Daily brief, Saturday, May 2, 2026

May 1, 8:00 PM to May 2, 8:00 PM ET

Generated Nov 7, 2026, 4:00 AM ET

0	0	0	2	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 new critical CVEs, 1 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-2026-4882**

The User Registration Advanced Fields plugin for WordPress is vulnerable to arbitrary file uploads due to missing file type validation in the 'URAF_AJAX::method_upload' function in all versions up to, and including, 1.6.20. This makes it possible for unauthent

9.8 **CVE-2026-7458**

The User Verification by PickPlugins plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 2.0.46. This is due to the use of a loose PHP comparison operator to validate OTP codes in the "user_verification_form_wrap_p

Ransomware

No leak-site posts collected.

New data breaches 1

ZenBusiness zenbusiness.com 5,118,184 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.