Daily brief, Sunday, March 8, 2026

Mar 7, 7:00 PM to Mar 8, 8:00 PM ET

Generated Nov 7, 2026, 2:04 PM ET

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

2 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

2

9.8 **CVE-2026-3703** Wavlink wl-nu516u1 firmware

A flaw has been found in Wavlink NU516U1 251208. This affects the function sub_401A10 of the file /cgi-bin/login.cgi. Executing a manipulation of the argument ipaddr can lead to out-of-bounds write. The attack may be performed from remote. The exploit has been

9.8 **CVE-2026-30909** Timlegge crypt\

Crypt::NaCl::Sodium versions through 2.002 for Perl has potential integer overflows. bin2hex, encrypt, aes256gcm_encrypt_afternm and seal functions do not check that output size will be less than SIZE_MAX, which could lead to integer wraparound causing an unde

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.