Daily brief, Wednesday, December 3, 2025

Dec 2, 7:00 PM to Dec 3, 7:00 PM ET

Generated Nov 9, 2026, 6:12 AM ET

0	1	0	12	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 12 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

8.8 **CVE-2021-26828** OpenPLC ScadaBR CISA KEV DETECTION

Authenticated remote users of OpenPLC ScadaBR can upload and execute arbitrary JSP files through view_edit.shtm, giving code execution on the server.

New public exploit code

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

New critical CVEs

12

9.6 **CVE-2025-64443** Docker mcp gateway

MCP Gateway allows easy and secure running and deployment of MCP servers. In versions 0.27.0 and earlier, when MCP Gateway runs in sse or streaming transport mode, it is vulnerable to DNS rebinding. An attacker who can get a victim to visit a malicious website

9.8 **CVE-2025-13486** DETECTION

The Advanced Custom Fields: Extended plugin for WordPress is vulnerable to Remote Code Execution in versions 0.9.0.5 through 0.9.1.1 via the prepare_form() function. This is due to the function accepting user input and then passing that through call_user_func_

9.8 **CVE-2024-32641** Masacms masacms DETECTION

Masa CMS is an open source Enterprise Content Management platform. Masa CMS versions prior to 7.2.8, 7.3.13, and 7.4.6 are vulnerable to remote code execution. The vulnerability exists in the addParam function, which accepts user input via the criteria paramet

10.0 **CVE-2025-13390** Wpdirectorykit wp directory kit DETECTION

The WP Directory Kit plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 1.4.4 due to incorrect implementation of the authentication algorithm in the "wdk_generate_auto_login_link" function. This is due to the feat

9.3 **CVE-2025-34319**

TOTOLINK N300RT wireless router firmware versions prior to V3.4.0-B20250430 (discovered in V2.1.8-B20201030.1539) contain an OS command injection vulnerability in the Boa formWsc handling functionality. An unauthenticated attacker can send specially crafted re

9.8 **CVE-2025-13342** DETECTION

The Frontend Admin by DynamiApps plugin for WordPress is vulnerable to unauthorized modification of arbitrary WordPress options in all versions up to, and including, 3.28.20. This is due to insufficient capability checks and input validation in the ActionOptio

9.8 **CVE-2025-66208** Collabora collabora online - built-in code server

Collabora Online - Built-in CODE Server (richdocumentscode) provides a built-in server with all of the document editing features of Collabora Online. In versions prior to 25.04.702, Collabora Online has a Configuration-Dependent RCE (OS Command Injection) in r

9.8 **CVE-2025-66489** Cal cal.com

Cal.com is open-source scheduling software. Prior to 5.9.8, A flaw in the login credentials provider allows an attacker to bypass password verification when a TOTP code is provided, potentially gaining unauthorized access to user accounts. This issue exists du

9.8 **CVE-2025-66032** Anthropic claude code

Claude Code is an agentic coding tool. Prior to 1.0.93, Due to errors in parsing shell commands related to $IFS and short CLI flags, it was possible to bypass the Claude Code read-only validation and trigger arbitrary code execution. Reliably exploiting this r

9.6 **CVE-2025-66222** Thinkinai deepchat

DeepChat is a smart assistant uses artificial intelligence. In 0.5.0 and earlier, there is a Stored Cross-Site Scripting (XSS) vulnerability in the Mermaid diagram renderer allows an attacker to execute arbitrary JavaScript within the application context. By l

9.8 **CVE-2025-64055** Fanvil x210 firmware

An issue was discovered in Fanvil x210 V2 2.12.20 allowing unauthenticated attackers on the local network to access administrative functions of the device (e.g. file upload, firmware update, reboot...) via a crafted authentication bypass.

9.0 **CVE-2025-65267** Frappe erpnext

In ERPNext v15.83.2 and Frappe Framework v15.86.0, improper validation of uploaded SVG avatar images allows attackers to embed malicious JavaScript. The payload executes when an administrator clicks the image link to view the avatar, resulting in stored cross-

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.