Daily brief, Saturday, June 13, 2026

Jun 12, 8:00 PM to Jun 13, 8:00 PM ET

Generated Nov 4, 2026, 11:54 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-2026-12183**

Nefteprodukttekhnika BUK TS-G Gas Station Automation System 2.9.1 through 2.10.2 on Linux contains an Improper Authentication vulnerability (CWE-287) in the system configuration module.

9.4 **CVE-2026-11624**

The Model Context Protocol has a security warning advising servers to validate the "Origin" header on all incoming connections to prevent DNS rebinding attacks. Prior to the v0.25.0 release, users had no way to validate the origin's host. In v0.25.0, a new "--

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. CVE IDs link to the full record on Watch Floor.