Daily brief, Saturday, February 21, 2026

Feb 20, 7:00 PM to Feb 21, 7:00 PM ET

Generated Nov 7, 2026, 4:24 PM ET

0	0	0	5	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

5 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

5

9.8 **CVE-2026-27194** Man d-tale

D-Tale is a visualizer for pandas data structures. Versions prior to 3.20.0 are vulnerable to Remote Code Execution through the /save-column-filter endpoint. Users hosting D-Tale publicly can be vulnerable to remote code execution allowing attackers to run mal

10.0 **CVE-2026-27211** Cloudhypervisor cloud hypervisor

Cloud Hypervisor is a Virtual Machine Monitor for Cloud workloads. Versions 34.0 through 50.0 arevulnerable to arbitrary host file exfiltration (constrained by process privileges) when using virtio-block devices backed by raw images. A malicious guest can over

9.9 **CVE-2026-27574** Hackerbay oneuptime

OneUptime is a solution for monitoring and managing online services. In versions 9.5.13 and below, custom JavaScript monitor feature uses Node.js's node:vm module (explicitly documented as not a security mechanism) to execute user-supplied code, allowing trivi

9.1 **CVE-2026-27197** Sentry sentry

Sentry is a developer-first error tracking and performance monitoring tool. Versions 21.12.0 through 26.1.0 have a critical vulnerability in its SAML SSO implementation which allows an attacker to take over any user account by using a malicious SAML Identity P

9.1 **CVE-2026-27471** Frappe erpnext

ERP is a free and open source Enterprise Resource Planning tool. In versions up to 15.98.0 and 16.0.0-rc.1 and through 16.6.0, certain endpoints lacked access validation which allowed for unauthorized document access. This issue has been fixed in versions 15.9

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.