Daily brief, Saturday, April 4, 2026

Apr 3, 8:00 PM to Apr 4, 8:00 PM ET

Generated Nov 7, 2026, 9:09 AM ET

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

2 new critical CVEs, 2 new breaches.

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-2016-20052** Snewscms snews

Snews CMS 1.7 contains an unrestricted file upload vulnerability that allows unauthenticated attackers to upload arbitrary files including PHP executables to the snews_files directory. Attackers can upload malicious PHP files through the multipart form-data up

9.8 **CVE-2018-25254** Nico-Ftp Project nico-ftp

NICO-FTP 3.0.1.19 contains a structured exception handler buffer overflow vulnerability that allows remote attackers to execute arbitrary code by sending crafted FTP commands. Attackers can connect to the FTP service and send oversized data in response handler

Ransomware

No leak-site posts collected.

New data breaches

2

Crunchyroll	crunchyroll.com	1,195,684 accounts
SongTrivia2	songtrivia2.io	291,739 accounts

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.