Daily brief, Wednesday, June 24, 2026

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

Generated Nov 4, 2026, 1:04 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-2026-56121** Feast-Dev feast EXPLOIT CODE

Feast before 0.63.0 contains an unsafe deserialization vulnerability that allows unauthenticated or unauthorized attackers to achieve remote code execution by sending a crafted gRPC request to the registry server. The user_defined_function.body field of an OnD

9.8 **CVE-2026-53055** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: crypto: hisilicon/sec2 - prevent req used-after-free for sec During packet transmission, if the system is under heavy load, the hardware might complete processing the packet and free the reque

9.8 **CVE-2026-52914** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: batman-adv: fix fragment reassembly length accounting batman-adv keeps a running payload length for queued fragments and uses it to validate a fragment chain before reassembly. That accounting

9.8 **CVE-2026-52924** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: sctp: purge outqueue on stale COOKIE-ECHO handling sctp_stream_update() is only invoked when the association is moved into COOKIE_WAIT during association setup/reconfiguration. In this path, t

9.8 **CVE-2026-52931** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: batman-adv: tp_meter: avoid use of uninit sender vars batadv_tp_recv_ack() and batadv_tp_stop() are only valid for tp_vars in the BATADV_TP_SENDER role. When called with a BATADV_TP_RECEIVER r

9.8 **CVE-2026-52955** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: libceph: Fix potential out-of-bounds access in crush_decode() A message of type CEPH_MSG_OSD_MAP containing a crush map with at least one bucket has two fields holding the bucket algorithm. If

9.8 **CVE-2026-52982** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: usb: rtl8150: fix use-after-free in rtl8150_start_xmit() syzbot reported a KASAN slab-use-after-free read in rtl8150_start_xmit() when accessing skb->len for tx statistics after usb_submi

9.8 **CVE-2026-52986** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: netfilter: nf_conntrack_sip: don't use simple_strtoul Replace unsafe port parsing in epaddr_len(), ct_sip_parse_header_uri(), and ct_sip_parse_request() with a new sip_parse_port() helper that

9.8 **CVE-2026-52989** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: nvmet-tcp: propagate nvmet_tcp_build_pdu_iovec() errors to its callers Currently, when nvmet_tcp_build_pdu_iovec() detects an out-of-bounds PDU length or offset, it triggers nvmet_tcp_fatal_er

9.8 **CVE-2026-52993** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: tipc: fix double-free in tipc_buf_append() tipc_msg_validate() can potentially reallocate the skb it is validating, freeing the old one. In tipc_buf_append(), it was being called with a pointe

9.8 **CVE-2026-53002** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: netfilter: conntrack: remove sprintf usage Replace it with scnprintf, the buffer sizes are expected to be large enough to hold the result, no need for snprintf+overflow check. Increase buffer

9.8 **CVE-2026-53006** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ipv6: fix possible UAF in icmpv6_rcv() Caching saddr and daddr before pskb_pull() is problematic since skb->head can change. Remove these temporary variables: - We only access &ipv6_hdr(skb)->

9.8 **CVE-2026-53010** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free in smb2_open during durable reconnect In smb2_open, the call to ksmbd_put_durable_fd(fp) drops the reference to the durable file descriptor early during the durable r

9.8 **CVE-2026-53045** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: memory: tegra124-emc: Fix dll_change check The code checking whether the specified memory timing enables DLL in the EMRS register was reversed. DLL is enabled if bit A0 is low. Fix the check.

9.8 **CVE-2026-53046** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: fix use-after-free from async crypto on Qualcomm crypto engine ksmbd_crypt_message() sets a NULL completion callback on AEAD requests and does not handle the -EINPROGRESS return code fr

9.8 **CVE-2026-53049** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: gfs2: add some missing log locking Function gfs2_logd() calls the log flushing functions gfs2_ail1_start(), gfs2_ail1_wait(), and gfs2_ail1_empty() without holding sdp->sd_log_flush_lock, but

9.8 **CVE-2026-53086** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: bcmgenet: fix racing timeout handler The bcmgenet_timeout handler tries to take down all tx queues when a single queue times out. This is over zealous and causes many race conditions with

9.8 **CVE-2026-53088** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: bcmgenet: fix off-by-one in bcmgenet_put_txcb The write_ptr points to the next open tx_cb. We want to return the tx_cb that gets rewinded, so we must rewind the pointer first then return

9.6 **CVE-2026-13028** Google chrome

+1 more CVEs in the same release

Use after free in WebGL in Google Chrome on Android prior to 149.0.7827.197 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: Critical)

9.1 **CVE-2026-52958** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: libceph: Fix potential out-of-bounds access in osdmap_decode() When decoding osd_state and osd_weight from an incoming osdmap in osdmap_decode(), both are decoded for each osd, i.e., map->max_

36 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Madison Square Garden Sports msgsports.com 9,796,738 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.