Daily brief, Friday, May 8, 2026

May 7, 8:00 PM to May 8, 8:00 PM ET

Generated Nov 7, 2026, 2:44 AM ET

0	1	0	54	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 54 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

9.3 **CVE-2026-42208** BerriAI LiteLLM CISA KEV DETECTION

An attacker can read data from the BerriAI LiteLLM proxy database via SQL injection, gaining unauthorized access to the proxy and the credentials it manages.

New public exploit code

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

New critical CVEs

54

9.3 **CVE-2026-42208** BerriAI LiteLLM KEV EXPLOIT CODE DETECTION

An attacker can read data from the BerriAI LiteLLM proxy database via SQL injection, gaining unauthorized access to the proxy and the credentials it manages.

9.8 **CVE-2026-41889** Jackc pgx EXPLOIT CODE

pgx is a PostgreSQL driver and toolkit for Go. Prior to version 5.9.2, SQL injection can occur when the non-default simple protocol is used, a dollar quoted string literal is used in the SQL query, that string literal contains text that would be would be inter

10.0 **CVE-2026-41070** Jkroepke openvpn-auth-oauth2

openvpn-auth-oauth2 is a plugin/management interface client for OpenVPN server to handle an OIDC based single sign-on (SSO) auth flows. From version 1.26.3 to before version 1.27.3, when openvpn-auth-oauth2 is deployed in the experimental plugin mode (shared l

9.8 **CVE-2026-43304** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: libceph: define and enforce CEPH_MAX_KEY_LEN When decoding the key, verify that the key material would fit into a fixed-size buffer in process_auth_done() and generally has a sane length. The

9.8 **CVE-2026-43341** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net/ipv6: ioam6: prevent schema length wraparound in trace fill ioam6_fill_trace_data() stores the schema contribution to the trace length in a u8. With bit 22 enabled and the largest schema p

9.8 **CVE-2026-43376** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free by using call_rcu() for oplock_info ksmbd currently frees oplock_info immediately using kfree(), even though it is accessed under RCU read-side critical sections in p

9.8 **CVE-2026-43378** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: smb: server: fix use-after-free in smb2_open() The opinfo pointer obtained via rcu_dereference(fp->f_opinfo) is dereferenced after rcu_read_unlock(), creating a use-after-free window.

9.8 **CVE-2026-43379** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in smb_lazy_parent_lease_break_close() opinfo pointer obtained via rcu_dereference(fp->f_opinfo) is being accessed after rcu_read_unlock() has been called. This creat

9.8 **CVE-2026-43384** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net/tcp-ao: Fix MAC comparison to be constant-time To prevent timing attacks, MACs need to be compared in constant time. Use the appropriate helper function for this.

9.8 **CVE-2026-43402** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: kthread: consolidate kthread exit paths to prevent use-after-free Guillaume reported crashes via corrupted RCU callback function pointers during KUnit testing. The crash was traced back to the

9.8 **CVE-2026-43414** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: scsi: qla2xxx: Completely fix fcport double free In qla24xx_els_dcmd_iocb() sp->free is set to qla2x00_els_dcmd_sp_free(). When an error happens, this function is called by qla2x00_sp_release(

9.8 **CVE-2026-43465** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net/mlx5e: RX, Fix XDP multi-buf frag counting for striding RQ XDP multi-buf programs can modify the layout of the XDP buffer when the program calls bpf_xdp_pull_data() or bpf_xdp_adjust_tail(

9.4 **CVE-2026-43383** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net/tcp-md5: Fix MAC comparison to be constant-time To prevent timing attacks, MACs need to be compared in constant time. Use the appropriate helper function for this.

9.1 **CVE-2026-43406** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: libceph: prevent potential out-of-bounds reads in process_message_header() If the message frame is (maliciously) corrupted in a way that the length of the control segment ends up being less th

9.1 **CVE-2026-43407** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: libceph: Fix potential out-of-bounds access in ceph_handle_auth_reply() This patch fixes an out-of-bounds access in ceph_handle_auth_reply() that can be triggered by a message of type CEPH_MSG

9.1 **CVE-2024-51092** Librenms librenms

LibreNMS before 24.10.0 allows a remote attacker to execute arbitrary code via OS command injection involving AboutController.php's index(), SettingsController.php's update(), and PollDevice.php's initRrdDirectory().

9.3 **CVE-2026-44128** SEPPmail AG Secure Email Gateway DETECTION

SEPPmail Secure Email Gateway before version 15.0.2.1 allows unauthenticated remote code execution in the new GINA UI because an endpoint passes attacker-controlled input from a parameter to Perl's eval.

9.8 **CVE-2026-42072** Orneryd NornicDB

Nornicdb is a distributed low-latency, Graph+Vector, Temporal MVCC with all sub-ms HNSW search, graph traversal, and writes. Prior to version 1.0.42-hotfix, the --address CLI flag (and NORNICDB_ADDRESS / server.host config key) is plumbed through to the HTTP s

9.8 **CVE-2026-44335** Praison praisonaiagents

PraisonAI is a multi-agent teams system. Prior to version 1.6.32, the URL checking logic in PraisonAI has a logical flaw that could be bypassed by attackers, leading to SSRF attacks. This issue has been patched in version 1.6.32.

9.1 **CVE-2026-41583** Zfnd zebra-script

ZEBRA is a Zcash node written entirely in Rust. Prior to zebrad version 4.3.1 and prior to zebra-script version 5.0.2, after a refactoring, Zebra failed to validate a consensus rule that restricted the possible values of sighash hash types for V5 transactions

34 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Zara zara.com 197,376 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.