Daily brief, Friday, April 24, 2026

Apr 23, 8:00 PM to Apr 24, 8:00 PM ET

Generated Nov 7, 2026, 5:32 AM ET

0	4	0	39	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

4 newly exploited, 39 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

4

9.9 **CVE-2024-57726** SimpleHelp SimpleHelp CISA KEV DETECTION

A low-privileged SimpleHelp technician creates API keys with excessive permissions through missing authorization, then escalates to the server admin role.

8.8 **CVE-2024-7399** Samsung MagicINFO 9 Server CISA KEV DETECTION

Path traversal in Samsung MagicINFO 9 Server lets an attacker write arbitrary files with system authority.

7.2 **CVE-2024-57728** SimpleHelp SimpleHelp CISA KEV DETECTION

Authenticated SimpleHelp admin users can upload a crafted zip (zip slip) to write files anywhere, achieving code execution as the SimpleHelp server user.

7.2 **CVE-2025-29635** D-Link DIR-823X CISA KEV DETECTION

D-Link DIR-823X contains a command injection vulnerability that allows an authorized attacker to execute arbitrary commands on remote devices by sending a POST request to /goform/set_prohibiting via the corresponding function. The impacted product could be end

New public exploit code

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

New critical CVEs

39

9.9 **CVE-2024-57726** SimpleHelp SimpleHelp KEV EXPLOIT CODE DETECTION

A low-privileged SimpleHelp technician creates API keys with excessive permissions through missing authorization, then escalates to the server admin role.

9.9 **CVE-2026-21515** Microsoft azure iot central

Exposure of sensitive information to an unauthorized actor in Azure IOT Central allows an authorized attacker to elevate privileges over a network.

9.8 **CVE-2026-31536** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: smb: server: let send_done handle a completion without IB_SEND_SIGNALED With smbdirect_send_batch processing we likely have requests without IB_SEND_SIGNALED, which will be destroyed in the fi

9.8 **CVE-2026-31589** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: mm: call ->free_folio() directly in folio_unmap_invalidate() We can only call filemap_free_folio() if we have a reference to (or hold a lock on) the mapping. Otherwise, we've already removed t

9.8 **CVE-2026-31607** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: usbip: validate number_of_packets in usbip_pack_ret_submit() When a USB/IP client receives a RET_SUBMIT response, usbip_pack_ret_submit() unconditionally overwrites urb->number_of_packets from

9.8 **CVE-2026-31608** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: smb: server: avoid double-free in smb_direct_free_sendmsg after smb_direct_flush_send_list() smb_direct_flush_send_list() already calls smb_direct_free_sendmsg(), so we should not call it agai

9.8 **CVE-2026-31609** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: smb: client: avoid double-free in smbd_free_send_io() after smbd_send_batch_flush() smbd_send_batch_flush() already calls smbd_free_send_io(), so we should not call it again after smbd_post_se

9.8 **CVE-2026-31633** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix integer overflow in rxgk_verify_response() In rxgk_verify_response(), there's a potential integer overflow due to rounding up token_len before checking it, thereby allowing the leng

9.8 **CVE-2026-31637** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: rxrpc: reject undecryptable rxkad response tickets rxkad_decrypt_ticket() decrypts the RXKAD response ticket and then parses the buffer as plaintext without checking whether crypto_skcipher_de

9.8 **CVE-2026-31649** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: stmmac: fix integer underflow in chain mode The jumbo_frm() chain-mode implementation unconditionally computes len = nopaged_len - bmax; where nopaged_len = skb_headlen(skb) (linear bytes

9.8 **CVE-2026-31657** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: batman-adv: hold claim backbone gateways by reference batadv_bla_add_claim() can replace claim->backbone_gw and drop the old gateway's last reference while readers still follow the pointer. Th

9.8 **CVE-2026-31659** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: batman-adv: reject oversized global TT response buffers batadv_tt_prepare_tvlv_global_data() builds the allocation length for a global TT response in 16-bit temporaries. When a remote originat

9.8 **CVE-2026-31668** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: seg6: separate dst_cache for input and output paths in seg6 lwtunnel The seg6 lwtunnel uses a single dst_cache per encap route, shared between seg6_input_core() and seg6_output_core(). These t

9.8 **CVE-2026-31669** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: mptcp: fix slab-use-after-free in __inet_lookup_established The ehash table lookups are lockless and rely on SLAB_TYPESAFE_BY_RCU to guarantee socket memory stability during RCU read-side crit

9.1 **CVE-2026-31636** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: rxrpc: fix RESPONSE authenticator parser OOB read rxgk_verify_authenticator() copies auth_len bytes into a temporary buffer and then passes p + auth_len as the parser limit to rxgk_do_verify_a

9.1 **CVE-2026-41677** Rust-Openssl Project rust-openssl

rust-openssl provides OpenSSL bindings for the Rust programming language. From 0.9.0 to before 0.10.78, the *_from_pem_callback APIs did not validate the length returned by the user's callback. A password callback that returns a value larger than the buffer it

9.9 **CVE-2026-41478** Saltcorn saltcorn

Saltcorn is an extensible, open source, no-code database application builder. Prior to 1.4.6, 1.5.6, and 1.6.0-beta.5, a SQL injection vulnerability in Saltcorn's mobile-sync routes allows any authenticated low-privilege user with read access to at least one t

9.8 **CVE-2026-25775**

A vulnerability in SenseLive X3050's remote management service allows firmware retrieval and update operations to be performed without authentication or authorization. The service accepts firmware-related requests from any reachable host and does not verify us

9.8 **CVE-2026-35503** Senselive x3500 firmware

A vulnerability in SenseLive X3050's web management interface allows authentication logic to be performed entirely on the client side, relying on hardcoded values within browser-executed scripts rather than server-side verification. An attacker with access to

9.8 **CVE-2026-40620** Senselive x3500 firmware

A vulnerability in SenseLive X3050's embedded management service allows full administrative control to be established without any form of authentication or authorization on the SenseLive config application. The service accepts management connections from any r

19 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Carnival carnivalcorp.com 7,531,359 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.