Daily brief, Wednesday, May 6, 2026

May 5, 8:00 PM to May 6, 8:00 PM ET

Generated Nov 7, 2026, 3:10 AM ET

0	1	0	21	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 21 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.3 **CVE-2026-0300** Palo Alto Networks PAN-OS CISA KEV

An out-of-bounds write in Palo Alto Networks PAN-OS lets an attacker execute arbitrary code and fully compromise the system.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

21

9.3 **CVE-2026-0300** Palo Alto Networks PAN-OS KEV EXPLOIT CODE

An out-of-bounds write in Palo Alto Networks PAN-OS lets an attacker execute arbitrary code and fully compromise the system.

9.8 **CVE-2026-43125** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: dlm: validate length in dlm_search_rsb_tree The len parameter in dlm_dump_rsb_name() is not validated and comes from network messages. When it exceeds DLM_RESNAME_MAXLEN, it can cause out-of-b

9.8 **CVE-2026-43185** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix signededness bug in smb_direct_prepare_negotiation() smb_direct_prepare_negotiation() casts an unsigned __u32 value from sp->max_recv_size and req->preferred_send_size to a signed i

9.8 **CVE-2026-43186** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ipv6: ioam: fix heap buffer overflow in __ioam6_fill_trace_data() On the receive path, __ioam6_fill_trace_data() uses trace->nodelen to decide how much data to write for each node. It trusts t

9.8 **CVE-2026-43198** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: tcp: fix potential race in tcp_v6_syn_recv_sock() Code in tcp_v6_syn_recv_sock() after the call to tcp_v4_syn_recv_sock() is done too late. After tcp_v4_syn_recv_sock(), the child socket is al

9.8 **CVE-2026-43208** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: do not pass flow_id to set_rps_cpu() Blamed commit made the assumption that the RPS table for each receive queue would have the same size, and that it would not change. Compute flow_id in

9.6 **CVE-2026-7908** Google chrome

Use after free in Fullscreen in Google Chrome prior to 148.0.7778.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.6 **CVE-2026-7910** Google chrome

Use after free in Views in Google Chrome prior to 148.0.7778.96 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page. (Chromium security severity: High)

9.4 **CVE-2026-43114** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: netfilter: nft_set_pipapo_avx2: don't return non-matching entry on expiry New test case fails unexpectedly when avx2 matching functions are used. The test first loads a ranomly generated pipap

9.1 **CVE-2026-43083** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: ioam6: fix OOB and missing lock When trace->type.bit6 is set: if (trace->type.bit6) { ... queue = skb_get_tx_queue(dev, skb); qdisc = rcu_dereference(queue->qdisc); This code can lead to

9.1 **CVE-2026-43117** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: btrfs: tracepoints: get correct superblock from dentry in event btrfs_sync_file() If overlay is used on top of btrfs, dentry->d_sb translates to overlay's super block and fsid assignment will

9.1 **CVE-2026-43197** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: netconsole: avoid OOB reads, msg is not nul-terminated msg passed to netconsole from the console subsystem is not guaranteed to be nul-terminated. Before recent commit 7eab73b18630 ("netconsol

10.0 **CVE-2026-40281** Thecodingmachine gotenberg DETECTION

Gotenberg is a Docker-powered stateless API for PDF files. In versions 8.30.1 and earlier, the metadata write endpoint validates metadata keys for control characters but leaves metadata values unsanitized. A newline character in a metadata value splits the Exi

9.8 **CVE-2026-41930**

Vvveb before version 1.0.8.2 contains a hard-coded credentials vulnerability in its docker-compose-apache.yaml configuration that allows unauthenticated attackers to access the bundled phpMyAdmin container with pre-configured database credentials. Attackers ca

9.8 **CVE-2026-43575** Openclaw openclaw

OpenClaw versions 2026.2.21 before 2026.4.10 contain an authentication bypass vulnerability in the sandbox noVNC helper route that exposes interactive browser session credentials. Attackers can access the noVNC helper route without bridge authentication to gai

9.8 **CVE-2026-44109** Openclaw openclaw

OpenClaw before 2026.4.15 contains an authentication bypass vulnerability in Feishu webhook and card-action validation that allows unauthenticated requests to reach command dispatch. Missing encryptKey configuration and blank callback tokens fail open instead

9.6 **CVE-2026-43581** Openclaw openclaw

OpenClaw before 2026.4.10 contains an improper network binding vulnerability in the sandbox browser CDP relay that exposes Chrome DevTools Protocol on 0.0.0.0. Attackers can access the DevTools protocol outside intended local sandbox boundaries by exploiting t

9.6 **CVE-2026-44112** Openclaw openclaw

OpenClaw before 2026.4.22 contains a time-of-check/time-of-use race condition in OpenShell sandbox filesystem writes that allows attackers to redirect writes outside the intended mount root. Attackers can exploit symlink swaps during filesystem operations to b

9.1 **CVE-2026-40010** Apache wicket

Missing invocation of Servlet http web request method changeSessionId after session binding can be exploited for a session fixation attack in Apache Wicket. This issue affects Apache Wicket: from 8.0.0 through 8.17.0, 9.0.0, from 10.0.0 through 10.8.0. Users a

9.1 **CVE-2026-5081** Chorny apache\

Apache::Session::Generate::ModUniqueId versions from 1.54 through 1.94 for Perl session ids are insecure. Apache::Session::Generate::ModUniqueId (added in version 1.54) uses the value of the UNIQUE_ID environment variable for the session id. The UNIQUE_ID vari

1 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

LegionProxy legionproxy.io 10,144 accounts

Watch Floor collects CVE records, CISA KEV, exploit indexes, official advisories, security news and chatter. CVSS is the headline score. Ransomware posts are criminal groups' claims, not confirmed by the victims. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.