Daily brief, Saturday, August 15, 2026

Aug 14, 8:00 PM to Aug 15, 8:00 PM ET

Generated Nov 2, 2026, 12:06 PM ET

0	0	0	148	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

148 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

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

New critical CVEs

148

10.0 **CVE-2026-72407**

In the Linux kernel, the following vulnerability has been resolved: geneve: validate inner network offset in geneve_gro_complete() Even with both paths gated on gs->gro_hint, geneve_gro_complete() re-derives the inner dispatch type and length from the packet a

10.0 **CVE-2026-72408**

In the Linux kernel, the following vulnerability has been resolved: geneve: gate GRO hint in geneve_gro_complete() on gs->gro_hint geneve_gro_receive() reads the GRO hint through geneve_sk_gro_hint_off(), which honours it only when the socket enabled IFLA_GENE

10.0 **CVE-2026-72421**

In the Linux kernel, the following vulnerability has been resolved: ipv4: fib: Don't ignore error route in local/main tables. When CONFIG_IP_MULTIPLE_TABLES is enabled but no rule is added, fib_lookup() performs route lookup directly on two tables. Since the f

10.0 **CVE-2026-74279**

In the Linux kernel, the following vulnerability has been resolved: crypto: cavium/cpt - fix DMA cleanup using wrong loop index The sg_cleanup error path used list[i] instead of list[j] when unmapping DMA buffers, leaking successfully mapped entries and repeat

10.0 **CVE-2026-74280**

In the Linux kernel, the following vulnerability has been resolved: crypto: marvell/octeontx - fix DMA cleanup using wrong loop index The sg_cleanup path used list[i] instead of list[j] when unmapping DMA buffers, leaking successfully mapped entries and repeat

10.0 **CVE-2026-74309**

In the Linux kernel, the following vulnerability has been resolved: vdpa/octeon_ep: fix IRQ-to-ring mapping in interrupt handler Look up the IRQ index in oct_hw->irqs instead of assuming irq - irqs[0]. This supports non-contiguous IRQ numbers and avoids incorr

10.0 **CVE-2026-74475**

In the Linux kernel, the following vulnerability has been resolved: vxlan: use neigh_ha_snapshot() in route_shortcircuit() The neighbour hardware address n->ha can be updated asynchronously by the neighbour subsystem, protected by n->ha_lock seqlock. Reading n

10.0 **CVE-2026-74764**

Pandora contains a path traversal vulnerability in its TAR archive extraction functionality. When processing a submitted TAR archive, the extractor passed archive member names directly to Python's tarfile.TarFile.extract() without applying an extraction filter

9.9 **CVE-2026-72493**

In the Linux kernel, the following vulnerability has been resolved: net: serialize netif_running() check in enqueue_to_backlog() Syzbot reported a KASAN slab-use-after-free in fib_rules_lookup(). The root cause is a race condition where packets can escape the

9.8 **CVE-2026-15303**

The 6Storage Rentals plugin for WordPress is vulnerable to authentication bypass in versions up to, and including, 2.27.0. This is due to the six_storage_create_wp_user() AJAX handler being registered on wp_ajax_nopriv_six_storage_create_wp_user without any no

9.8 **CVE-2026-15341**

The User Session Synchronizer plugin for WordPress is vulnerable to Authentication Bypass leading to Account Takeover in all versions up to, and including, 1.4.0. The `synchronize_session()` function, hooked on `init` and therefore executed on every request, p

9.8 **CVE-2026-68476**

In the Linux kernel, the following vulnerability has been resolved: ipvs: reload ip header after head reallocation __ip_vs_get_out_rt() calls skb_ensure_writable() which may reallocate skb->head.

9.8 **CVE-2026-68477**

In the Linux kernel, the following vulnerability has been resolved: ipvs: fix more places with wrong ipv6 transport offsets Sashiko reports for more incorrect IPv6 transport offsets. The app code for TCP was assuming IPv4 network header even after the ipvsh ar

9.8 **CVE-2026-72014**

In the Linux kernel, the following vulnerability has been resolved: drbd: reject data replies with an out-of-range payload size recv_dless_read() receives a P_DATA_REPLY from a peer into the bio of an outstanding read request. The peer-supplied payload length

9.8 **CVE-2026-72020**

In the Linux kernel, the following vulnerability has been resolved: ipvs: reset full ip_vs_seq structs in ip_vs_conn_new Commit 9a05475cebdd ("ipvs: avoid kmem_cache_zalloc in ip_vs_conn_new") changed ip_vs_conn_new() to allocate an ip_vs_conn object with kmem

9.8 **CVE-2026-72033**

In the Linux kernel, the following vulnerability has been resolved: orangefs: keep the readdir entry size 64-bit in fill_from_part() fill_from_part() computes the size of a directory entry in size_t but stores it in a __u32. An entry length near U32_MAX wraps

9.8 **CVE-2026-72041**

In the Linux kernel, the following vulnerability has been resolved: espintcp: use sk_msg_free_partial to fix partial send sk_msg_free_partial() ensures consistency of the skmsg at every iteration, without having to manually handle uncharges and offsets. This s

9.8 **CVE-2026-72046**

In the Linux kernel, the following vulnerability has been resolved: gve: fix header buffer corruption with header-split and HW-GRO The DQO RX datapath programs a per-buffer-queue-descriptor header_buf_addr at post time and reads the split header back at comple

9.8 **CVE-2026-72064**

In the Linux kernel, the following vulnerability has been resolved: net: mana: Sync page pool RX frags for CPU MANA allocates RX buffers from page pool fragments when frag_count is greater than 1. In that case the buffers remain DMA mapped by page pool and the

9.8 **CVE-2026-72065**

In the Linux kernel, the following vulnerability has been resolved: net: mana: Validate the packet length reported by the NIC Validate the packet length reported in the RX CQE before passing it to skb processing. The CQE is supplied by the NIC device and shoul

128 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches

No new breaches published.

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. CVE IDs link to the full record on Watch Floor.