Daily brief, Thursday, June 25, 2026

Jun 24, 8:00 PM to Jun 25, 8:00 PM ET

Generated Nov 4, 2026, 11:58 AM ET

0	2	0	40	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 40 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild 2

9.3 **CVE-2026-12569** PTC Windchill and FlexPLM CISA KEV

An unauthenticated, remote attacker can execute arbitrary code on PTC Windchill and FlexPLM.

8.6 **CVE-2026-20230** Cisco Unified Communications Manager CISA KEV DETECTION

Cisco Unified Communications Manager (Unified CM) and Cisco Unified Communications Manager Session Management Edition (Unified CM SME) contain a server-side request forgery (SSRF) Vulnerability that could allow an unauthenticated, remote attacker to write file

New public exploit code

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

New critical CVEs 40

9.3 **CVE-2026-12569** PTC Windchill and FlexPLM KEV EXPLOIT CODE

An unauthenticated, remote attacker can execute arbitrary code on PTC Windchill and FlexPLM.

9.8 **CVE-2026-53151** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: rxrpc: Fix the ACK parser to extract the SACK table for parsing Fix modification of the received skbuff in rxrpc_input_soft_acks() and a potential incorrect access of the buffer in a fragmente

9.8 **CVE-2026-53175** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: inet: frags: fix use-after-free caused by the fqdir_pre_exit() flush On netns teardown, fqdir_pre_exit() walks the fqdir rhashtable and flushes every fragment queue that is not yet complete us

9.8 **CVE-2026-53176** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: IB/isert: Reject login PDUs shorter than ISER_HEADERS_LEN In drivers/infiniband/ulp/isert/ib_isert.c, isert_login_recv_done() computes the login request payload length as wc->byte_len minus IS

9.8 **CVE-2026-53215** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: mvpp2: refill RX buffers before XDP or skb use The RX error path returns the current descriptor buffer to the hardware BM pool. That is only valid while the driver still owns the buffer.

9.8 **CVE-2026-53216** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: mvpp2: limit XDP frame size to the RX buffer mvpp2 has short and long BM pools, and short pool buffers can be smaller than PAGE_SIZE. The XDP path nevertheless initializes every xdp_buff

9.8 **CVE-2026-53221** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ip6_vti: fix incorrect tunnel matching in vti6_tnl_lookup() In vti6_tnl_lookup(), when an exact match for a tunnel fails, the code falls back to searching for wildcard tunnels: - Tunnels match

9.8 **CVE-2026-53228** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ipv6: sit: reload inner IPv6 header after GSO offloads ipip6_tunnel_xmit() caches the inner IPv6 header pointer at function entry and continues using it after iptunnel_handle_offloads(). For G

9.8 **CVE-2026-53246** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: sctp: validate cached peer INIT chunk length in COOKIE_ECHO processing When a listening SCTP server processes a COOKIE_ECHO chunk, the cached peer INIT chunk embedded after the cookie is parse

9.8 **CVE-2026-53247** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: net: ethernet: mtk_eth_soc: Fix use-after-free in metadata dst teardown mtk_free_dev() calls metadata_dst_free() which frees the metadata_dst with kfree() immediately, bypassing the RCU grace

9.8 **CVE-2026-53260** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: tcp: Add preempt_{disable,enable}_nested() in reqsk_queue_hash_req(). syzbot reported a weird reqsk->rsk_refcnt underflow in __inet_csk_reqsk_queue_drop(). The captured reqsk_put() in __inet_c

9.4 **CVE-2026-53131** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: netfilter: require Ethernet MAC header before using eth_hdr() `ip6t_eui64`, `xt_mac`, the `bitmap:ip,mac`, `hash:ip,mac`, and `hash:mac` ipset types, and `nf_log_syslog` access `eth_hdr(skb)`

9.1 **CVE-2026-53186** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: RDMA/srp: bound SRP_RSP sense copy by the received length srp_process_rsp() copies sense data from rsp->data + resp_data_len, where resp_data_len is the full 32-bit value supplied by the SRP t

9.1 **CVE-2026-53224** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: sctp: validate embedded INIT chunk and address list lengths in cookie sctp_unpack_cookie() only checked that the embedded INIT chunk length did not exceed the remaining cookie payload, but did

9.1 **CVE-2026-53225** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: sctp: fix uninit-value in __sctp_rcv_asconf_lookup() __sctp_rcv_asconf_lookup() in net/sctp/input.c only checks that the ASCONF chunk can hold the ADDIP header and a parameter header, then cal

9.8 **CVE-2025-71334** Flowiseai flowise DETECTION

Flowise before 3.0.6 contains an arbitrary file access vulnerability due to missing validation that the chatflowId and chatId parameters are UUIDs or numbers in file handling operations. By supplying a path-traversal value (e.g., '../../../../../tmp') as the c

10.0 **CVE-2026-46752**

Redis Lua HEAP overflow in cjson library vulnerability in Apache Kvrocks. This issue affects Apache Kvrocks: from 2.0.4 through 2.15.0. Users are recommended to upgrade to version 2.16.0, which fixes the issue.

10.0 **CVE-2026-54917** Seaweedfs seaweedfs DETECTION

SeaweedFS is a distributed storage system for object storage (S3), file systems, and Iceberg tables. Prior to 4.30, the S3 API gateway and the Iceberg REST catalog gateway construct their routers with mux.NewRouter().SkipClean(true). With path cleaning disable

10.0 **CVE-2026-57700**

Unrestricted Upload of File with Dangerous Type vulnerability in Daan.Dev OMGF Pro allows Using Malicious Files. This issue affects OMGF Pro: from n/a through 5.2.6.

10.0 **CVE-2025-71338** Flowiseai flowise

Flowise through 2.2.7 fails to sanitize path segments in the document-store loader endpoint, allowing unauthenticated attackers to write files outside the storage directory. Attackers can use parent-directory sequences to escape the storage directory and overw

20 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.