Daily brief, Saturday, May 16, 2026

May 15, 8:00 PM to May 16, 8:00 PM ET

Generated Nov 7, 2026, 1:04 AM ET

0	0	0	3	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

3 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

3

9.8 **CVE-2020-37228**

iDS6 DSSPro Digital Signage System 6.2 contains a CAPTCHA security bypass vulnerability that allows attackers to bypass authentication by requesting the autoLoginVerifyCode object. Attackers can retrieve valid CAPTCHA codes via the login endpoint and use them

9.8 **CVE-2020-37239**

libbabl 0.1.62 contains a broken double free detection vulnerability that allows attackers to bypass memory safety checks by exploiting signature overwriting in freed chunks. Attackers can call babl_free() twice on the same pointer without triggering detection

9.8 **CVE-2021-47952**

python jsonpickle 2.0.0 contains a remote code execution vulnerability that allows attackers to execute arbitrary Python commands by deserializing malicious JSON payloads containing py/repr objects. Attackers can craft JSON strings with py/repr directives that

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.