8.1

		process_one_work (kernel/workqueue.c:3322) bh_worker (kernel/workqueue.c:3708) tasklet_action (kernel/softirq.c:965) handle_softirqs (kernel/softirq.c:622) ... Reject the frame when packet_len >= skb->len before reading.		
CVE-2026-64713	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in Safari 26.6, iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Websites may know if the user has visited a given link.	2026-07-27	8.1
CVE-2026-64719	apple - multiple products	An out-of-bounds access issue was addressed with improved bounds checking. This issue is fixed in Safari 26.6, iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2026-07-27	8.1
CVE-2026-64768	apple - multiple products	An out-of-bounds read issue was addressed with improved input validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6. A remote attacker may cause an unexpected app termination.	2026-07-27	8.1
CVE-2026-7769	ibm - multiple products	IBM Sterling B2B Integrator 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify, or delete information in the back-end database.	2026-07-28	8.1
CVE-2026-14974	ibm - multiple products	IBM WebSphere Application Server 8.5, and 9.0 traditional could allow a remote attacker to execute arbitrary code caused by unsafe deserialization of untrusted data.	2026-07-28	8.1
CVE-2026-17686	google - chrome	Insufficient validation of untrusted input in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	2026-07-30	8.1
CVE-2026-17869	google - chrome	Out of bounds read in WebXR in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	8.1
CVE-2026-17995	google - chrome	Out of bounds read in Dawn in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	8.1
CVE-2026-17543	php - multiple products	Improper escaping of backslashes in attacker-provided parameters would allow for trivial SQL injection in PHP versions from 8.2.* before 8.2.33, from 8.3.* before 8.3.33, from 8.4.* before 8.4.24, and from 8.5.* before 8.5.9.	2026-07-30	8.1
CVE-2026-17544	php - multiple products	Attacker-provided inputs to bccomp() could lead to an out-of-bounds write with stack and heap corruption in PHP versions from 8.4.* before 8.4.24 and from 8.5.* before 8.5.9.	2026-07-30	8.1
CVE-2026-14537	google - multiple products	Incorrect Authorization in the direct HTTP API tool invocation endpoint in Google mcp-toolbox versions v1.3.0 and v1.4.0 allows an unauthenticated attacker to invoke tools protected by the scopeRequired feature via sending tool invocation requests through legacy HTTP endpoints when the --enable-api flag is active.	2026-07-31	8.1
CVE-2026-62391	apache software foundation - Apache Kyuubi	The security fix for CVE-2025-66518 is incomplete. Any client who can access to Apache Kyuubi Server via Kyuubi frontend protocols can bypass server-side config kyuubi.session.local.dir.allowlist via unprefixed Spark config aliases. This issue affects Apache Kyuubi: from 1.6.0 before 1.12.0. Users are recommended to upgrade to version 1.12.0, which fixes the issue.	2026-07-31	8.1
CVE-2026-12703	teamviewer - multiple products	TeamViewer Full Client and Host for macOS before version 15.80 contain a business logic error that can allow an authenticated attacker to bypass a configured 2FA for Connections approval flow via Unattended Access and establish a remote connection to an affected macOS host.	2026-07-29	8
CVE-2026-14540	google - mcp_toolbox_for_databases	A Server-Side Request Forgery (SSRF) vulnerability exists in the generic HTTP source and tool components of Google mcp-toolbox versions 0.3.0 through 1.4.0. While the toolbox implements baseline input sanitization for user-controlled parameters, the underlying HTTP client (internal/sources/http/http.go) fails to safely regulate request redirection boundaries. Specifically, the client is initialized without a restrictive CheckRedirect policy hook and lacks target IP validation. An attacker or a malicious data-driven prompt can supply a crafted path parameter that triggers an open redirect or a direct destination swap on the target backend, coercing the mcp-toolbox into blindly following the redirection and making unauthorized requests to internal or arbitrary external endpoints.	2026-07-31	8
CVE-2026-14541	google - mcp_toolbox_for_databases	An authentication bypass and audience confusion vulnerability exists in the Google OAuth provider component of Google mcp-toolbox version 1.4.0. When a Google authService is initialized with mcpEnabled: true but lacks an explicitly defined audience or clientId, the ValidateMCPAuth pipeline for opaque tokens skips audience validation entirely. As a result, the toolbox will accept any valid Google OAuth access token—even those minted for unrelated ecosystem applications—granting unauthorized clients access to protected tools and data backends.	2026-07-31	8
CVE-2024-14040	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: nexthop: Increase weight to u16 In CLOS networks, as link failures occur at various points in the network, ECMP weights of the involved nodes are adjusted to compensate. With high fan-out of the involved nodes, and overall high number of nodes, a (non-)ECMP weight ratio that we would like to configure does not fit into 8 bits. Instead of, say, 255:254, we might like to configure something like 1000:999. For these deployments, the 8-bit weight may not be enough. To that end, in this patch increase the next hop weight from u8 to u16. Increasing the width of an integral type can be tricky, because while the	2026-07-26	7.8

		code still compiles, the types may not check out anymore, and numerical errors come up. To prevent this, the conversion was done in two steps. First the type was changed from u8 to a single-member structure, which invalidated all uses of the field. This allowed going through them one by one and audit for type correctness. Then the structure was replaced with a vanilla u16 again. This should ensure that no place was missed.
		
		The UAPI for configuring nexthop group members is that an attribute NHA_GROUP carries an array of struct nexthop_grp entries:
		
		struct nexthop_grp {
		__u32 id; /* nexthop id - must exist */
		__u8 weight; /* weight of this nexthop */
		__u8 resvd1;
		__u16 resvd2;
		};
		
		The field resvd1 is currently validated and required to be zero. We can lift this requirement and carry high-order bits of the weight in the reserved field:
		
		struct nexthop_grp {
		__u32 id; /* nexthop id - must exist */
		__u8 weight; /* weight of this nexthop */
		__u8 weight_high;
		__u16 resvd2;
		};
		
		Keeping the fields split this way was chosen in case an existing userspace makes assumptions about the width of the weight field, and to sidestep any endianness issues.
		
		The weight field is currently encoded as the weight value minus one, because weight of 0 is invalid. This same trick is impossible for the new weight_high field, because zero must mean actual zero. With this in place:
		
		- Old userspace is guaranteed to carry weight_high of 0, therefore configuring 8-bit weights as appropriate. When dumping nexthops with 16-bit weight, it would only show the lower 8 bits. But configuring such nexthops implies existence of userspace aware of the extension in the first place.
		
		- New userspace talking to an old kernel will work as long as it only attempts to configure 8-bit weights, where the high-order bits are zero. Old kernel will bounce attempts at configuring >8-bit weights.
		
		Renaming reserved fields as they are allocated for some purpose is commonly done in Linux. Whoever touches a reserved field is doing so at their own risk. nexthop_grp::resvd1 in particular is currently used by at least strace, however they carry an own copy of UAPI headers, and the conversion should be trivial. A helper is provided for decoding the weight out of the two fields. Forcing a conversion seems preferable to bending backwards and introducing anonymous unions or whatever.		

CVE-2026-64531	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: openvswitch: reject oversized nested action attrs Open vSwitch stores generated flow actions as nlattrs, whose nla_len field is u16. Commit a1e64addf3ff ("net: openvswitch: remove misbehaving actions length check") allowed the total sw_flow_actions stream to grow beyond 64 KiB, which is valid, but also removed the last guard preventing a generated nested action attribute from exceeding U16_MAX. An oversized generated container can thus be closed with a truncated nla_len. A later dump or teardown then walks a structurally different stream than the one that was validated. In particular, an oversized nested CLONE/CT action may cause subsequent bytes in the generated stream to be interpreted as independent actions. Keep the larger total-action-stream behavior, but make nested action close reject generated containers that do not fit in nla_len, and return the error through all callers. For recursive SAMPLE, CLONE, DEC_TTL, and CHECK_PKT_LEN builders, trim resource-owning action-list tails in reverse construction order before discarding failed wrappers, so resources copied into the rejected tails are released before the wrappers are removed. Most failed outer wrappers are discarded by truncating actions_len after child resources have been released. CHECK_PKT_LEN also trims its parent after branch resources are gone. SET/TUNNEL close failures unwind their	2026-07-27	7.8

		known tun_dst ownership directly, and SET_TO_MASKED has no external ownership and truncates on close failure.		
CVE-2026-64532	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: bound NTFS_DE view.data_off in UpdateRecordData{Root,Allocation} In do_action()'s UpdateRecordDataRoot (fslog.c:3489) and UpdateRecordDataAllocation (fslog.c:3697) cases, the memmove destination is `Add2Ptr(e, le16_to_cpu(e->view.data_off))`, where e->view.data_off comes from an on-disk NTFS_DE inside an INDEX_ROOT or INDEX_BUFFER. Neither case validates view.data_off + dlen against e->size; the existing check_if_index_root / check_if_alloc_index helpers walk the entry chain and validate the entry's offset, but not its internal view fields. The neighbouring read sites (e.g., fs/ntfs3/index.c when iterating view entries) check view.data_off + view.data_size <= e->size. Apply the same bound at the two memmove sites. Reproduced under UML+KASAN on mainline 8d90b09e6741 via pr_warn-only probe instrumentation: with view.data_off forced to 0xFFFC, the memmove writes 32 bytes past the end of the NTFS_DE. This is similar in shape to Pavitra Jha's 2026-05-02 patch "fs/ntfs3: prevent oob in case UpdateRecordDataRoot" (<20260502105008.21827-1-jhapavitra98@gmail.com>) which proposes calling ntfs3_bad_de_range(); that helper does not exist in mainline. This patch uses inline checks.	2026-07-27	7.8
CVE-2026-64533	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: fs/ntfs3: validate lcns_follow in log_replay conversion log_replay() converts DIR_PAGE_ENTRY_32 records into DIR_PAGE_ENTRY records when replaying version 0 restart tables. During this conversion, the memmove() length is derived directly from the on-disk lcns_follow field: memmove(&dp->vcn, &dp0->vcn_low, 2 * sizeof(u64) + le32_to_cpu(dp->lcns_follow) * sizeof(u64)); check_rstbl() validates restart table structure, but does not constrain per-entry lcns_follow values relative to the entry size. A malformed filesystem image can provide an oversized lcns_follow value, causing the conversion memmove() to access memory beyond the bounds of the allocated restart table buffer. The same field is later used to bound iteration over page_lcns[], so validating lcns_follow during conversion also prevents downstream out-of-bounds access from the same malformed metadata. Compute the maximum valid lcns_follow from the already-validated restart table entry size and reject entries that exceed this bound. Reuse the existing t16/t32 scratch variables already declared in log_replay() to avoid introducing new declarations. [almaz.alexandrovich@paragon-software.com: fixed the conflicts]	2026-07-27	7.8
CVE-2026-17523	red hat - multiple products	A flaw was found in the Linux kernel in net/can/bcm.c in can: bcm, where an unprivileged local user can exploit this vulnerability to execute arbitrary code within the kernel, which leads to a local privilege escalation (LPE). This allows the attacker to gain root privileges and take full control of the affected system.	2026-07-27	7.8
CVE-2026-28912	apple - multiple products	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Sequoia 15.7.8, macOS Tahoe 26.6. A user may be able to elevate privileges.	2026-07-27	7.8
CVE-2026-28981	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. Processing a maliciously crafted image may lead to arbitrary code execution.	2026-07-27	7.8
CVE-2026-39874	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A malicious app may be able to gain root privileges.	2026-07-27	7.8
CVE-2026-39875	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A malicious app may be able to gain root privileges.	2026-07-27	7.8
CVE-2026-39877	apple - multiple products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8. An app may be able to disclose kernel memory.	2026-07-27	7.8
CVE-2026-43673	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing a maliciously crafted audio file may corrupt process memory.	2026-07-27	7.8

CVE-2026-43698	apple - multiple products	An injection issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8. An app may be able to gain root privileges.	2026-07-27	7.8
CVE-2026-43711	apple - multiple products	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing a maliciously crafted video file may lead to unexpected app termination.	2026-07-27	7.8
CVE-2026-43723	apple - multiple products	A path handling issue was addressed with improved validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to gain root privileges.	2026-07-27	7.8
CVE-2026-43729	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6. Processing a maliciously crafted image may corrupt process memory.	2026-07-27	7.8
CVE-2026-43733	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Tahoe 26.6. Processing a maliciously crafted image may corrupt process memory.	2026-07-27	7.8
CVE-2026-43749	apple - multiple products	A parsing issue in the handling of directory paths was addressed with improved path validation. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to gain root privileges.	2026-07-27	7.8
CVE-2026-43776	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Tahoe 26.6. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution.	2026-07-27	7.8
CVE-2026-43780	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing a maliciously crafted texture may lead to unexpected app termination.	2026-07-27	7.8
CVE-2026-64539	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: Bluetooth: eir: Fix stack OOB write when prepending the Flags AD eir_create_adv_data() builds the advertising data into a fixed-size buffer ("size", 31 for the legacy path). It may prepend a 3-byte "Flags" AD structure (LE_AD_NO_BREDR on an LE-only controller) and then copies the per-instance data without checking that it still fits: memcpy(ptr, adv->adv_data, adv->adv_data_len); tlv_data_max_len() only reserves those 3 bytes when the user-supplied flags carry a managed-flags bit, so an instance added with flags == 0 is accepted with adv_data_len up to the full buffer. At advertise time the flags are still prepended, and the memcpy() writes 3 + adv_data_len bytes into the size-byte buffer: BUG: KASAN: stack-out-of-bounds in eir_create_adv_data (net/bluetooth/eir.c:301) Write of size 31 at addr ffff88800a547bdc by task kworker/u9:0/65 Workqueue: hci0 hci_cmd_sync_work __asan_memcpy (mm/kasan/shadow.c:106) eir_create_adv_data (net/bluetooth/eir.c:301) hci_update_adv_data_sync (net/bluetooth/hci_sync.c:1310) hci_schedule_adv_instance_sync (net/bluetooth/hci_sync.c:1817) hci_cmd_sync_work (net/bluetooth/hci_sync.c:332) This frame has 1 object: [32, 64) 'cp' The "Flags" structure is added by the kernel, not requested by userspace, so only prepend it when it fits together with the instance advertising data; when there is no room for both, drop the flags rather than the user-provided data. Reachable by a local user with CAP_NET_ADMIN owning an LE-only controller on the legacy advertising path.	2026-07-27	7.8
CVE-2026-64543	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: tipc: fix use-after-free of the discoverer in tipc_disc_rcv() bearer_disable() frees b->disc with tipc_disc_delete()'s plain kfree(), but tipc_disc_rcv() still dereferences b->disc in RX softirq under rcu_read_lock() (tipc_udp_recv -> tipc_rcv -> tipc_disc_rcv). L2 bearers are safe thanks to the synchronize_net() in tipc_disable_l2_media(), but the UDP bearer defers that call to the cleanup_bearer() workqueue, so the discoverer is freed with no grace period: BUG: KASAN: slab-use-after-free in tipc_disc_rcv (net/tipc/discover.c:149) Read of size 8 at addr ffff88802348b728 by task poc_tipc/184 <IRQ> tipc_disc_rcv (net/tipc/discover.c:149) tipc_rcv (net/tipc/node.c:2126) tipc_udp_recv (net/tipc/udp_media.c:391) udp_rcv (net/ipv4/udp.c:2643)	2026-07-27	7.8

		ip_local_deliver_finish (net/ipv4/ip_input.c:241) </IRQ> Freed by task 181: kfree (mm/slub.c:6565) bearer_disable (net/tipc/bearer.c:418) tipc_nl_bearer_disable (net/tipc/bearer.c:1001) The bearer is freed with kfree_rcu(); free the discoverer the same way. Add an rcu_head to struct tipc_discoverer and free it and its skb from an RCU callback. Because the RCU callback (tipc_disc_free_rcu) lives in module text, a call_rcu() that is still pending when the tipc module is unloaded would invoke a freed function. Add an rcu_barrier() to tipc_exit() after the bearer subsystem has been torn down, so all pending discoverer callbacks have run before the module text goes away. Reachable from an unprivileged user namespace: the TIPCv2 genl family is netnsok and its bearer commands have no GENL_ADMIN_PERM. Needs CONFIG_TIPC and CONFIG_TIPC_MEDIA_UDP.		
CVE-2026-64716	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing a maliciously crafted image may corrupt process memory.	2026-07-27	7.8
CVE-2026-64747	apple - multiple products	A buffer overflow was addressed with improved size validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to execute arbitrary code with kernel privileges.	2026-07-27	7.8
CVE-2026-64749	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Tahoe 26.6, visionOS 26.6. An app may be able to cause unexpected system termination or corrupt kernel memory.	2026-07-27	7.8
CVE-2026-64758	apple - multiple products	The issue was addressed with improved bounds checks. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing a maliciously crafted file may lead to unexpected app termination.	2026-07-27	7.8
CVE-2026-64763	apple - multiple products	An out-of-bounds write issue was addressed by removing the vulnerable code. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution.	2026-07-27	7.8
CVE-2026-64764	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution.	2026-07-27	7.8
CVE-2026-64765	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution.	2026-07-27	7.8
CVE-2026-64766	apple - multiple products	An integer overflow was addressed with improved input validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing a maliciously crafted file may lead to unexpected app termination or arbitrary code execution.	2026-07-27	7.8
CVE-2026-48372	adobe - format_plugins	Format Plugins is affected by a Heap-based Buffer Overflow vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-07-28	7.8
CVE-2026-18107	red hat - multiple products	A flaw was found in CRIU's handling of restartable sequences (rseq) during checkpoint/restore. A malicious process inside a container can register an rseq critical section that hijacks CRIU's parasite code injection during checkpoint, allowing it to spoof the process credentials saved in the checkpoint image. On restore, the container process gains elevated capabilities and zeroed UIDs/GIDs. The practical impact on Red Hat products is limited by several factors: checkpoint/restore requires root privileges (podman) or cluster-admin RBAC (OpenShift) to trigger and cannot be initiated from within the container itself; on OpenShift prior to 4.17 the feature required explicit opt-in, and on 4.17+ the kubelet checkpoint API RBAC is not configured by default; OpenShift enforces user namespaces by default for regular workloads (hostUsers is gated behind admin-only SCCs), which makes the spoofed capabilities namespace-scoped and ineffective for privilege escalation; SELinux type enforcement (container_t) blocks privilege transitions independently of capabilities; seccomp filters persist through checkpoint/restore and cannot be corrupted via the parasite; and kernel mount namespace ownership checks on RHEL 9/10 kernels prevent mount-based container escape even with spoofed capabilities.	2026-07-28	7.8
CVE-2026-48374	adobe - multiple products	Bridge is affected by an Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability that could lead to arbitrary file system read. An attacker could exploit this vulnerability to access sensitive files and directories outside the intended access scope. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-07-28	7.8
CVE-2026-48392	adobe - multiple products	Bridge is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-07-28	7.8
CVE-2026-48393	adobe - multiple products	Bridge is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-07-28	7.8

CVE-2026-48394	adobe - multiple products	Bridge is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-07-28	7.8
CVE-2026-58150	apache - multiple products	Apache Traffic Server does not reject Transfer-Encoding in HTTP/2 requests, allowing downgrade request smuggling. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	7.8
CVE-2026-64556	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: perf/core: Detach event groups during remove_on_exec perf_event_remove_on_exec() removes events by calling perf_event_exit_event(). For top-level events, this removes the event from the context with DETACH_EXIT only. This can leave inconsistent group state when a removed event is a group leader and the group contains siblings without remove_on_exec. If the group was active, the surviving siblings can remain active and attached to the removed leader's sibling list, but are no longer represented by a valid group leader on the PMU context active lists. A later close of the removed leader uses DETACH_GROUP and can promote the still-active siblings from this stale group state. The next schedule-in can then add an already-linked active_list entry again, corrupting the PMU context active list. With DEBUG_LIST enabled, this is caught as a list_add double-add in merge_sched_in(). Fix this by detaching group relationships when remove_on_exec removes an event. This preserves the existing task-exit and revoke behavior, while ensuring surviving siblings are ungrouped before the removed event leaves the context.	2026-07-29	7.8
CVE-2026-18220	red hat - multiple products	An out-of-bounds write vulnerability was found in the BFD library's DLX ELF backend (bfd/elf32-dlx.c) in GNU binutils. The dlx_rtype_to_howto() function maps ELF relocation types to internal howto structures but fails to perform adequate bounds checking on attacker-controlled relocation type values (via ELF32_R_TYPE(r_info)) before indexing into the dlx_elf_howto_table[] array. The DLX relocation type number space is non-contiguous (basic types 0-6, extended types at 0x10000+), but the default case in the switch statement allows arbitrary index values to reach the array access. A specially crafted ELF/DLX object file can trigger this out-of-bounds write when processed by any BFD-consuming tool (objdump, readelf, strip, ld, nm, objcopy). The vulnerability has been demonstrated to achieve arbitrary code execution via a File Stream Oriented Programming (FSOP) attack against glibc FILE structures (stderr), redirecting control flow to system(). Attack scenarios include CI/CD pipelines performing automated binary analysis, developer workstations running objdump/readelf on untrusted binaries, automated security scanning or malware analysis tools invoking binutils, and package build systems processing third-party code. Note: This vulnerability is only exploitable when binutils is built with the DLX backend enabled (typically via --enable-targets=all).	2026-07-29	7.8
CVE-2026-64558	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Check length in pkey_pckmo handler implementation Explicitly check the length of the target buffer in the pkey_pckmo implementation of the key_to_protkey() handler function. The handler function fails, if the generated output data exceeds the length of the provided target buffer.	2026-07-29	7.8
CVE-2026-64559	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: s390/pkey: Check length in PKEY_VERIFYPROTK ioctl Explicitly check the buffer length request structure provided by user-space and fail, if it exceeds the buffer size.	2026-07-29	7.8

CVE-2026-64560	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved:
		
		posix-cpu-timers: Prevent UAF caused by non-leader exec() race
		
		Wongi and Jungwoo decoded and reported a non-leader exec() related race which can result in an UAF:
		
		sys_timer_delete()
		  posix_cpu_timer_del()
		  // Observes old leader
		  p = pid_task(pid, pid_type);
		
		exec()
		
		de_thread()
		  switch_leader();
			2026-07-29	7.8

```
                                                  release_task(old_leader)
                                                    __exit_signal(old_leader)
                                                      sighand = lock(old_leader, sighand);
                                                      posix_cpu_timers*_exit();
  sighand = lock_task_sighand(p)                      unhash_task(old_leader);
    sh = lock(p, sighand)                       old_leader->sighand = NULL;
                                                      unlock(sighand);
    (p->sighand == NULL)
          unlock(sh)
          return NULL;

  // Returns without action
  if(!sighand)
     return 0;
  free_posix_timer();
```

This is "harmless" unless the deleted timer was armed and enqueued in p->signal because on exec() a TGID targeted timer is inherited.

As sys_timer_delete() freed the underlying posix timer object run_posix_cpu_timers() or any timerqueue related add/delete operations on other timers will access the freed object's timerqueue node, which results in an UAF.

There is a similar problem vs. posix_cpu_timer_set(). For regular posix timers it just transiently returns -ESRCH to user space, but for the use case in do_cpu_nanosleep() it's the same UAF just that the k_itimer is allocated on the stack.

Also posix_cpu_timer_rearm() fails to rearm the timer, which means it stops to expire.

While debating solutions Frederic pointed out another problem:

```
  posix_cpu_timer_del(tmr)
                                                  __exit_signal(p)
                                                    posix_cpu_timers*_exit(p);
                                                    unhash_task(p);
                                                    p->sighand = NULL;
    sh = lock_task_sighand(p)
      sighand = p->sighand;
          if (!sighand)
             return NULL;
          lock(sighand);

    if (!sh)
          WARN_ON_ONCE(timer_queued(tmr));
```

On weakly ordered architectures it is not guaranteed that posix_cpu_timer_del() will observe the stores in posix_cpu_timers*_exit() when p->sighand is observed as NULL, which means the WARN() can be a false positive.

Solve these issues by:

1) Changing the store in __exit_signal() to smp_store_release().

2) Adding a smp_acquire__after_ctrl_dep() into the !sighand path of lock_task_sighand().

3) Creating a helper function for looking up the task and locking sighand which does not return when sighand == NULL. Instead it retries the task lookup and only if that fails it gives up.

4) Using that helper in the three affected functions.

#1/#2 ensures that the reader side which observes sighand == NULL also observes all preceeding stores, i.e. the stores in posix_cpu_timers*_exit() and the ones in unhash_task().

#3 ensures that the above described non-leader exec() situation is handled gracefully. When the task lookup returns the old leader, but sighand == NULL then it retries. In the non-leader exec() case the subsequent task lookup will observe the new leader due to #1/#2. In normal exit() scenarios the subsequent lookup fails.

When the task lookup fails, the function also checks whether the timer is still enqueued and issues a warning if that's the case. Unfortunately there is nothing which can be done about it, but as the task is already not longer visible the timer should not be accessed anymore. This check also

		requires memory ordering, which is not provided when the first lookup fails. To achieve that the check is preceeded by a smp_rmb() which pairs with the smp_wmb() in write_seqlock() in __exit_signal(). That ensures that the stores in posix_cpu_timers*_exit() are visible. The history of the non-leader exec() issue goes back to the early days of posix CPU timers, which stored a pointer to the group leader task in the timer. That obviously fails when a non-leader exec() switches the leader. commit e0a70217107e ("posix-cpu-timers: workaround to suppress the problems with mt exec") added a temporary workaround for that in 2010 which surv ---truncated---		
CVE-2026-17654	google - chrome	Race in Updater in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: Critical)	2026-07-30	7.8
CVE-2026-17861	google - chrome	Insufficient validation of untrusted input in Updater in Google Chrome prior to 151.0.7922.72 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: Medium)	2026-07-30	7.8
CVE-2026-17862	google - chrome	Use after free in Tracing in Google Chrome on Windows prior to 151.0.7922.72 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: Medium)	2026-07-30	7.8
CVE-2026-17863	google - chrome	Inappropriate implementation in Browser in Google Chrome on Windows prior to 151.0.7922.72 allowed a local attacker to perform privilege escalation via a malicious file. (Chromium security severity: Medium)	2026-07-30	7.8
CVE-2026-17864	google - chrome	Inappropriate implementation in Updater in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: Medium)	2026-07-30	7.8
CVE-2026-16524	red hat - multiple products	A command injection flaw in PCP's linux_sockets PMDA allows malicious shell metacharacters via the network.persocket.filter metric. This failed validation lets attackers execute arbitrary commands as the PMDA user when metrics refresh.	2026-07-30	7.8
CVE-2026-34641	adobe - multiple products	Premiere Pro is affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	2026-07-31	7.8
CVE-2026-17527	red hat - multiple products	In containerized-data-importer (CDI), the aggregated cdi.kubevirt.io:view ClusterRole, intended to provide read-only access to CDI resources, includes a rule granting create on the datavolumes/source subresource. CDI's DataVolume clone authorization accepts this permission as sufficient to authorize cloning the contents of any PVC the caller can name, without requiring write access to the source namespace. A user or service account bound to the view role, commonly granted cluster-wide via ClusterRoleBinding, who also has ordinary write access (edit/admin) to any single namespace, can use this to exfiltrate the contents of any PVC in the cluster into a namespace they control, bypassing namespace isolation and the read-only guarantee of the view role.	2026-07-27	7.7
CVE-2026-28896	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8. An attacker may be able to cause unexpected system termination or read kernel memory.	2026-07-27	7.7
CVE-2026-33267	apache - multiple products	Improper Input Validation vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 9.2.0 through 9.2.14, from 10.1.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fixes the issue.	2026-07-29	7.7
CVE-2026-16313	red hat - multiple products	A flaw was found in sg3_utils. The sg_inq command, when invoked with the --export option, outputs device identification data without sanitizing control characters in SCSI name string fields. A newline character embedded in a device-supplied name string can inject arbitrary properties into the udev device database. This could allow an attacker who can present a crafted SCSI device to execute arbitrary commands as root when the device is disconnected.	2026-07-28	7.6
CVE-2026-18378	red hat - Cost Management Metrics Operator	A flaw was found in koku-metrics-operator. The operator's CostManagementMetricsConfig custom resource allows user able to edit the CR to specify an arbitrary upload URL. When authentication.type is set to token (the default), the cluster-global Red Hat Cloud pull-secret bearer token is attached to HTTP requests sent to this user-controlled URL, allowing the attacker to obtain the token.	2026-07-30	7.6
CVE-2026-18381	red hat - Cost Management Metrics Operator	A flaw was found in the koku-metrics-operator for Red Hat OpenShift. The operator's CostManagementMetricsConfig custom resource allows a user able to edit the CR to specify an arbitrary upload URL. The operator attaches its own Kubernetes service-account bearer token to queries sent to this user-controlled URL, allowing the attacker to obtain the token.	2026-07-30	7.6
CVE-2026-41703	vmware - multiple products	VMware ESX, Workstation, and Fusion contain an out-of-bounds read vulnerability. A malicious actor with VM deployment privileges could trigger an out-of-bounds read, potentially leading to information disclosure or more likely a Denial-of-Service (DoS) condition of the host process. On Workstation and Fusion, the impact of this vulnerability is restricted to information disclosure.	2026-07-30	7.6
CVE-2026-41608	apache - thrift	Improper Handling of Highly Compressed Data (Data Amplification) vulnerability in Apache Thrift Python bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	7.5
CVE-2026-49158	apache - thrift	Improper Handling of Highly Compressed Data (Data Amplification) vulnerability in Apache Thrift Ruby bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	7.5

CVE-2026-12383	red hat - multiple products	A flaw was found in the Event-Driven Ansible (EDA) server. The ExternalEventStreamViewSet uses permissive access controls (permission_classes=[AllowAny], authentication_classes=[]) and relies solely on the Subject HTTP header value for mTLS authentication without verifying that the header originated from a trusted proxy. Additionally, the expected certificate Distinguished Name is leaked in the 403 error response body. An attacker who can reach the EDA API endpoint with a spoofed Subject header can inject arbitrary events into mTLS-protected event streams, triggering downstream automation actions.	2026-07-27	7.5
CVE-2026-43728	apple - macos	This issue was addressed through improved state management. This issue is fixed in macOS Tahoe 26.6. An attacker may be able to modify the state of the Keychain.	2026-07-27	7.5
CVE-2026-43777	apple - multiple products	This issue was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A remote attacker may be able to cause a denial of service.	2026-07-27	7.5
CVE-2026-64545	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net, bpf: check master for NULL in xdp_master_redirect() xdp_master_redirect() dereferences the result of netdev_master_upper_dev_get_rcu() without a NULL check, but that helper returns NULL when the receiving device has no upper-master adjacency. The reach guard only checks netif_is_bond_slave(). On bond slave release bond_upper_dev_unlink() drops the upper-master adjacency before clearing IFF_SLAVE, so an XDP_TX reaching xdp_master_redirect() in that window still passes netif_is_bond_slave() while master is already NULL, and faults on master->flags at offset 0xb0: BUG: kernel NULL pointer dereference, address: 00000000000000b0 RIP: 0010:xdp_master_redirect (net/core/filter.c:4432) Call Trace: xdp_master_redirect (net/core/filter.c:4432) bpf_prog_run_generic_xdp (include/net/xdp.h:700) do_xdp_generic (net/core/dev.c:5608) __netif_receive_skb_one_core (net/core/dev.c:6204) process_backlog (net/core/dev.c:6319) __napi_poll (net/core/dev.c:7729) net_rx_action (net/core/dev.c:7792) handle_softirqs (kernel/softirq.c:622) __dev_queue_xmit (include/linux/bottom_half.h:33) packet_sendmsg (net/packet/af_packet.c:3082) __sys_sendto (net/socket.c:2252) Kernel panic - not syncing: Fatal exception in interrupt The missing check dates back to the original code; commit 1921f91298d1 ("net, bpf: fix null-ptr-deref in xdp_master_redirect() for down master") later added the master->flags read where the fault now lands but kept the unconditional deref. Check master for NULL before use; a NULL master is treated the same as one that is not up.	2026-07-27	7.5
CVE-2026-59878	apache - multiple products	Improper Input Validation vulnerability in Apache ActiveMQ AMQP, Apache ActiveMQ, Apache ActiveMQ All. A remote unauthenticated peer that can reach an exposed AMQP NIO connector can trigger denial-of-service behavior by sending a frame size value. This cause the NIO threads to die and if done rapidly enough can lead to exhaustion of the NIO thread pool denying service to other connections. This issue affects Apache ActiveMQ AMQP: before 5.19.9, from 6.0.0 before 6.2.8; Apache ActiveMQ: before 5.19.9, from 6.0.0 before 6.2.8; Apache ActiveMQ All: before 5.19.9, from 6.0.0 before 6.2.8. Users are recommended to upgrade to version 5.19.9, 6.2.8, or 6.3.0 which fixes the issue.	2026-07-28	7.5
CVE-2026-66299	apache - multiple products	Uncontrolled Resource Consumption vulnerability in Apache Tomcat's WebSocket chat example. This issue affects Apache Tomcat: from 11.0.0-M20 through 11.0.24, from 10.1.24 through 10.1.57, from 9.0.89 through 9.0.120. Users who have followed the security guidance to remove the examples web application are not affected by this issue. Users are recommended to remove the examples web application or to upgrade to version 11.0.25, 10.1.58 or 9.0.121 (when released), which fix the issue.	2026-07-28	7.5
CVE-2026-13463	ibm - Cloud Pak System	IBM Cloud Pak System 2.3.5.0 could allow a local attacker to obtain sensitive information due to the insertion of credentials into log files.	2026-07-28	7.5
CVE-2026-14981	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 are affected by a denial of service vulnerability in the HTTP channel due to unbounded allocation of resources without limits.	2026-07-28	7.5
CVE-2026-15057	ibm - websphere_application_server	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 is vulnerable to a denial of service due to uncontrolled heap allocation.	2026-07-28	7.5
CVE-2026-15280	ibm - websphere_application_server	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 ND Collective Controller is affected by a path-segment injection vulnerability in the collective routing mechanism.	2026-07-28	7.5

CVE-2026-17698	google - chrome	Insufficient validation of untrusted input in UI in Google Chrome on Android prior to 151.0.7922.72 allowed a local attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	7.5
CVE-2026-17774	google - chrome	Insufficient validation of untrusted input in Variations in Google Chrome prior to 151.0.7922.72 allowed an attacker in a privileged network position to potentially exploit heap corruption via malicious network traffic. (Chromium security severity: Medium)	2026-07-30	7.5
CVE-2026-17816	google - chrome	Insufficient policy enforcement in Speech in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	7.5
CVE-2026-17887	google - chrome	Use after free in TabStrip in Google Chrome prior to 151.0.7922.72 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: Medium)	2026-07-30	7.5
CVE-2026-17896	google - chrome	Use after free in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	7.5
CVE-2026-17898	google - chrome	Use after free in DevTools in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Low)	2026-07-30	7.5
CVE-2026-17916	google - chrome	Insufficient policy enforcement in Settings in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	7.5
CVE-2026-17930	google - chrome	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	7.5
CVE-2026-17948	google - chrome	Type Confusion in V8 in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Low)	2026-07-30	7.5
CVE-2026-17952	google - chrome	Inappropriate implementation in V8 in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Low)	2026-07-30	7.5
CVE-2026-17979	google - chrome	Race in V8 in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	7.5
CVE-2026-16529	red hat - multiple products	A signed integer overflow in the PCP __pmGetPDU() function can be exploited via crafted network packets during PDU processing or SASL negotiation. This permanently blinds the affected daemon, resulting in a total denial of service (DoS) for subsequent packet reads.	2026-07-30	7.5
CVE-2026-11897	ibm - websphere_application_server	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 is vulnerable to a denial of service, caused by sending a specially crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources.	2026-07-30	7.5
CVE-2026-12947	ibm - multiple products	IBM App Connect Enterprise 13.0.1.0 through 13.0.7.2, and 12.0.1.0 through 12.0.12.27 stores potentially sensitive information in log files that could be read by a local user.	2026-07-30	7.5
CVE-2026-14519	ibm - multiple products	IBM App Connect Enterprise 13.0.1.0 through 13.0.7.2, and 12.0.1.0 through 12.0.12.27 could allow a remote attacker to read arbitrary files due to a path traversal vulnerability.	2026-07-30	7.5
CVE-2026-16308	ibm - Enterprise Build of Quarkus	IBM Enterprise Build of Quarkus 3.27.1 through 3.27.4.SP2, and 3.33.1 through 3.33.2.SP2 Quarkus REST could allow a remote attacker to cause a denial of service due to unbounded accumulation of multipart MIME part-header bytes.	2026-07-30	7.5
CVE-2026-10842	ibm - multiple products	IBM WebSphere Application Server 8.5, and 9.0 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 Traditional and Liberty could allow a remote attacker to bypass security constraints.	2026-07-30	7.5
CVE-2026-28811	apache - jspwiki	Debug Messages Revealing Unnecessary Information in Apache JSPWiki up to 2.12.3. Users are recommended to upgrade to version 2.12.4, which fixes this issue.	2026-07-30	7.5
CVE-2026-28814	apache - jspwiki	Arbitrary Wiki Markup rendering due to lack of authentication in Apache JSPWiki up to 2.12.3 allows attacker to obtain sensitive data stored in JSPWiki variables. Users are recommended to upgrade to version 2.12.4 or 3.0.0, which fixes this issue.	2026-07-30	7.5
CVE-2026-9322	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 are vulnerable to a denial of service via a crafted HTTP request.	2026-07-30	7.5
CVE-2024-25039	ibm - Engineering Requirements Management DOORS and DOORS Web Access	IBM Engineering Requirements Management DOORS and DOORS Web Access 9.7.2.1 through 9.7.2.11, and 9.6.1.1 through 9.6.1.13 do not limit the length of a connection which could allow for a Slowloris HTTP denial of service attack to take place. This can cause the web server to become unresponsive.	2026-07-30	7.5
CVE-2026-10545	ibm - Planning Analytics Local	IBM Planning Analytics Local 2.1.0 through 2.1.21 is vulnerable to an open redirect that allows an attacker to redirect users to arbitrary external websites via a crafted URL. If used in SSO authentication flows, this could result in exposure of session tokens and allow attackers to hijack user sessions.	2026-07-30	7.5
CVE-2026-12733	ibm - multiple products	IBM DataPower Gateway could allow a remote attacker to cause a denial of service due to improper resource limitations.	2026-07-30	7.5
CVE-2026-11770	redhat - multiple products	A flaw was found in 389 Directory Server. An unauthenticated remote attacker can inject LDAP search filters into the CleanAllRUV replication status-check extended operation. Because the handler performs the search against cn=config with elevated replication plugin privileges and returns a boolean match result, the attacker can extract sensitive server configuration metadata, including replication bind DNs and password storage scheme information.	2026-07-31	7.5
CVE-2026-15722	redhat - multiple products	A stack buffer overflow flaw was found in 389 Directory Server (389-ds-base). The get_ruvelement_from_berval() function in repl5_ruv.c copies digit characters from a network-supplied RUV berval into a fixed 16-byte stack buffer without bounds checking. A remote unauthenticated attacker can crash the LDAP server by sending a crafted StartNSDS50ReplicationRequest extended operation containing a replica ID field with more than 16 digit characters. The overflow occurs during payload decoding, before any authorization check. Stack protectors limit impact to denial of service.	2026-07-31	7.5

CVE-2026-57989	microsoft - edge_chromium	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	2026-07-26	7.4
CVE-2026-57990	microsoft - edge_chromium	Files or directories accessible to external parties in Microsoft Edge (Chromium-based) allows an unauthorized attacker to disclose information over a network.	2026-07-26	7.4
CVE-2026-14528	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 traditional could allow a remote attacker to obtain sensitive information.	2026-07-28	7.4
CVE-2026-15328	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 and IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.7 is vulnerable to HTTP request smuggling.	2026-07-28	7.4
CVE-2026-64550	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: net: qualcomm: rmnet: validate MAP frame length before ingress parsing When ingress deaggregation is disabled, rmnet_map_ingress_handler() passes the skb straight to __rmnet_map_ingress_handler(), skipping the length validation that rmnet_map_deaggregate() performs on the aggregated path. The parser then dereferences the MAP header and csum header/trailer based on the on-wire pkt_len without checking skb->len, so a short frame is read out of bounds: BUG: KASAN: slab-out-of-bounds in rmnet_map_checksum_downlink_packet Read of size 1 at addr ffff88801118ed00 by task exploit/147 Call Trace: ... rmnet_map_checksum_downlink_packet (drivers/net/ethernet/qualcomm/rmnet/rmnet_map_data.c:413) __rmnet_map_ingress_handler (drivers/net/ethernet/qualcomm/rmnet/rmnet_handlers.c:96) rmnet_rx_handler (drivers/net/ethernet/qualcomm/rmnet/rmnet_handlers.c:129) __netif_receive_skb_core.constprop.0 (net/core/dev.c:6089) netif_receive_skb (net/core/dev.c:6460) tun_get_user (drivers/net/tun.c:1955) tun_chr_write_iter (drivers/net/tun.c:2001) vfs_write (fs/read_write.c:688) ksys_write (fs/read_write.c:740) do_syscall_64 (arch/x86/entry/syscall_64.c:94) ... Factor that validation out of rmnet_map_deaggregate() into rmnet_map_validate_packet_len() and run it on the no-aggregation path too. The MAP header is bounds-checked first, since this path can receive a frame shorter than the header.	2026-07-27	7.3
CVE-2026-14893	ibm - Observability with Instana (Agent)	IBM Observability with Instana (Agent) Build 1.0.303 through 1.0.320 IBM Instana Node.js tracer component @instana/core version 6.2.1 is vulnerable to prototype pollution through its configuration normalization API.	2026-07-28	7.3
CVE-2026-23904	apache - kyuubi	Kyuubi Engine UI proxy accepts a host and port from the request path and proxies HTTP requests to that destination. A remote requester with network access to the proxy can cause the Kyuubi server to send HTTP requests to arbitrary reachable hosts, resulting in SSRF or open-proxy behavior. This issue affects Apache Kyuubi: from 1.8.0 before 1.12.0. Users are recommended to upgrade to version 1.12.0, which disables the proxy by default. To restore proxied Engine UI, set kyuubi.frontend.rest.engine.ui.proxy.enabled=true and configure allowed target hosts with kyuubi.frontend.rest.engine.ui.proxy.hosts.	2026-07-29	7.3
CVE-2026-16527	red hat - multiple products	An unauthenticated remote attacker can bypass access controls by sending crafted requests to the PCP pmproxy /store endpoint. This allows the attacker to overwrite any PMDA metric, leading to arbitrary code execution and system takeover.	2026-07-30	7.3
CVE-2026-11980	ibm - Aspera Desktop App	IBM Aspera Desktop App 1.0.5 through 1.0.19 can allow arbitrary code execution by loading DLL files at start-up.	2026-07-30	7.3
CVE-2026-18255	red hat - multiple products	A flaw was found in Quay. A user configured in GLOBAL_READONLY_SUPER_USERS is able to view robot account tokens for repositories they are not a member of, allowing an attacker with read-only superuser privileges to impersonate any robot account.	2026-07-29	7.2
CVE-2026-16843	hikvision - multiple products	Some Hikvision Networking Products are vulnerable to authenticated command execution due to insufficient input validation. Attackers with valid credentials can exploit this flaw by sending crafted packets containing malicious commands to affected devices, leading to arbitrary command execution.	2026-07-31	7.2
CVE-2026-28945	apple - multiple products	A permissions issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to bypass network restrictions.	2026-07-27	7.1
CVE-2026-43672	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A malicious application may be able to bypass Privacy preferences.	2026-07-27	7.1
CVE-2026-43681	apple - multiple products	A buffer overflow was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. A local user may be able to read kernel memory.	2026-07-27	7.1
CVE-2026-43747	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. Parsing a maliciously crafted file may lead to an unexpected app termination.	2026-07-27	7.1
CVE-2026-43771	apple - multiple products	A stack overflow was addressed with improved input validation. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause a denial-of-service.	2026-07-27	7.1

CVE-2026-43813	apple - multiple products	A validation issue was addressed with improved input sanitization. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. A maliciously crafted app may be able to bypass code signing enforcement.	2026-07-27	7.1
CVE-2026-64546	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/edid: fix OOB read in drm_parse_tiled_block() drm_parse_tiled_block() casts the DisplayID block to a struct displayid_tiled_block and reads the full fixed layout up to tile->topology_id[7] without checking block->num_bytes. The DisplayID iterator only validates the declared payload length, so a crafted EDID can advertise a tiled-display block (tag DATA_BLOCK_TILED_DISPLAY, or DATA_BLOCK_2_TILED_DISPLAY_TOPOLOGY for v2.0) with a small num_bytes at the end of a DisplayID extension. The read then runs past the end of the exact-sized kmemdup()'d EDID allocation, a heap out-of-bounds read. Reject blocks shorter than the spec's 22-byte tiled payload before reading the fixed struct, as drm_parse_vesa_mso_data() already does. BUG: KASAN: slab-out-of-bounds in drm_edid_connector_update Read of size 2 at addr ffff888010077700 by task exploit/147 dump_stack_lvl (lib/dump_stack.c:94 ...) print_report (mm/kasan/report.c:378 ...) kasan_report (mm/kasan/report.c:595) drm_edid_connector_update (drivers/gpu/drm/drm_edid.c:7581) bochs_connector_helper_get_modes (drivers/gpu/drm/tiny/bochs.c:574) drm_helper_probe_single_connector_modes (drivers/gpu/drm/drm_probe_helper.c:426) status_store (drivers/gpu/drm/drm_sysfs.c:219) ... vfs_write (fs/read_write.c:595 fs/read_write.c:688) ksys_write (fs/read_write.c:740)	2026-07-27	7.1
CVE-2026-64692	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to cause a denial-of-service.	2026-07-27	7.1
CVE-2026-64725	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to cause a denial-of-service.	2026-07-27	7.1
CVE-2026-16192	ibm - websphere_application_server	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 is affected by a denial of service vulnerability when the restConnector-2.0 feature is enabled.	2026-07-28	7.1
CVE-2026-14976	ibm - websphere_application_server	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 is affected by remote code execution with the collectiveController-1.0 feature enabled.	2026-07-28	7.1
CVE-2026-17741	google - chrome	Insufficient validation of untrusted input in WebView in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	7.1
CVE-2026-17744	google - chrome	Inappropriate implementation in File Input in Google Chrome on Linux prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	7.1
CVE-2026-17750	google - chrome	Use after free in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	7.1
CVE-2026-17811	google - chrome	Use after free in ANGLE in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	7.1
CVE-2026-17867	google - chrome	Insufficient validation of untrusted input in Dawn in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	7.1
CVE-2026-17888	google - chrome	Insufficient validation of untrusted input in WebUI in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to potentially perform a sandbox escape via malicious network traffic. (Chromium security severity: Medium)	2026-07-30	7.1
CVE-2026-28926	apple - multiple products	A race condition was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8. An app may be able to elevate privileges.	2026-07-27	7
CVE-2026-43693	apple - multiple products	A race condition was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to gain root privileges.	2026-07-27	7
CVE-2026-43755	apple - multiple products	A race condition was addressed with improved state management. This issue is fixed in macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to gain root privileges.	2026-07-27	7
CVE-2026-16184	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 could allow a remote attacker to bypass authentication by sending a crafted unauthenticated request.	2026-07-28	7
CVE-2026-41920	apache - multiple products	Improper Access Control vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 9.0.0 through 9.1.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.1.15 or 10.1.4, which fixes the issue.	2026-07-29	7
CVE-2026-57834	apache - multiple products	Apache Traffic Server allows request smuggling if chunked messages are malformed. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3.	2026-07-29	7

		Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.		
CVE-2026-58159	apache - multiple products	Apache Traffic Server can bypass IP access controls on UDS listeners and through ACL matching errors. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	7
CVE-2026-17993	google - chrome	Race in Updater in Google Chrome on Windows prior to 151.0.7922.72 allowed a local attacker to perform privilege escalation via a malicious file. (Chromium security severity: Low)	2026-07-30	7
CVE-2026-45112	apache - thrift	Allocation of Resources Without Limits or Throttling vulnerability in Apache Thrift Java bindings. This issue affects Apache Thrift: from 0.19.0 before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	6.9
CVE-2026-55970	apache - thrift	Buffer Over-read vulnerability in Apache Thrift C++ bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	6.9
CVE-2026-58023	apache - thrift	Out-of-bounds Read vulnerability in Apache Thrift c_glib bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue.	2026-07-27	6.9
CVE-2026-22068	apache - multiple products	Regular Expression without Anchors vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 10.0.X through 10.1.3, from 9.0.X through 9.2.14. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fixes the issue.	2026-07-29	6.9
CVE-2026-24033	apache - multiple products	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') vulnerability in Apache Traffic Server. This issue affects Apache Traffic Server: from 10.0.0 through 10.1.3, from 9.0.0 through 9.2.14. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fixes the issue.	2026-07-29	6.9
CVE-2026-58152	apache - multiple products	Apache Traffic Server mishandles integers while decoding HPACK/XPACK headers, corrupting memory. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	6.9
CVE-2026-58157	apache - multiple products	Apache Traffic Server can reuse server sessions and tunnels improperly, exposing data across client connections. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	6.9
CVE-2026-14227	mikrotik - RouterOS	An API session-management flaw in products with the MikroTik RouterOS API enabled are vulnerable to a Insufficient Session Expiration vulnerability. This could allow active sessions to retain their previous permission set after inactivity timeouts or user-group changes. As a result, an authenticated user whose permissions have been reduced may continue accessing information.	2026-07-30	6.9
CVE-2026-66756	apache software foundation - Apache Tika	Improper Protection of Alternate Path vulnerability in Apache Tika. This issue affects Apache Tika: from 4.0.0-alpha-1 before 4.0.0-beta-1. Users are recommended to upgrade to version 4.0.0-beta-1, which fixes the issue.	2026-07-30	6.9
CVE-2026-56389	gnu - Bison	GNU Bison allows for an execution of an arbitrary program during HTML report generation due to improper handling of grammar-defined configuration variables. A grammar file can override the executable used for the XML-to-HTML transformation step via %define tool.xsltproc, which is accepted without restriction and passed directly to execvp(). When running bison --html on a attacker-provided grammar, this behavior allows execution of an arbitrary program with the privileges of the Bison process. Maintainers of this project were notified about this vulnerability, and fixed the issue in commit 3169c1e7a2c6acc4c59dfcf8b089896d6881925b. However, they did not provide vulnerable version range. Version 3.8.2 was tested and confirmed as vulnerable, other versions were not tested but might also be vulnerable.	2026-07-29	6.8
CVE-2026-17919	google - chrome	Insufficient policy enforcement in Enterprise in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to perform privilege escalation via physical access to the device. (Chromium security severity: Low)	2026-07-30	6.8
CVE-2026-18382	red hat - Cost Management Metrics Operator	A flaw was found in koku-metrics-operator. The operator's CostManagementMetricsConfig custom resource allows a user able to edit the CR to specify an arbitrary OAuth token endpoint. When	2026-07-30	6.8

		authentication.type is set to service-account, the operator sends the tenant's Red Hat SSO client_id and client_secret to this user-controlled URL, allowing the attacker to obtain the credentials.		
CVE-2026-18214	redhat - build_of_keycloak	Keycloak allows users to log in using Google accounts and can be configured to only allow users from specific Google Workspace domains. A flaw was found where the token exchange feature, which allows swapping a Google token for a Keycloak token, does not check these domain restrictions. This means an attacker with a valid Google account from a different domain could bypass the security check and gain access to the Keycloak realm.	2026-07-31	6.8
CVE-2026-18215	redhat - build_of_keycloak	Keycloak provides a way to let users log in using Microsoft accounts while restricting access to a specific organization (tenant). A flaw was discovered where this restriction is ignored when using the token exchange feature. This means an attacker with a valid Microsoft token from a completely different organization could gain access to the Keycloak realm, potentially accessing sensitive data or performing unauthorized actions.	2026-07-31	6.8
CVE-2026-14539	google - mcp_toolbox_for_databases	An allocation of resources without limits vulnerability in the HTTP handler component of Google mcp-toolbox versions up to and including 1.4.0 allows an unauthenticated attacker to cause a denial of service (DoS). The /mcp endpoint handler reads incoming payloads directly into system memory using an unrestricted buffer loop (io.ReadAll) without applying defensive constraints such as http.MaxBytesReader or pre-read Content-Length enforcement. By submitting a single, massive HTTP request body, an attacker can linearly consume available host memory until the runtime process is terminated by an Out-Of-Memory (OOM) error.	2026-07-31	6.6
CVE-2026-66391	apache - multiple products	Use of Insufficiently Random Values, Protection Mechanism Failure vulnerability in Apache Wicket. This issue affects Apache Wicket: from 9.0.0 through 9.23.0, from 10.0.0 through 10.9.0. Users are recommended to upgrade to version 10.10.0, which fixes the issue.	2026-07-27	6.5
CVE-2026-43792	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in Safari 26.6, macOS Tahoe 26.6. An app may be able to access sensitive user data.	2026-07-27	6.5
CVE-2026-43804	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in Safari 26.6, iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, visionOS 26.6. Visiting a website may lead to an app denial-of-service.	2026-07-27	6.5
CVE-2026-43821	apple - multiple products	An access issue was addressed with improved access restrictions. This issue is fixed in Safari 26.6, iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to read files outside of its sandbox.	2026-07-27	6.5
CVE-2026-64728	apple - multiple products	A permissions issue was addressed with improved validation. This issue is fixed in Safari 26.6, iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Maliciously crafted web content may violate iframe sandboxing policy.	2026-07-27	6.5
CVE-2026-64730	apple - multiple products	The issue was addressed with improved UI. This issue is fixed in Safari 26.6, iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Visiting a website that frames malicious content may lead to UI spoofing.	2026-07-27	6.5
CVE-2026-64735	apple - multiple products	An inconsistent user interface issue was addressed with improved state management. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. A remote attacker may be able to bypass network filters.	2026-07-27	6.5
CVE-2026-64742	apple - multiple products	This issue was addressed by using HTTPS when sending information over the network. This issue is fixed in iOS 26.6 and iPadOS 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to access sensitive user data.	2026-07-27	6.5
CVE-2026-64743	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to access sensitive user data.	2026-07-27	6.5
CVE-2026-18047	red hat - multiple products	A flaw was found in Dogtag PKI's ACME responder where the web.xml security constraints use exact URL pattern matching for admin-only enable/disable endpoints. By appending a trailing slash to the URL, an unauthenticated attacker can bypass the Tomcat authentication constraint while RESTEasy still routes the request to the handler, allowing unauthorized toggling of the ACME service state including persistent denial of service.	2026-07-28	6.5
CVE-2026-61487	apache - multiple products	Improper Authorization vulnerability in Apache ActiveMQ Broker, Apache ActiveMQ All, Apache ActiveMQ. An authenticated low-privilege user can bypass a per-destination write ACL by sending to an ActiveMQ temporary composite destination whose physical name is a comma-separated composite of real queues. This allows publishing messages to any of the destinations in the list without proper write ACL permissions because the authorization check is bypassed due to the composite destination being marked as temporary. This issue affects Apache ActiveMQ Broker: before 5.19.9, from 6.0.0 before 6.2.8; Apache ActiveMQ All: before 5.19.9, from 6.0.0 before 6.2.8; Apache ActiveMQ: before 5.19.9, from 6.0.0 before 6.2.8. Users are recommended to upgrade to version 5.19.9, 6.2.8 or 6.3.0, which fixes the issue.	2026-07-28	6.5
CVE-2026-7868	ibm - OPENBMC	IBM OPENBMC FW1110.00 through FW1110.20, and FW1060.00 through FW1060.71 allows ReadOnly users to escalate privileges and give themselves administrator privileges.	2026-07-28	6.5
CVE-2026-18207	red hat - multiple products	A flaw was found in the client policy enforcement mechanism of Keycloak. The issue occurs when the system checks group membership by name instead of a unique identifier. An attacker with client management privileges could bypass security policies by joining a group with a matching name in a different part of the group hierarchy, potentially allowing them to register or update clients without following required security hardening profiles.	2026-07-29	6.5
CVE-2026-17664	google - Chrome	Insufficient validation of untrusted input in Loader in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	6.5
CVE-2026-17667	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	6.5

CVE-2026-17668	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	6.5
CVE-2026-17674	google - Chrome	Inappropriate implementation in HTML in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: High)	2026-07-30	6.5
CVE-2026-17679	google - chrome	Insufficient validation of untrusted input in Print Preview in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	6.5
CVE-2026-17683	google - chrome	Inappropriate implementation in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-07-30	6.5
CVE-2026-17690	google - chrome	Insufficient validation of untrusted input in PDF in Google Chrome on Android prior to 151.0.7922.72 allowed a local attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	6.5
CVE-2026-17703	google - chrome	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: High)	2026-07-30	6.5
CVE-2026-17707	google - chrome	Uninitialized Use in Media in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-07-30	6.5
CVE-2026-17714	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-07-30	6.5
CVE-2026-17743	google - Chrome	Insufficient policy enforcement in ControlledFrame in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17748	google - Chrome	Inappropriate implementation in Extensions in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17754	google - chrome	Inappropriate implementation in Blink in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17756	google - chrome	Insufficient policy enforcement in Presentation in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17759	google - chrome	Uninitialized Use in Codecs in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17764	google - chrome	Inappropriate implementation in FedCM in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17787	google - chrome	Inappropriate implementation in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17789	google - chrome	Insufficient validation of untrusted input in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via malicious network traffic. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17791	google - chrome	Insufficient validation of untrusted input in Payments in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17792	google - chrome	Inappropriate implementation in Credential Management in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17793	google - chrome	Inappropriate implementation in Messages in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17796	google - chrome	Side-channel information leakage in WebXR in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17800	google - chrome	Inappropriate implementation in MediaRecording in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17805	google - chrome	Insufficient policy enforcement in Glic in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17813	google - chrome	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17814	google - chrome	Insufficient validation of untrusted input in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17819	google - chrome	Inappropriate implementation in WebAppInstalls in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17821	google - chrome	Insufficient policy enforcement in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17822	google - chrome	Race in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5

CVE-2026-17823	google - chrome	Insufficient policy enforcement in WebXR in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17824	google - chrome	Insufficient policy enforcement in ServiceWorker in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17825	google - chrome	Insufficient policy enforcement in Passwords in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17828	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17830	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17831	google - chrome	Insufficient validation of untrusted input in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17835	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17838	google - chrome	Incorrect security UI in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17839	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17840	google - chrome	Incorrect security UI in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17841	google - chrome	Race in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17842	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17846	google - chrome	Inappropriate implementation in Media in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17850	google - chrome	Inappropriate implementation in Permissions in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17852	google - chrome	Inappropriate implementation in Media Router in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17854	google - chrome	Insufficient policy enforcement in WebMCP in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17873	google - chrome	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17882	google - chrome	Policy bypass in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to bypass site isolation via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17883	google - chrome	Inappropriate implementation in Headless in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17892	google - chrome	Inappropriate implementation in WebXR in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.5
CVE-2026-17917	google - chrome	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17921	google - chrome	Insufficient validation of untrusted input in Navigation in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17923	google - chrome	Policy bypass in Enterprise in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted domain name. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17926	google - chrome	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17929	google - chrome	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a malicious file. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17931	google - chrome	Inappropriate implementation in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17936	google - chrome	Inappropriate implementation in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5

CVE-2026-17946	google - chrome	Uninitialized Use in Dawn in Google Chrome prior to 151.0.7922.72 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: Low)	2026-07-30	6.5
CVE-2026-17953	google - chrome	Insufficient policy enforcement in WebView in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17968	google - chrome	Uninitialized Use in WebXR in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17974	google - chrome	Insufficient policy enforcement in DevTools in Google Chrome prior to 151.0.7922.72 allowed a local attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17975	google - chrome	Inappropriate implementation in IME in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17985	google - chrome	Insufficient policy enforcement in Speech in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass site isolation via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17986	google - chrome	Insufficient policy enforcement in Bluetooth in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17988	google - chrome	Insufficient validation of untrusted input in Navigation in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17992	google - chrome	Uninitialized Use in Skia in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-17999	google - chrome	Race in PictureInPicture in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-18001	google - chrome	Inappropriate implementation in WebGL in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-18005	google - chrome	Inappropriate implementation in WebXR in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-18014	google - chrome	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a malicious file. (Chromium security severity: Low)	2026-07-30	6.5
CVE-2026-16530	red hat - multiple products	A flaw was found in the PCP (Performance Co-Pilot) `pmproxy` service. A remote attacker can exploit a vulnerability in the `pmLogLoadInDom()` function by sending a specially crafted request. This bypasses a critical bounds check, which can lead to the `pmproxy` service crashing, causing a Denial of Service (DoS). Additionally, this flaw may enable the leakage of sensitive information from the system's memory.	2026-07-30	6.5
CVE-2026-44616	apache - zeppelin	LDAP injection vulnerability in Apache Zeppelin. ActiveDirectoryGroupRealm constructed LDAP search filters without escaping user-controlled input, allowing an authenticated attacker to inject LDAP filter syntax through the user-search endpoint and potentially expose directory information. The role-lookup path was also affected after successful LDAP authentication. This issue affects Apache Zeppelin versions 0.6.0 through 0.12.0. Users are recommended to upgrade to version 0.12.1, which fixes this issue.	2026-07-30	6.5
CVE-2026-44617	apache - zeppelin	LDAP filter injection vulnerability in Apache Zeppelin. LdapRealm used RFC 4514 distinguished-name escaping when constructing LDAP search filters instead of RFC 4515 filter escaping, leaving special filter characters insufficiently escaped. This is an incomplete fix of CVE-2024-31867. This issue affects Apache Zeppelin versions 0.11.1, 0.11.2, and 0.12.0. Users are recommended to upgrade to version 0.12.1, which fixes this issue.	2026-07-30	6.5
CVE-2026-48910	apache - jspwiki	A carefully crafted editing request could trigger an XSS vulnerability on Apache JSPWiki when parsing errors on the markdown renderer, which could allow the attacker to execute javascript in the victim's browser and get some sensitive information about the victim. This issue affects Apache JSPWiki: through 2.12.3. Users are recommended to upgrade to version 2.12.4, which fixes the issue.	2026-07-30	6.5
CVE-2026-18203	redhat - build_of_keycloak	A flaw was found in the group policy evaluation logic of Keycloak, an identity and access management solution. When a group policy is set to extend permissions to child groups, the system incorrectly uses a simple text-based prefix check to verify group membership. This allows a user who belongs to a different group with a similar starting name to bypass security checks and gain unauthorized access to administrative functions or protected resources.	2026-07-31	6.5
CVE-2026-18208	redhat - build_of_keycloak	A flaw was found in the OIDC token introspection endpoint of the keycloak-services component. Keycloak is an open-source identity and access management solution used to secure modern applications and services. The issue occurs when a confidential client, configured to receive signed JWT introspection responses, attempts to introspect a token issued for a different audience. Although the endpoint correctly identifies the token as inactive for that client, it still returns the full set of token claims within a signed JWT field. This allows an unauthorized client to bypass audience-based restrictions and access sensitive information contained in the token.	2026-07-31	6.5
CVE-2026-44615	apache software foundation - Apache Zeppelin	Path traversal vulnerability in Apache Zeppelin. When FileSystemNotebookRepo is configured, an authenticated attacker with permission to rename a note, or access to folder operations, could supply traversal segments in note or folder paths. Zeppelin composed these values into filesystem paths using the server's filesystem or Hadoop identity without ensuring that the result remained under the configured notebook directory. This could allow notebook files or directories to	2026-07-31	6.5

		be moved, written, or deleted outside the notebook root. This issue affects Apache Zeppelin versions 0.9.0 through 0.12.0. Users are recommended to upgrade to version 0.12.1, which fixes this issue.		
CVE-2026-58153	apache - traffic_server	Apache Traffic Server forwards HTTP/2 origin trailers to HTTP/1 clients without proper chunked framing when converting HTTP/2 to HTTP/1. This issue affects Apache Traffic Server: from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	6.3
CVE-2026-58156	apache - multiple products	Apache Traffic Server mis-parses ports in URLs and userinfo, allowing port-based access-control bypass. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	6.3
CVE-2026-65325	apache - multiple products	Apache Traffic Server reuses multiplexed HTTP/2 origin connections without verifying the server certificate covers the new request hostname. This issue affects Apache Traffic Server: from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	6.3
CVE-2026-58160	apache - multiple products	Apache Traffic Server reads out of bounds while parsing DNS answers. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	6.3
CVE-2026-58187	apache - multiple products	The Apache Traffic Server multiplexer plugin overruns its chunk-decode buffer on upstream input, enabling denial of service. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	6.3
CVE-2026-65100	apache - multiple products	Apache Traffic Server updates the HTTP/2 HPACK dynamic table before confirming the header block encoded successfully, so an encode failure leaves the encoder out of sync with the peer decoder and corrupts subsequent header blocks on the connection. This issue affects Apache Traffic Server: from 8.0.0 through 8.1.9, from 9.0.0 through 9.2.14, from 10.0.0 through 10.1.3. Users are recommended to upgrade to version 9.2.15 or 10.1.4, which fix the issue.	2026-07-29	6.3
CVE-2026-17780	google - chrome	Inappropriate implementation in Isolated Web Apps in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.3
CVE-2024-40683	ibm - Operations Analytics - Log Analysis	IBM Operations Analytics - Log Analysis 1.3.5.0, 1.3.5.1, 1.3.5.2, 1.3.5.3, 1.3.6.0, 1.3.6.1, 1.3.7.0, 1.3.7.1, 1.3.7.2, and 1.3.8.0, 1.3.8.1, 1.3.8.2, 1.3.8.3, 1.3.8.4 does not invalidate session after a password chance which could allow an authenticated user to impersonate another user on the system.	2026-07-30	6.3
CVE-2026-17966	google - chrome	Inappropriate implementation in Views in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.2
CVE-2026-17996	google - chrome	Inappropriate implementation in Browser in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to bypass navigation restrictions via a malicious file. (Chromium security severity: Low)	2026-07-30	6.2
CVE-2026-10695	ibm - db2	IBM Db2 12.1.0 through 12.1.4 federated server is vulnerable to a denial of service when running non fenced federated queries.	2026-07-30	6.2
CVE-2026-68562	red hat - multiple products	A flaw was found in ansible-collection-redhat-leapp. An attacker with privileged write access to a managed node's Leapp report content can manipulate it. When an operator runs a specific remediation task, this manipulated report can cause the Ansible controller to read its own local files and copy them to the managed node. This vulnerability leads to information disclosure, potentially exposing sensitive controller-side data such as private keys or credentials.	2026-07-30	6.2
CVE-2026-66390	apache - multiple products	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apache Wicket. This issue affects Apache Wicket: from 9.0.0 through 9.23.0, from 10.0.0 through 10.9.0. Users are recommended to upgrade to version 10.10.0, which fixes the issue.	2026-07-27	6.1
CVE-2026-14515	ibm - multiple products	IBM WebSphere Application Server 8.5, and 9.0 traditional could allow a remote attacker to conduct a cross-site scripting attack.	2026-07-28	6.1
CVE-2026-17797	google - chrome	Inappropriate implementation in CSS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.1
CVE-2026-17818	google - chrome	Inappropriate implementation in Network in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.1

CVE-2026-17827	google - chrome	Inappropriate implementation in CSS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.1
CVE-2026-17845	google - chrome	Inappropriate implementation in CSS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.1
CVE-2026-17853	google - chrome	Inappropriate implementation in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to inject scripts or HTML into a privileged page via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.1
CVE-2026-17872	google - chrome	Cryptographic Flaw in WebAppInstalls in Google Chrome on Android prior to 151.0.7922.72 allowed a local attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.1
CVE-2026-17878	google - chrome	Inappropriate implementation in CSS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	6.1
CVE-2026-17962	google - chrome	Inappropriate implementation in Blink in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	6.1
CVE-2026-44613	apache - zeppelin	Cross-Site Request Forgery (CSRF) vulnerability in Apache Zeppelin. The default CORS configuration allowed cross-origin state-changing requests and accepted text/plain request bodies, allowing an attacker who lures an authenticated user to a malicious site to perform actions on the user's behalf through REST and WebSocket endpoints. This issue affects Apache Zeppelin versions 0.6.0 through 0.12.0. Users are recommended to upgrade to version 0.12.1, which fixes this issue.	2026-07-30	6.1
CVE-2025-0152	ibm - Engineering Requirements Management DOORS and DOORS Web Access	IBM Engineering Requirements Management DOORS and DOORS Web Access 9.7.2.1 through 9.7.2.11, and 9.6.1.1 through 9.6.1.13 is vulnerable to cross-site scripting. This vulnerability allows an unauthenticated attacker to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-07-30	6.1
CVE-2026-66053	apache - thrift	Improper Validation of Certificate with Host Mismatch vulnerability in Apache Thrift Python bindings. This issue affects Apache Thrift: before 0.24.0. Users are recommended to upgrade to version 0.24.0, which fixes the issue. This replaces CVE-2026-41603	2026-07-27	5.9
CVE-2026-16107	ibm - TS4500 CLI tool	IBM TS4500 CLI tool Versions: 0.1.31 through 1.12.0.0 does not validate or improperly validates TLS certificate validation, which could allow an attacker to obtain sensitive information using man in the middle techniques.	2026-07-28	5.9
CVE-2026-66755	apache software foundation - Apache Tika	Relative Path Traversal in the ISA-Tab parser in Apache Software Foundation Apache Tika from 1.8 through 3.3.1, and 4.0.0-alpha-1, allows an attacker who can place files in a directory that the application subsequently parses to read arbitrary files accessible to the Tika process and have their contents emitted into the extracted text output, via a "Study Assay File Name" value in the ISA-Tab investigation file that traverses outside the dataset directory. Users are recommended to upgrade to version 3.3.2 or 4.0.0-beta-1, which fixes this issue.	2026-07-30	5.9
CVE-2026-17736	google - chrome	Insufficient validation of untrusted input in WebView in Google Chrome on Android prior to 151.0.7922.72 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)	2026-07-30	5.8
CVE-2026-17745	google - chrome	Out of bounds read in Skia in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	5.8
CVE-2026-17746	google - chrome	Use after free in GPU in Google Chrome on Mac prior to 151.0.7922.72 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)	2026-07-30	5.8
CVE-2026-17770	google - chrome	Out of bounds read in Media in Google Chrome on Mac prior to 151.0.7922.72 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)	2026-07-30	5.8
CVE-2026-17776	google - chrome	Policy bypass in Receiver in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	5.8
CVE-2026-17806	google - chrome	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	5.8
CVE-2026-17809	google - chrome	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	5.8
CVE-2026-17866	google - chrome	Type Confusion in Tab in Google Chrome on Android prior to 151.0.7922.72 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)	2026-07-30	5.8
CVE-2026-17890	google - chrome	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 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)	2026-07-30	5.8
CVE-2026-17891	google - chrome	Use after free in ANGLE in Google Chrome on Android prior to 151.0.7922.72 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)	2026-07-30	5.8
CVE-2026-17893	google - chrome	Insufficient validation of untrusted input in Updater in Google Chrome on Mac prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to	2026-07-30	5.8

		potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)		
CVE-2026-17906	google - chrome	Insufficient validation of untrusted input in Bluetooth in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	5.8
CVE-2026-17908	google - chrome	Insufficient validation of untrusted input in Printing in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	5.8
CVE-2026-18369	red hat - multiple products	A flaw was found in Dogtag PKI's ACME responder where the HTTP-01 challenge validator accepts IP address literals as dns identifiers and follows HTTP redirects without validating that the target is a public address. An unauthenticated ACME account holder can exploit this to perform server-side request forgery (SSRF), making the Dogtag server send HTTP GET requests to internal network services. With the InMemory database backend, the response body of internal targets is disclosed to the attacker through the ACME challenge error.	2026-07-30	5.8
CVE-2026-14538	google - mcp_toolbox_for_databases	An improper authorization and security-boundary bypass vulnerability in the bigquery-execute-sql tool component of Google mcp-toolbox versions 0.16.1 through 1.4.0 allows an authenticated attacker to bypass allowedDatasets validation checks. The toolbox relies on the BigQuery dry-run API to enforce dataset restrictions, but due to a fail-open logic flaw, it bypasses validation when the API returns an empty array for specialized constructs. This allows the attacker to extract structural DDL schemas for explicitly excluded datasets via INFORMATION_SCHEMA, and access downstream federated row data via EXTERNAL_QUERY connections.	2026-07-31	5.7
CVE-2026-15003	red hat - multiple products	A flaw was found in the GNU Binutils (Binary Utilities) linker. This vulnerability, a heap-buffer-overflow read (CWE-125), occurs when the linker processes a specially crafted 32-bit XCOFF (Extended Common Object File Format) object file. An attacker could exploit this by providing a malicious file, leading to an out-of-bounds read of memory. This can result in information disclosure, potentially revealing sensitive heap data, and a Denial of Service (DoS) due to the linker crashing.	2026-07-27	5.6
CVE-2026-20672	apple - multiple products	An information disclosure issue was addressed with improved privacy controls. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8. An app may be able to access sensitive user data.	2026-07-27	5.5
CVE-2026-28849	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8. A maliciously crafted ZIP archive may bypass Gatekeeper checks.	2026-07-27	5.5
CVE-2026-28900	apple - multiple products	A file quarantine bypass was addressed with additional checks. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8. A maliciously crafted ZIP archive may bypass Gatekeeper checks.	2026-07-27	5.5
CVE-2026-28932	apple - multiple products	A logic issue existed resulting in memory corruption. This was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause a denial of service.	2026-07-27	5.5
CVE-2026-43665	apple - multiple products	This issue was addressed with additional entitlement checks. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8. A local attacker may be able to determine the legacy VNC password configured for Screen Sharing.	2026-07-27	5.5
CVE-2026-43714	apple - multiple products	The issue was addressed with improved input sanitization. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, visionOS 26.6, watchOS 26.6. A malicious app may be able to access protected user data.	2026-07-27	5.5
CVE-2026-43738	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8. Processing a maliciously crafted asset catalog may result in disclosure of process memory.	2026-07-27	5.5
CVE-2026-43739	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	5.5
CVE-2026-43744	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing an audio stream in a maliciously crafted media file may terminate the process.	2026-07-27	5.5
CVE-2026-43754	apple - multiple products	This issue was addressed with improved redaction of sensitive information. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to leak sensitive kernel state.	2026-07-27	5.5
CVE-2026-43756	apple - multiple products	A logic issue was addressed with improved validation. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to access user-sensitive data.	2026-07-27	5.5
CVE-2026-43758	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, watchOS 26.6. An app may be able to access sensitive user data.	2026-07-27	5.5
CVE-2026-43759	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in macOS Tahoe 26.6, watchOS 26.6. An app may be able to access sensitive user data.	2026-07-27	5.5
CVE-2026-43763	apple - multiple products	A permissions issue was addressed by removing the vulnerable code. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to read files outside of its sandbox.	2026-07-27	5.5
CVE-2026-43765	apple - multiple products	This issue was addressed with improved handling of symlinks. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to modify protected parts of the file system.	2026-07-27	5.5
CVE-2026-43768	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination.	2026-07-27	5.5
CVE-2026-43774	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to access sensitive user data.	2026-07-27	5.5
CVE-2026-43775	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.8, macOS Tahoe 26.6. An app may be able to access sensitive user data.	2026-07-27	5.5
CVE-2026-43782	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to access sensitive user data.	2026-07-27	5.5

CVE-2026-43796	apple - multiple products	This issue was addressed with improved data protection. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to access sensitive user data.	2026-07-27	5.5
CVE-2026-43797	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6. An app may be able to access information about a user's contacts.	2026-07-27	5.5
CVE-2026-43800	apple - multiple products	An information disclosure issue was addressed by removing the vulnerable code. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, watchOS 26.6. An app may be able to access sensitive user data.	2026-07-27	5.5
CVE-2026-43801	apple - multiple products	This issue was addressed with improved checks. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to access sensitive user data.	2026-07-27	5.5
CVE-2026-43806	apple - macos	A denial of service issue was addressed by removing the vulnerable code. This issue is fixed in macOS Tahoe 26.6. A local attacker may be able to cause a denial of service.	2026-07-27	5.5
CVE-2026-43816	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	5.5
CVE-2026-43817	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to cause unexpected system termination.	2026-07-27	5.5
CVE-2026-43819	apple - macos	An access issue was addressed with additional sandbox restrictions. This issue is fixed in macOS Tahoe 26.6. An app may be able to access sensitive user data.	2026-07-27	5.5
CVE-2026-64693	apple - multiple products	A type confusion issue was addressed with improved checks. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing a maliciously crafted image may lead to a denial-of-service.	2026-07-27	5.5
CVE-2026-64699	apple - multiple products	A memory initialization issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to disclose kernel memory.	2026-07-27	5.5
CVE-2026-64707	apple - multiple products	A permissions issue was addressed with improved validation. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, visionOS 26.6. An app may be able to delete files for which it does not have permission.	2026-07-27	5.5
CVE-2026-64708	apple - multiple products	A file quarantine bypass was addressed with additional checks. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may bypass Gatekeeper checks.	2026-07-27	5.5
CVE-2026-64709	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to disclose kernel memory.	2026-07-27	5.5
CVE-2026-64710	apple - multiple products	A privacy issue was addressed by removing sensitive data. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to leak sensitive user information.	2026-07-27	5.5
CVE-2026-64711	apple - multiple products	This issue was addressed with additional entitlement checks. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to leak sensitive user information.	2026-07-27	5.5
CVE-2026-64718	apple - multiple products	A use-after-free issue was addressed with improved memory management. This issue is fixed in Safari 26.6, iOS 26.6 and iPadOS 26.6, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing maliciously crafted web content may lead to an unexpected Safari crash.	2026-07-27	5.5
CVE-2026-64721	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to access sensitive user data.	2026-07-27	5.5
CVE-2026-64722	apple - multiple products	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Tahoe 26.6. Processing a 3D model may result in disclosure of process memory.	2026-07-27	5.5
CVE-2026-64723	apple - multiple products	A logic issue was addressed with improved checks. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to access sensitive user data.	2026-07-27	5.5
CVE-2026-64724	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An attacker on the local network may be able to cause a denial-of-service.	2026-07-27	5.5
CVE-2026-64734	apple - multiple products	The issue was addressed with improved checks. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, visionOS 26.6, watchOS 26.6. Processing a maliciously crafted contact may leak sensitive data.	2026-07-27	5.5
CVE-2026-64741	apple - multiple products	A permissions issue was addressed with additional restrictions. This issue is fixed in iOS 26.6 and iPadOS 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. An app may be able to read a persistent device identifier.	2026-07-27	5.5
CVE-2026-64744	apple - multiple products	An information leakage was addressed with additional validation. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to disclose kernel memory.	2026-07-27	5.5
CVE-2026-64754	apple - multiple products	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6, visionOS 26.6, watchOS 26.6. Processing a maliciously crafted file may lead to a denial-of-service.	2026-07-27	5.5
CVE-2026-64755	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in iOS 26.6 and iPadOS 26.6. An app may be able to access sensitive user data.	2026-07-27	5.5
CVE-2026-64776	apple - multiple products	The issue was addressed with improved bounds checks. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to disclose kernel memory.	2026-07-27	5.5
CVE-2026-7775	ibm - multiple products	IBM Sterling B2B Integrator 6.2.0.0 through 6.2.0.6, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.0.0 through 6.2.0.6, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 is vulnerable to stored cross-site scripting. This vulnerability allows a privileged user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-07-28	5.5
CVE-2026-18201	redhat - build_of_keycloak	Keycloak provides a way to manage identity providers and organizations through its administrative API. A flaw was discovered where an administrator with permission to manage identity providers	2026-07-29	5.5

		could link a new provider to an organization without having the required permissions to manage that organization. This could allow an unauthorized administrator to influence how users log into specific organizations.		
CVE-2026-17932	google - chrome	Use after free in DataTransfer in Google Chrome on Windows prior to 151.0.7922.72 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	5.5
CVE-2026-17973	google - chrome	Inappropriate implementation in Views in Google Chrome on Mac prior to 151.0.7922.72 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	5.5
CVE-2025-36374	ibm - multiple products	IBM DataPower Gateway is vulnerable to an XML external entity injection (XXE) attack when processing XML data. A privileged user could exploit this vulnerability to expose sensitive information or consume memory resources.	2026-07-30	5.5
CVE-2026-68563	red hat - multiple products	A flaw was found in ansible-collection-redhat-leapp. When a remediation task is executed with elevated privileges and the `leapp_old_postgresql_data` option is selected, a PostgreSQL data backup archive is created with insecure permissions. This allows a local non-root user on the managed node to read sensitive archived PostgreSQL data, leading to information disclosure.	2026-07-30	5.5
CVE-2026-57978	microsoft - edge_chromium	Origin validation error in Microsoft Edge (Chromium-based) allows an unauthorized attacker to perform spoofing over a network.	2026-07-26	5.4
CVE-2026-62828	microsoft - edge	Improper input validation in Microsoft Edge for Android allows an unauthorized attacker to perform tampering over a network.	2026-07-28	5.4
CVE-2026-17728	google - Chrome	Inappropriate implementation in Extensions in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	5.4
CVE-2026-17734	google - Chrome	Inappropriate implementation in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	5.4
CVE-2026-17761	google - chrome	Insufficient validation of untrusted input in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via malicious network traffic. (Chromium security severity: Medium)	2026-07-30	5.4
CVE-2026-17779	google - chrome	Inappropriate implementation in Site Isolation in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass site isolation via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	5.4
CVE-2026-17799	google - chrome	Insufficient validation of untrusted input in Safe Browsing in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass discretionary access control via a malicious file. (Chromium security severity: Medium)	2026-07-30	5.4
CVE-2026-17812	google - chrome	Inappropriate implementation in DigitalCredentials in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	5.4
CVE-2026-17874	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	5.4
CVE-2026-17903	google - chrome	Insufficient policy enforcement in Chromecast in Google Chrome prior to 151.0.7922.72 allowed an attacker on the local network segment to inject scripts or HTML into a privileged page via malicious network traffic. (Chromium security severity: Low)	2026-07-30	5.4
CVE-2026-17913	google - Chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	5.4
CVE-2026-17915	google - chrome	Inappropriate implementation in WebView in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	5.4
CVE-2026-7260	php - multiple products	Circular symbolic links in phar archives could lead to unbounded recursion, exhausting the C stack and crashing the PHP process, in PHP versions from 8.2.* before 8.2.33, from 8.3.* before 8.3.33, from 8.4.* before 8.4.24, and from 8.5.* before 8.5.9.	2026-07-30	5.4
CVE-2025-36298	ibm - multiple products	IBM Sterling B2B Integrator 6.1.2.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.1.2.0 through 6.1.2.7_2, 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 Ebics server component is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-07-30	5.4
CVE-2025-36431	ibm - multiple products	IBM Sterling B2B Integrator 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.2.0 through 6.2.2.0_1 is vulnerable to cross-site scripting. This vulnerability allows an authenticated user to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	2026-07-30	5.4
CVE-2026-11383	ibm - Tivoli System Automation Application Manager	IBM Tivoli System Automation Application Manager 4.1 and IBM WebSphere Application Server is affected by cross-site scripting in the Administrative Console.	2026-07-30	5.4
CVE-2026-20316	cisco - multiple products	A vulnerability in the web interface of Cisco Secure Firewall Management Center (FMC) Software could allow an unauthenticated, remote attacker to log in to an affected device using a low-privileged account to access sensitive data within the impacted systems. This vulnerability is due to the presence of static user credentials for a low-privileged account. An attacker could exploit this vulnerability by using the account to log in to an affected system. A successful exploit could allow the attacker to log in to the affected system and access sensitive data as the low-privileged user. Note: If the FMC management interface does not have public internet access, the attack surface that is associated with this vulnerability is reduced. Cisco has assigned this security advisory a Security Impact Rating (SIR) of High rather than Medium	2026-07-29	5.3

		as the score indicates. The reason is that this vulnerability can be used with other Cisco Secure FMC Software vulnerabilities to elevate privileges.		
CVE-2026-17909	google - chrome	Insufficient validation of untrusted input in Isolated Web Apps in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via malicious network traffic. (Chromium security severity: Low)	2026-07-30	5.3
CVE-2026-17914	google - chrome	Side-channel information leakage in Skia in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	5.3
CVE-2026-17978	google - chrome	Side-channel information leakage in WebCodecs in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	5.3
CVE-2026-16531	red hat - multiple products	An unauthenticated remote attacker can exploit a path traversal vulnerability in the PCP pmproxy logger servlet using a crafted hostname. This allows arbitrary file and directory creation, potentially leading to a denial of service.	2026-07-30	5.3
CVE-2026-64635	veeam - Service Provider Console	Improper handling of the returnUrl parameter in the Forgot Password function of Veeam Service Provider Console allows an unauthenticated attacker to control the domain of the generated password reset link. When the targeted user clicks the link delivered by email, the reset code is transmitted to an attacker-controlled host, allowing the attacker to take over the account.	2026-07-30	5.3
CVE-2026-58218	red hat - multiple products	A flaw was found in Samba's internal DNS server where unauthenticated TKEY registration requests were added to the TKEY name cache before being rejected. A remote, unauthenticated attacker can exploit this behavior by sending a large number of TKEY requests with arbitrary names, exhausting the cache and evicting legitimate TKEY entries. This can prevent legitimate TSIG authentication for signed DNS queries, resulting in a denial of service.	2026-07-30	5.3
CVE-2026-23981	apache - superset	An Improper Authorization vulnerability exists in Apache Superset allowing an authenticated user with permissions to update charts to modify dashboards they do not own. When updating a chart's properties via the REST API, a user can provide a list of dashboard IDs (dashboards) to associate the chart with. The validation logic in the UpdateChartCommand failed to verify that the user had write permissions for the target dashboards specified in the request body. This issue affects Apache Superset: before 6.0.0. Users are recommended to upgrade to version 6.0.0, which fixes the issue.	2026-07-30	5.3
CVE-2026-23985	apache - superset	A Regular Expression Denial of Service (ReDoS) vulnerability exists in Apache Superset versions 1.5.0 through 5.0.0. The vulnerability is located in the sql_parse.py component, specifically within the SQL_REGEX used for parsing SQL statements in the sqlparse library integration. The affected regular expression contains overlapping disjunctions that share a common outer quantifier. An authenticated attacker can exploit this by sending a maliciously crafted input string (specifically a long sequence of backslashes or similar characters) to endpoints that process SQL queries This issue affects Apache Superset: before 6.0.0. Users are recommended to upgrade to version 6.0.0, which fixes the issue. Workarounds: ● WAF Rules: Implement Web Application Firewall (WAF) rules to detect and block requests containing excessively long sequences of backslashes or suspicious repeated patterns in the queries.extras.where parameter. ● Rate Limiting: Ensure strict rate limiting is applied to the /api/v1/chart/data endpoint to reduce the impact of potential attacks.	2026-07-30	5.3
CVE-2026-58216	red hat - multiple products	An out-of-bounds read flaw was found in Samba's Kerberos Key Distribution Center's (KDC) password change (kpasswd) service. When processing malformed ASN.1-encoded Kerberos password change request, Samba server miscalculates the structure size and attempts to read up to six bytes beyond the end of the allocated buffer. While this out-of-bounds read typically results in a harmless decryption failure, if the read hits unmapped memory, it causes the KDC process to crash. An authenticated attacker can send a specially crafted kpasswd request containing malformed ASN.1 data to trigger the out-of-bounds read, which may cause the KDC process to terminate, resulting in a denial of service.	2026-07-30	5.3
CVE-2026-11904	ibm - multiple products	IBM Verify Identity Access 11.0 through 11.0.2 and IBM Security Verify Access 10.0 through 10.0.9.1 and IBM Verify Identity Access Container 11.0 through 11.0.2 and IBM Security Verify Access Container 10.0 through 10.0.9.1 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system.	2026-07-30	5.3
CVE-2026-64607	apache software foundation - Apache HttpComponents Client	HttpClient based on the classic i/o model fails to correctly release the underlying connection back to the connection manager if it encounters an invalid or unsupported `Content-Encoding` header value in the response message. Please note this defect does not affect HttpClient based on the async i/o model. This issue affects Apache HttpComponents Client: from 5.0-alpha1 through 5.6.2.	2026-07-31	5.3
CVE-2026-43767	apple - multiple products	The issue was addressed with improved memory handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to cause unexpected system termination.	2026-07-27	5
CVE-2026-17737	google - chrome	Use after free in Bluetooth in Google Chrome on Android prior to 151.0.7922.72 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)	2026-07-30	5
CVE-2026-1918	ibm - multiple products	IBM Sterling B2B Integrator 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 stores potentially sensitive information in log files that could be read by a privileged user.	2026-07-28	4.9

CVE-2026-16105	redhat - build_of_keycloak	A flaw was found in the RoleContainerResource component of Keycloak. The issue occurs because certain name-based endpoints in the admin REST API do not properly enforce authorization checks when managing composite roles. This allows a delegated administrator with manage-realm permissions to remove essential child roles from built-in admin roles, potentially disrupting administrative functions within a realm.	2026-07-31	4.9
CVE-2026-43770	apple - multiple products	A race condition was addressed with additional validation. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6, tvOS 26.6. An app may be able to access sensitive user data.	2026-07-27	4.7
CVE-2026-43781	apple - multiple products	A race condition was addressed with improved state handling. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An app may be able to access sensitive user data.	2026-07-27	4.7
CVE-2026-43811	apple - multiple products	A race condition was addressed with improved checks. This issue is fixed in iOS 26.6 and iPadOS 26.6. An app may be able to modify protected parts of the file system.	2026-07-27	4.7
CVE-2026-43753	apple - multiple products	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 26.6 and iPadOS 26.6, macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An attacker with physical access to a locked device may be able to view sensitive user information.	2026-07-27	4.6
CVE-2026-43766	apple - multiple products	An authorization issue was addressed with improved state management. This issue is fixed in macOS Sequoia 15.7.8, macOS Sonoma 14.8.8, macOS Tahoe 26.6. An attacker with physical access to a locked device may be able to view sensitive user information.	2026-07-27	4.6
CVE-2026-64732	apple - multiple products	This issue was addressed through improved state management. This issue is fixed in iOS 26.6 and iPadOS 26.6. An attacker with physical access may be able to access sensitive user data during iPhone Mirroring.	2026-07-27	4.6
CVE-2026-56390	gnu - Bison	GNU Bison improperly handles grammar-defined output paths. Grammar directives such as %output and %header allow specifying file paths, which are accepted without restriction and override caller-supplied output options. When processing attacker-supplied grammar, this behavior allows directing generated files to arbitrary writable locations on the filesystem, potentially overwriting existing files accessible to the Bison process. Maintainers of this project were notified about this vulnerability, and fixed the issue in commit 8d101c19d4d9aaedf83a448c925513742d4efcf0. However, they did not provide vulnerable version range. Version 3.8.2 was tested and confirmed as vulnerable, other versions were not tested but might also be vulnerable.	2026-07-29	4.6
CVE-2026-8058	ibm - OPENBMC	IBM OPENBMC FW1110.00 through FW1110.20, and FW1060.00 through FW1060.71 allows a user to supply a password with a resource dump request stores that password into the BMC audit log where an admin user can see it.	2026-07-28	4.5
CVE-2026-7362	ibm - multiple products	IBM Sterling B2B Integrator 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 could allow an authenticated user to obtain sensitive information that should only be available to a privileged user.	2026-07-28	4.3
CVE-2026-3157	ibm - multiple products	IBM Sterling B2B Integrator 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 is vulnerable to an information disclosure due to sensitive information being included in the source code comments of a mailbox component.	2026-07-28	4.3
CVE-2026-3158	ibm - multiple products	IBM Sterling B2B Integrator 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 and IBM Sterling File Gateway 6.2.0.0 through 6.2.0.5_2, 6.2.1.0 through 6.2.1.1_2, and 6.2.2.0 through 6.2.2.0_1 is vulnerable to an information disclosure due to sensitive information being included in the source code comments of a dashboard component.	2026-07-28	4.3
CVE-2026-17662	google - Chrome	Insufficient policy enforcement in Prefetch in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	4.3
CVE-2026-17689	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	4.3
CVE-2026-17693	google - chrome	Insufficient policy enforcement in FileSystem in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	4.3
CVE-2026-17696	google - chrome	Side-channel information leakage in Media in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	4.3
CVE-2026-17700	google - chrome	Insufficient validation of untrusted input in Actor in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	4.3
CVE-2026-17706	google - Chrome	Insufficient validation of untrusted input in Media in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	4.3
CVE-2026-17730	google - chrome	Side-channel information leakage in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17731	google - chrome	Inappropriate implementation in Autofill in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17733	google - chrome	Inappropriate implementation in QUIC in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17740	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17742	google - chrome	Insufficient policy enforcement in Payments in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3

CVE-2026-17753	google - chrome	Inappropriate implementation in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17755	google - chrome	Incorrect security UI in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17757	google - chrome	Uninitialized Use in Skia in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17760	google - chrome	Side-channel information leakage in NoStatePrefetch in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17762	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17763	google - chrome	Inappropriate implementation in GPU in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17765	google - chrome	Inappropriate implementation in WebProtect in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17767	google - chrome	Insufficient validation of untrusted input in WebView in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17769	google - chrome	Insufficient validation of untrusted input in Cast in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17771	google - chrome	Uninitialized Use in Skia in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17772	google - chrome	Out of bounds read in WebGL in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17773	google - chrome	Insufficient validation of untrusted input in Cast in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17775	google - chrome	Inappropriate implementation in PresentationAPI in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17777	google - chrome	Inappropriate implementation in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17781	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17782	google - chrome	Incorrect security UI in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17783	google - chrome	Inappropriate implementation in Loader in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17785	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17788	google - chrome	Inappropriate implementation in Blink in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17790	google - chrome	Uninitialized Use in ANGLE in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17794	google - chrome	Insufficient validation of untrusted input in Mobile in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17795	google - chrome	Inappropriate implementation in GetUserMedia in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17798	google - chrome	Inappropriate implementation in Cast in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17802	google - chrome	Side-channel information leakage in GPU in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17808	google - chrome	Uninitialized Use in WebGL in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17810	google - chrome	Uninitialized Use in Dawn in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17815	google - chrome	Insufficient policy enforcement in GuestView in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17817	google - chrome	Inappropriate implementation in ReportingAndNEL in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17820	google - chrome	Insufficient policy enforcement in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3

CVE-2026-17829	google - chrome	Insufficient policy enforcement in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17833	google - chrome	Inappropriate implementation in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17843	google - chrome	Inappropriate implementation in CSS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17844	google - chrome	Insufficient validation of untrusted input in Cast in Google Chrome prior to 151.0.7922.72 allowed an attacker on the local network segment to leak cross-origin data via malicious network traffic. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17849	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via malicious network traffic. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17851	google - chrome	Side-channel information leakage in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17857	google - chrome	Inappropriate implementation in Network in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17858	google - chrome	Uninitialized Use in WebNN in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17859	google - chrome	Inappropriate implementation in Favicons in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17870	google - chrome	Insufficient validation of untrusted input in Cast in Google Chrome prior to 151.0.7922.72 allowed an attacker on the local network segment to leak cross-origin data via malicious network traffic. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17871	google - chrome	Inappropriate implementation in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17876	google - chrome	Inappropriate implementation in Payments in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17879	google - chrome	Inappropriate implementation in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17880	google - chrome	Inappropriate implementation in Autofill in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17885	google - chrome	Inappropriate implementation in Paint in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17889	google - chrome	Uninitialized Use in WebXR in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17895	google - chrome	Inappropriate implementation in DataTransfer in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17897	google - chrome	Inappropriate implementation in ORB in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.3
CVE-2026-17900	google - chrome	Inappropriate implementation in Enterprise in Google Chrome on Windows prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a malicious file. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17901	google - chrome	Insufficient validation of untrusted input in Sharing in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via malicious network traffic. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17904	google - chrome	Insufficient policy enforcement in NFC in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17905	google - chrome	Inappropriate implementation in SurfaceCapture in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17907	google - chrome	Side-channel information leakage in Network in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17910	google - chrome	Insufficient policy enforcement in NFC in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17911	google - chrome	Insufficient policy enforcement in SVG in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17912	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17925	google - chrome	Inappropriate implementation in Cast in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17927	google - chrome	Insufficient policy enforcement in DevTools in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension. (Chromium security severity: Low)	2026-07-30	4.3

CVE-2026-17928	google - chrome	Inappropriate implementation in DataTransfer in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17933	google - chrome	Inappropriate implementation in DOMStorage in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17934	google - chrome	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17937	google - chrome	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17938	google - chrome	Inappropriate implementation in FullScreen in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17939	google - chrome	Insufficient validation of untrusted input in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17941	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17942	google - chrome	Side-channel information leakage in SVG in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17943	google - chrome	Inappropriate implementation in Parser in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17944	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17945	google - chrome	Insufficient validation of untrusted input in Navigation in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17949	google - chrome	Uninitialized Use in GPU in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17954	google - chrome	Policy bypass in MHTML in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted MHTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17955	google - chrome	Insufficient validation of untrusted input in Payments in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17958	google - chrome	Inappropriate implementation in Views in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17959	google - chrome	Inappropriate implementation in Network in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17960	google - chrome	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to bypass no-referrer policy via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17961	google - chrome	Inappropriate implementation in Session in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17963	google - chrome	Inappropriate implementation in SVG in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17964	google - chrome	Incorrect security UI in UI in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17965	google - chrome	Incorrect security UI in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17970	google - chrome	Insufficient validation of untrusted input in Passwords in Google Chrome prior to 151.0.7922.72 allowed an attacker in a privileged network position to perform UI spoofing via malicious network traffic. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17972	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17976	google - chrome	Insufficient policy enforcement in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to bypass discretionary access control via a crafted domain name. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17977	google - chrome	Policy bypass in CSS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17981	google - chrome	Inappropriate implementation in Blink in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17982	google - chrome	Insufficient validation of untrusted input in Cast in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17983	google - chrome	Inappropriate implementation in Global Media Controls in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-17994	google - chrome	Inappropriate implementation in Media in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3

CVE-2026-17998	google - chrome	Incorrect security UI in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to perform UI spoofing via a crafted Chrome Extension. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-18003	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-18004	google - chrome	Insufficient policy enforcement in Speech in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-18006	google - chrome	Inappropriate implementation in Google Lens in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-18007	google - chrome	Inappropriate implementation in Input in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-18008	google - chrome	Inappropriate implementation in Settings in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-18009	google - chrome	Insufficient validation of untrusted input in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-18010	google - chrome	Inappropriate implementation in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-18013	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-18016	google - chrome	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-18019	google - chrome	Side-channel information leakage in Media in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	4.3
CVE-2026-10569	ibm - multiple products	IBM UCD - IBM UrbanCode Deploy 7.2 through 7.2.3.23, and 7.3 through 7.3.2.18 and IBM UCD - IBM DevOps Deploy 8.0 through 8.0.1.13, 8.1 through 8.1.2.6, and 8.2 through 8.2.1.0 is susceptible to an Exposure of Sensitive Information Vulnerability in plugin output logs. This exposure could allow an attacker with access to the logs to potentially obtain senstive values related to that step.	2026-07-30	4.3
CVE-2026-4932	ibm - PowerVM Hypervisor	IBM PowerVM Hypervisor FW1110.00 through FW1110.20, and FW1060.00 through FW1060.71 could allow an attacker with physical access to the Transparent Memory Encryption (TME) hardware to decrypt encrypted memory due to insufficient cryptographic entropy.	2026-07-28	4.2
CVE-2026-17659	google - chrome	Inappropriate implementation in SiteIsolation in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	2026-07-30	4.2
CVE-2026-17724	google - Chrome	Race in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: High)	2026-07-30	4.2
CVE-2026-17739	google - chrome	Insufficient policy enforcement in Extensions in Google Chrome prior to 151.0.7922.72 allowed an attacker who convinced a user to install a malicious extension to inject arbitrary scripts or HTML (UXSS) via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-07-30	4.2
CVE-2026-17747	google - chrome	Insufficient validation of untrusted input in Payments in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	4.2
CVE-2026-18211	redhat - build_of_keycloak	A flaw was found in the secure-client-uris client policy executor within Keycloak core services. This component is responsible for enforcing security requirements on client configurations, such as requiring encrypted connections for redirect URIs. Due to an improper check that only looks at the start of a web address rather than properly verifying the host, an attacker can bypass these security restrictions by using a specially crafted domain name. This could allow an attacker to intercept sensitive authentication codes over unencrypted connections.	2026-07-31	4.2
CVE-2026-18218	redhat - build_of_keycloak	A flaw was found in the TokenManager component of the Keycloak identity management service. When an administrator attempts to revoke tokens for a specific application (client) using a "not-before" policy, the revocation may be silently ignored if the overall security realm already has an older, non-zero revocation policy in place. This issue can allow previously issued tokens to remain valid for refreshing sessions and accessing user information even after an administrator has attempted to invalidate them. ———	2026-07-31	4.2
CVE-2026-18018	google - chrome	Inappropriate implementation in Updater in Google Chrome on Windows prior to 151.0.7922.72 allowed a local attacker to perform UI spoofing via a malicious file. (Chromium security severity: Low)	2026-07-30	4
CVE-2026-18206	redhat - build_of_keycloak	A flaw was found in the keycloak-services component of Keycloak, which provides identity and access management services. The issue occurs when a realm administrator uses a wildcard domain (like *.example.com) to restrict which hosts can register or update clients. Due to improper validation, the system accepts any hostname that ends with the specified domain suffix, even if it is not a legitimate subdomain. An attacker who can control the reverse DNS of their connection can bypass these host-based restrictions, potentially allowing unauthorized client modifications.	2026-07-31	3.7
CVE-2026-17902	google - chrome	Inappropriate implementation in Editing in Google Chrome on Linux prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	3.5

CVE-2026-18209	redhat - build_of_keycloak	A flaw was found in the keycloak-services component of Keycloak, which handles OpenID Connect (OIDC) authentication flows. The issue occurs because the security check designed to prevent HTTP parameter pollution only inspects the query portion of a redirect URL and ignores the fragment portion. When a client is configured with a wildcard redirect URI, an attacker can use this to inject duplicate security parameters into the login response. If a client application is not configured correctly, it might trust the attacker's injected data instead of the real security information from Keycloak, leading to session fixation or account confusion.	2026-07-31	3.4
CVE-2026-18217	redhat - build_of_keycloak	A flaw was found in the SAML protocol implementation of Keycloak, an open-source identity and access management solution. The issue occurs when Keycloak handles SAML authentication requests using the HTTP-Redirect binding. If a client is configured with a wildcard redirect URL, an attacker can craft a request that includes malicious parameters. When a user authenticates, Keycloak appends its legitimate response to the attacker's parameters. This can cause some service providers to process the attacker's data instead of the real login information, potentially leading to a user being logged into the wrong account.	2026-07-31	3.4
CVE-2026-17072	red hat - multiple products	A flaw was found in GStreamer's gst-plugins-good. A heap-based out-of-bounds read of 4 bytes can occur when parsing FLAC audio stream headers embedded in a Matroska or WebM container file. The vulnerability is triggered by a boundary check that does not account for the full size of the data being copied, allowing a small read past the end of the allocated buffer. An attacker could exploit this by crafting a malicious Matroska or WebM file and tricking a user into opening it, potentially leaking a small amount of adjacent heap memory.	2026-07-28	3.3
CVE-2026-17766	google - chrome	Insufficient validation of untrusted input in Clipboard in Google Chrome on Android prior to 151.0.7922.72 allowed a local attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	3.3
CVE-2026-17860	google - chrome	Insufficient validation of untrusted input in Mobile in Google Chrome on Android prior to 151.0.7922.72 allowed a local attacker to spoof the contents of the Omnibox (URL bar) via a malicious file. (Chromium security severity: Medium)	2026-07-30	3.3
CVE-2026-17984	google - chrome	Inappropriate implementation in Browser in Google Chrome on Android prior to 151.0.7922.72 allowed a local attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	3.3
CVE-2026-2482	ibm - websphere_application_server	IBM WebSphere Application Server - Liberty 17.0.0.3 through 26.0.0.8 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts.	2026-07-29	3.1
CVE-2026-17702	google - chrome	Inappropriate implementation in Skia in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	3.1
CVE-2026-17715	google - chrome	Inappropriate implementation in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	3.1
CVE-2026-17720	google - chrome	Insufficient policy enforcement in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-07-30	3.1
CVE-2026-17732	google - chrome	Inappropriate implementation in SVG in Google Chrome prior to 151.0.7922.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	3.1
CVE-2026-17826	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-07-30	3.1
CVE-2026-17957	google - chrome	Inappropriate implementation in CORS in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	3.1
CVE-2026-17980	google - chrome	Inappropriate implementation in UI in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who convinced a user to engage in specific UI gestures to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	3.1
CVE-2026-17997	google - chrome	Inappropriate implementation in Passwords in Google Chrome prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	3.1
CVE-2026-18000	google - chrome	Insufficient policy enforcement in USB in Google Chrome on Android prior to 151.0.7922.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-07-30	3.1
CVE-2026-41709	vmware - multiple products	VMware ESX contains an insufficient logging vulnerability. A malicious administrator could exploit this issue to perform certain operations without them being logged.	2026-07-30	2.7
CVE-2026-64745	apple - multiple products	This issue was addressed with additional restrictions on the lock screen. This issue is fixed in macOS Sequoia 15.7.8, macOS Tahoe 26.6. A person with physical access to a locked device may be able to access contacts and photos.	2026-07-27	2.4
CVE-2026-18011	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 151.0.7922.72 allowed a local attacker to obtain potentially sensitive information from process memory via physical access to the device. (Chromium security severity: Low)	2026-07-30	2.4

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.