Daily brief, Saturday, February 7, 2026

Feb 6, 7:00 PM to Feb 7, 7:00 PM ET

Generated Nov 7, 2026, 6:39 PM ET

0	0	0	6	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

6 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

6

9.8 **CVE-2020-37161** Wedding-Slideshow-Studio wedding slideshow studio

Wedding Slideshow Studio 1.36 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting the registration name field with malicious payload. Attackers can craft a specially designed payload to trigger remote code ex

9.8 **CVE-2020-37095**

Cyberoam Authentication Client 2.1.2.7 contains a buffer overflow vulnerability that allows remote attackers to execute arbitrary code by overwriting Structured Exception Handler (SEH) memory. Attackers can craft a malicious input in the 'Cyberoam Server Addre

9.8 **CVE-2026-25560** Wekan Project wekan

WeKan versions prior to 8.19 contain an LDAP filter injection vulnerability in LDAP authentication. User-supplied username input is incorporated into LDAP search filters and DN-related values without adequate escaping, allowing an attacker to manipulate LDAP q

9.8 **CVE-2020-37162** Wedding-Slideshow-Studio wedding slideshow studio

Wedding Slideshow Studio 1.36 contains a buffer overflow vulnerability in the registration key input that allows attackers to execute arbitrary code by overwriting memory. Attackers can craft a malicious payload of 1608 bytes to trigger a stack-based buffer ov

9.1 **CVE-2026-25858** Macrozheng mall

macrozheng mall version 1.0.3 and prior contains an authentication vulnerability in the mall-portal password reset workflow that allows an unauthenticated attacker to reset arbitrary user account passwords using only a victim's telephone number. The password r

9.8 **CVE-2020-37159**

Parallaxis Cuckoo Clock 5.0 contains a buffer overflow vulnerability that allows attackers to execute arbitrary code by overwriting memory registers in the alarm scheduling feature. Attackers can craft a malicious payload exceeding 260 bytes to overwrite EIP a

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.