

Daily brief, Friday, October 16, 2026

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

Generated Oct 30, 2026, 1:56 AM ET

0

Breaking

2

Newly exploited

0

Exploit code

6

Critical CVEs

0

Ransomware posts

0

New breaches

2 newly exploited, 6 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

9.3

CVE-2026-102764 BeyondTrust Remote Support CISA KEV

A remote attacker can perform file operations on the BeyondTrust Remote Support appliance.

5.4

CVE-2025-61624 Fortinet Multiple Products CISA KEV

An attacker gains ability to read and write arbitrary files on Fortinet FortiGate, FortiWeb, and FortiAnalyzer appliances.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

6

9.3

CVE-2026-102764 BeyondTrust Remote Support KEV

A remote attacker can perform file operations on the BeyondTrust Remote Support appliance.

9.8

CVE-2026-89079 Jfarthing84 Theme My Login EXPLOIT CODE DETECTION

The Theme My Login plugin for WordPress is vulnerable to privilege escalation via account takeover in versions up to, and including, 7.2.1. This is due to the plugin not properly validating a user's identity prior to updating their password. This makes it poss

9.8

CVE-2026-109219 Kitae-Park Mang Board

The Mang Board plugin for WordPress is vulnerable to Arbitrary File Upload in version 2.4.4 via the mbw_file_upload function. This is due to missing file extension validation on the attacker-supplied image_path parameter, whose basename-derived file name bypas

9.8**CVE-2026-111643** L429609201 misaka danmu server

An attacker bypasses authentication to misaka danmu server with user interaction.

9.8**CVE-2026-111693** Databufflabs databuff

An attacker gains administrator access to databuff without authentication.

9.6**CVE-2026-57169** Finsys dockhand

An attacker can bypass authentication in Dockhand.

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.