Daily brief, Saturday, July 25, 2026

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

Generated Nov 3, 2026, 8:29 AM ET

0	0	0	25	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

25 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

25

9.8 **CVE-2026-64268** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: RDMA/siw: bound Read Response placement to the RREAD length In drivers/infiniband/sw/siw/siw_qp_rx.c, siw_proc_rresp() places each inbound Read Response DDP segment at sge->laddr + wqe->proces

9.8 **CVE-2026-64303** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: spi: fsl-lpspi: terminate the RX channel on TX prepare failure path When dmaengine_prep_slave_sg() fails for the TX channel, the error path terminates the TX DMA channel but leaves the RX chan

9.8 **CVE-2026-64355** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: bpf: Reject fragmented frames in devmap Devmap broadcast redirects clone the packet for all but the last destination. For native XDP, that clone path copies only the linear xdp_frame data, whi

9.8 **CVE-2026-64383** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: smb: client: fix double-free in SMB2_flush() replay SMB2_flush() keeps its response buffer bookkeeping across replay attempts. If a replayable flush response is received and the retry then fai

9.8 **CVE-2026-64384** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: smb: client: fix change notify replay double-free A response-bearing attempt can return a replayable error and free its response buffer. If SMB2_notify_init() fails before the next send, clean

9.8 **CVE-2026-64385** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: smb: client: fix double-free in SMB2_ioctl() replay A response-bearing attempt can return a replayable error and free its response buffer. If SMB2_ioctl_init() fails before the next send, clea

9.8 **CVE-2026-64386** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: smb: client: fix query_info() replay double-free A response-bearing attempt can return a replayable error and free its response buffer. If SMB2_query_info_init() fails before the next send, cl

9.8 **CVE-2026-64387** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: smb: client: fix query directory replay double-free A response-bearing attempt can return a replayable error and free its response buffer. If SMB2_query_directory_init() fails before the next

9.8 **CVE-2026-64391** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: use opener credentials for ADS I/O Alternate data streams are stored as xattrs. Unlike regular file I/O, their read and write paths therefore call VFS xattr helpers which recheck inode

9.8 **CVE-2026-64397** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: serialize QUERY_DIRECTORY requests per file smb2_query_dir() stores a pointer to its stack-allocated private data in the ksmbd_file readdir_data. Concurrent QUERY_DIRECTORY requests usi

9.8 **CVE-2026-64399** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: add permission checks for FSCTL_DUPLICATE_EXTENTS_TO_FILE The FSCTL_DUPLICATE_EXTENTS_TO_FILE arm of smb2_ioctl() overwrites the destination file's data via vfs_clone_file_range() with

9.8 **CVE-2026-64410** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: netfilter: flowtable: IPIP tunnel hardware offload is not yet support No driver supports for IPIP tunnels yet, give up early on setting up the hardware offload for this scenario. This patch ad

9.8 **CVE-2026-64439** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: crypto: krb5 - filter out async aead implementations at alloc krb5_aead_encrypt(), krb5_aead_decrypt() in rfc3961_simplified.c and rfc8009_encrypt(), rfc8009_decrypt() in rfc8009_aes2.c set a

9.1 **CVE-2026-64257** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: smb: client: reject overlapping data areas in SMB2 responses Commit 53b7c271f06b ("smb: client: restrict implied bcc[0] exemption to responses without data area") restricted the implied bcc[0]

9.1 **CVE-2026-64269** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: RDMA/rtrs-srv: Bound RDMA-Write length to chunk size in rdma_write_sg When the server answers an RTRS READ, rdma_write_sg() builds the source scatter/gather entry for the IB_WR_RDMA_WRITE that

9.1 **CVE-2026-64319** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: nvmet-auth: validate reply message payload bounds against transfer length nvmet_auth_reply() accesses the variable-length rval[] array using attacker-controlled hl (hash length) and dhvlen (DH

9.1 **CVE-2026-64320** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: nvmet: fix pre-auth out-of-bounds heap read in Discovery Get Log Page nvmet_execute_disc_get_log_page() validates only the dword alignment of the host-supplied Log Page Offset (lpo). The 64-bi

9.1 **CVE-2026-64392** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: use opener credentials for delete-on-close Delete-on-close can be completed by deferred or durable handle teardown, where no request work is available. Both the base-file unlink and the

9.1 **CVE-2026-64393** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: ksmbd: run set info with opener credentials SMB2 SET_INFO handlers call path-based VFS helpers after checking the access mask granted to the SMB handle. Those helpers perform their owner, inod

9.1 **CVE-2026-64450** Linux linux kernel

In the Linux kernel, the following vulnerability has been resolved: tipc: fix out-of-bounds read in broadcast Gap ACK blocks A broadcast PROTOCOL/STATE_MSG can carry a Gap ACK blocks record in its data area. tipc_get_gap_ack_blks() only verifies that the recor

5 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.