Daily brief, Sunday, May 17, 2026

May 16, 8:00 PM to May 17, 8:00 PM ET

Generated Nov 7, 2026, 12:56 AM 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-2026-8507** JONASBN Crypt::OpenSSL::PKCS12

Crypt::OpenSSL::PKCS12 versions through 1.94 for Perl have out-of-bounds (OOB) write flaws. When parsing a PKCS12 file, with a >= 1 GiB OCTET STRING (or BIT STRING) attribute on a SAFEBAG, via info() or info_as_hash(), a heap out-of-bounds write would be trigg

9.8 **CVE-2018-25320**

ACL Analytics versions 11.x through 13.0.0.579 contain an arbitrary code execution vulnerability that allows attackers to execute arbitrary commands by leveraging the EXECUTE function. Attackers can use bitsadmin to download malicious PowerShell scripts and ex

9.8 **CVE-2018-25332** Gitbucket gitbucket

GitBucket 4.23.1 contains an unauthenticated remote code execution vulnerability that allows attackers to execute arbitrary commands by exploiting weak secret token generation and insecure file upload functionality. Attackers can brute-force the Blowfish encry

9.8 **CVE-2018-25335**

WordPress Plugin Peugeot Music 1.0 contains an arbitrary file upload vulnerability that allows unauthenticated attackers to upload malicious files by sending POST requests to the upload.php endpoint. Attackers can upload files with arbitrary extensions by mani

9.8 **CVE-2026-8721**

Crypt::OpenSSL::PKCS12 versions through 1.94 for Perl truncates passwords with embedded NULLs. Password parameters in PKCS12.xs are declared char *, which routes through Perl's default typemap to SvPV_nolen. The Perl length is discarded. The C code (or OpenSSL

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.