Daily brief, Wednesday, January 7, 2026

Jan 6, 7:00 PM to Jan 7, 7:00 PM ET

Generated Nov 9, 2026, 12:33 AM ET

0	2	0	16	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 16 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

2

10.0 **CVE-2025-37164** Hewlett Packard Enterprise (HPE) OneView CISA KEV DETECTION

Remote unauthenticated attacker can execute arbitrary code in Hewlett Packard Enterprise (HPE) OneView via code injection, requiring no authentication.

8.8 **CVE-2009-0556** Microsoft Office CISA KEV

Microsoft Office PowerPoint contains a code injection vulnerability that allows remote attackers to execute arbitrary code via a PowerPoint file with an OutlineTextRefAtom containing an invalid index value that triggers memory corruption.

New public exploit code

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

New critical CVEs

16

10.0 **CVE-2025-37164** Hewlett Packard Enterprise (HPE) OneView KEV EXPLOIT CODE DETECTION

Remote unauthenticated attacker can execute arbitrary code in Hewlett Packard Enterprise (HPE) OneView via code injection, requiring no authentication.

9.8 **CVE-2025-15471** Trendnet tew-713re firmware DETECTION

A vulnerability was detected in TRENDnet TEW-713RE 1.02. The impacted element is an unknown function of the file /goformX/formFSrvX. The manipulation of the argument SZCMD results in os command injection. It is possible to launch the attack remotely. The explo

9.8 **CVE-2025-68705** Rustfs rustfs

RustFS is a distributed object storage system built in Rust. In versions 1.0.0-alpha.13 to 1.0.0-alpha.78, RustFS contains a path traversal vulnerability in the /rustfs/rpc/read_file_stream endpoint. This issue has been patched in version 1.0.0-alpha.79.

9.1 **CVE-2025-69222** Librechat librechat

LibreChat is a ChatGPT clone with additional features. Version 0.8.1-rc2 is prone to a server-side request forgery (SSRF) vulnerability due to missing restrictions of the Actions feature in the default configuration. LibreChat enables users to configure agents

10.0 **CVE-2025-61492** Gongrzhe terminal-controller-mcp

A command injection vulnerability in the execute_command function of terminal-controller-mcp 0.1.7 allows attackers to execute arbitrary commands via a crafted input.

9.3 **CVE-2026-0650** OpenFlagr Flagr DETECTION

OpenFlagr versions prior to and including 1.1.18 contain an authentication bypass vulnerability in the HTTP middleware. Due to improper handling of path normalization in the whitelist logic, crafted requests can bypass authentication and access protected API e

9.6 **CVE-2025-12543** Redhat build of apache camel

A flaw was found in the Undertow HTTP server core, which is used in WildFly, JBoss EAP, and other Java applications. The Undertow library fails to properly validate the Host header in incoming HTTP requests.As a result, requests containing malformed or malicio

9.8 **CVE-2026-22189** Cmu panda3d

The egg-mkfont utility in Panda3D versions up to and including 1.10.16 contains a stack-based buffer overflow vulnerability due to use of an unbounded sprintf() call with attacker-controlled input. When constructing glyph filenames, egg-mkfont formats a user-s

9.8 **CVE-2026-21854** Tarkov tarkov data manager

The Tarkov Data Manager is a tool to manage the Tarkov item data. Prior to 02 January 2025, an authentication bypass vulnerability in the login endpoint allows any unauthenticated user to gain full admin access to the Tarkov Data Manager admin panel by exploit

9.8 **CVE-2025-47552**

Deserialization of Untrusted Data vulnerability in Digital zoom studio DZS Video Gallery allows Object Injection.This issue affects DZS Video Gallery: from n/a through 12.37.

9.2 **CVE-2026-22540**

The massive sending of ARP requests causes a denial of service on one board of the charger that allows control of the EV interfaces. Since the board must be operating correctly for the charger to also function correctly.

9.2 **CVE-2026-22542**

An attacker with access to the system's internal network can cause a denial of service on the system by making two concurrent connections through the Telnet service.

9.8 **CVE-2025-15018**

The Optional Email plugin for WordPress is vulnerable to Privilege Escalation via Account Takeover in all versions up to, and including, 1.3.11. This is due to the plugin not restricting its 'random_password' filter to registration contexts, allowing the filte

9.3 **CVE-2025-32303**

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Mojoomla WPCHURCH allows Blind SQL Injection.This issue affects WPCHURCH: from n/a through 2.7.0.

9.1 **CVE-2025-68637** Apache uniffle

The Uniffle HTTP client is configured to trust all SSL certificates and disables hostname verification by default. This insecure configuration exposes all REST API communication between the Uniffle CLI/client and the Uniffle Coordinator service to potential Ma

9.3 **CVE-2026-21855** Tarkov tarkov data manager

The Tarkov Data Manager is a tool to manage the Tarkov item data. Prior to 02 January 2025, a reflected Cross Site Scripting (XSS) vulnerability in the toast notification system allows any attacker to execute arbitrary JavaScript in the context of a victim's b

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.