Daily brief, Sunday, July 19, 2026

Jul 18, 8:00 PM to Jul 19, 8:00 PM ET

Generated Nov 3, 2026, 1:59 PM ET

0	0	0	57	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

57 new critical CVEs, 1 new breaches.

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

57

9.8 **CVE-2026-63888** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: scsi: target: iscsi: Fix CRC overread and double-free in iscsit_handle_text_cmd() Two latent bugs in the Text-phase handler, both present since the original LIO integration in commit e48354ce0

9.8 **CVE-2026-63922** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ipv6: exthdrs: refresh nh after handling HAO option ip6_parse_tlv() caches skb_network_header(skb) in nh while walking IPv6 TLVs. ipv6_dest_hao() may call pskb_expand_head() for a cloned skb,

9.8 **CVE-2026-63912** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: xfrm: esp: restore combined single-frag length gate The ESP out-of-place fast path appends the trailer in esp_output_head() before esp_output_tail() allocates the destination page frag. The he

9.4 **CVE-2026-64024** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: tcp: fix stale per-CPU tcp_tw_isn leak enabling ISN prediction Blamed commit moved the TIME_WAIT-derived ISN from the skb control block to a per-CPU variable, assuming the value would always b

9.3 **CVE-2026-63939** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: KVM: SEV: Compute the correct max length of the in-GHCB scratch area When setting the length of the GHCB scratch area, and the area is in the GHCB shared buffer, set the effective length of th

9.3 **CVE-2026-63938** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: KVM: SEV: Check PSC request indices against the actual size of the buffer When processing Page State Change (PSC) requests, validate the PSC buffer against the effective size of the scratch ar

9.3 **CVE-2026-63940** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: KVM: SEV: Ignore Port I/O requests of length '0' Explicitly ignore Port I/O requests of length '0' (or count '0'), so that setting up the software scratch area (and other code) doesn't have to

10.0 **CVE-2026-63795** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: 9p: avoid putting oldfid in p9_client_walk() error path When p9_client_walk() is called with clone set to false, fid aliases oldfid. If the walk subsequently fails after the request has been s

9.8 **CVE-2026-53384** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: serial: 8250_dw: unregister 8250 port if clk_notifier_register() fails dw8250_probe() registers the 8250 port via serial8250_register_8250_port() and then, if the device has a clock, registers

9.8 **CVE-2026-53398** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: NFSD: Fix SECINFO_NO_NAME decode error cleanup nfsd4_decode_secinfo_no_name() currently initializes sin_exp after decoding sin_style. If the XDR stream is truncated, the decoder returns nfserr

9.8 **CVE-2026-53399** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: nfsd: release layout stid on setlease failure nfs4_alloc_stid() publishes the new stid into cl->cl_stateids via idr_alloc_cyclic() under cl_lock before returning to nfsd4_alloc_layout_stateid(

9.8 **CVE-2026-63800** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: pNFS: Fix use-after-free in pnfs_update_layout() When hitting the NFS_LAYOUT_RETURN branch in pnfs_update_layout(), the code calls pnfs_prepare_to_retry_layoutget(lo). If it succeeds, pnfs_put

9.8 **CVE-2026-63808** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: exfat: fix potential use-after-free in exfat_find_dir_entry() In exfat_find_dir_entry(), the buffer_head obtained from exfat_get_dentry() is released with brelse(bh) before the fall-through TY

9.8 **CVE-2026-63886** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: scsi: target: iscsi: Validate CHAP_R length before base64 decode chap_server_compute_hash() allocates client_digest as kzalloc(chap->digest_size) and then, for BASE64-encoded responses, passes

9.8 **CVE-2026-63887** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: scsi: target: iscsi: Bound iscsi_encode_text_output() appends to rsp_buf iscsi_encode_text_output() concatenates "key=value\0" records into login->rsp_buf, an 8192-byte kzalloc(MAX_KEY_VALUE_P

9.8 **CVE-2026-63924** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ipv6: exthdrs: refresh nh pointer after ipv6_hop_jumbo() ipv6_hop_jumbo() calls pskb_trim_rcsum(), which can change skb pointers. Let's recompute nh pointer to make sure any change won't mess

9.8 **CVE-2026-63993** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: vxlan: do not reuse cached ip_hdr() value after skb_tunnel_check_pmtu() skb_tunnel_check_pmtu() can change skb->head. Reusing old_iph afer skb_tunnel_check_pmtu() can cause an UAF. Use instead

9.8 **CVE-2026-63994** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: tunnels: load network headers after skb_cow() in iptunnel_pmtud_build_icmp[v6]() Sashiko found that iptunnel_pmtud_build_icmp() and iptunnel_pmtud_build_icmpv6() were caching ip_hdr() and ipv6

9.8 **CVE-2026-64000** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: hsr: fix potential OOB access in supervision frame handling Ensure the entire TLV header is linearized before access by adding sizeof(struct hsr_sup_tlv) to the pskb_may_pull() calls. Wit

9.8 **CVE-2026-64007** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: netfilter: synproxy: refresh tcphdr after skb_ensure_writable synproxy_tstamp_adjust() rewrites the TCP timestamp option in place and then patches the TCP checksum via inet_proto_csum_replace4

37 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Paidwork paidwork.com 23,272,765 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. CVE IDs link to the full record on Watch Floor.