Daily brief, Saturday, March 21, 2026

Mar 20, 8:00 PM to Mar 21, 8:00 PM ET

Generated Nov 7, 2026, 11:23 AM 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-2019-25568** Microvirt memu

Memu Play 6.0.7 contains an insecure file permissions vulnerability that allows low-privilege users to escalate privileges by replacing the MemuService.exe executable. Attackers can rename and overwrite MemuService.exe in the installation directory with a mali

9.1 **CVE-2026-24060**

Service information is not encrypted when transmitted as BACnet packets over the wire, and can be sniffed, intercepted, and modified by an attacker. Valuable information such as the File Start Position and File Data can be sniffed from network traffic using Wi

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.