Daily brief, Thursday, December 4, 2025

Dec 3, 7:00 PM to Dec 4, 7:00 PM ET

Generated Nov 9, 2026, 6:05 AM ET

0	0	0	15	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

15 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

15

9.8 **CVE-2025-29268** Allnet all-rut22gw firmware DETECTION

ALLNET ALL-RUT22GW v3.3.8 was discovered to store hardcoded credentials in the libicos.so library.

9.8 **CVE-2025-29269** Allnet all-rut22gw firmware DETECTION

ALLNET ALL-RUT22GW v3.3.8 was discovered to contain an OS command injection vulnerability via the command parameter in the popen.cgi endpoint.

9.8 **CVE-2025-66576** Remotecontrolio remote keyboard desktop

Remote Keyboard Desktop 1.0.1 enables remote attackers to execute system commands via the rundll32.exe exported function export, allowing unauthenticated code execution.

9.1 **CVE-2025-65346** Alexusmai laravel file manager

alexusmai laravel-file-manager 3.3.1 and below is vulnerable to Directory Traversal. The unzip/extraction functionality improperly allows archive contents to be written to arbitrary locations on the filesystem due to insufficient validation of extraction paths

9.3 **CVE-2025-66571**

UNA CMS versions 9.0.0-RC1 - 14.0.0-RC4 contain a PHP object injection vulnerability in BxBaseMenuSetAclLevel.php where the profile_id POST parameter is passed to PHP unserialize() without proper handling, allowing remote, unauthenticated attackers to inject a

9.8 **CVE-2025-40252**

In the Linux kernel, the following vulnerability has been resolved: net: qlogic/qede: fix potential out-of-bounds read in qede_tpa_cont() and qede_tpa_end() The loops in 'qede_tpa_cont()' and 'qede_tpa_end()', iterate over 'cqe->len_list[]' using only a zero-l

9.8 **CVE-2025-63362** Waveshare rs232\/485 to wifi eth \(b\) firmware

Waveshare RS232/485 TO WIFI ETH (B) Serial to Ethernet/Wi-Fi Gateway Firmware V3.1.1.0: HW 4.3.2.1: Webpage V7.04T.07.002880.0301 allows attackers to set the Administrator password and username as blank values, allowing attackers to bypass authentication.

9.8 **CVE-2025-40261**

In the Linux kernel, the following vulnerability has been resolved: nvme: nvme-fc: Ensure ->ioerr_work is cancelled in nvme_fc_delete_ctrl() nvme_fc_delete_assocation() waits for pending I/O to complete before returning, and an error can cause ->ioerr_work to

9.8 **CVE-2025-54304** Thermofisher ion torrent onetouch 2 firmware

An issue was discovered on Thermo Fisher Ion Torrent OneTouch 2 INS1005527 devices. When they are powered on, an X11 display server is started. The display server listens on all network interfaces and is accessible over port 6000. The X11 access control list,

9.8 **CVE-2025-40257**

In the Linux kernel, the following vulnerability has been resolved: mptcp: fix a race in mptcp_pm_del_add_timer() mptcp_pm_del_add_timer() can call sk_stop_timer_sync(sk, &entry->add_timer) while another might have free entry already, as reported by syzbot. Ad

9.8 **CVE-2025-40258**

In the Linux kernel, the following vulnerability has been resolved: mptcp: fix race condition in mptcp_schedule_work() syzbot reported use-after-free in mptcp_schedule_work() [1] Issue here is that mptcp_schedule_work() schedules a work, then gets a refcount o

9.8 **CVE-2025-53963** Thermofisher ion torrent onetouch 2 firmware

An issue was discovered on Thermo Fisher Ion Torrent OneTouch 2 INS1005527 devices. They run an SSH server accessible over the default port 22. The root account has a weak default password of ionadmin, and a password change policy for the root account is not e

9.8 **CVE-2025-66509** Laradashboard lara dashboard

LaraDashboard is an all-In-one solution to start a Laravel Application. In 2.3.0 and earlier, the password reset flow trusts the Host header, allowing attackers to redirect the administrator’s reset token to an attacker-controlled server. This can be combined

9.8 **CVE-2025-54303** Thermofisher torrent suite software

The Thermo Fisher Torrent Suite Django application 5.18.1 has weak default credentials, which are stored as fixtures for the Django ORM API. The ionadmin user account can be used to authenticate to default deployments with the password ionadmin. The user guide

9.6 **CVE-2024-45538** Synology DiskStation Manager (DSM)
Product not on watchlist.

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. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.