Daily brief, Friday, December 5, 2025

Dec 4, 7:00 PM to Dec 5, 7:00 PM ET

Generated Nov 9, 2026, 5:54 AM ET

0	1	0	8	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 8 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

10.0 **CVE-2025-55182** Meta React Server Components CISA KEV DETECTION

Meta React Server Components flaw lets an attacker execute arbitrary code on the server.

New public exploit code

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

New critical CVEs

8

10.0 **CVE-2025-55182** Meta React Server Components KEV EXPLOIT CODE DETECTION

Meta React Server Components flaw lets an attacker execute arbitrary code on the server.

9.3 **CVE-2020-36877**

ReQuest Serious Play F3 Media Server 7.0.3 contains an unauthenticated remote code execution vulnerability that allows attackers to execute arbitrary commands as the web server user. Attackers can upload PHP executable files via the Quick File Uploader page, r

9.8 **CVE-2025-34256** Advantech wise-deviceon server

Advantech WISE-DeviceOn Server versions prior to 5.4 contain a hard-coded cryptographic key vulnerability. The product uses a static HS512 HMAC secret for signing EIRMMToken JWTs across all installations. The server accepts forged JWTs that need only contain a

9.8 **CVE-2025-13313**

The CRM Memberships plugin for WordPress is vulnerable to privilege escalation via password reset in all versions up to, and including, 2.6. This is due to missing authorization and authentication checks on the `ntzcrm_changepassword` AJAX action. This makes i

9.6 **CVE-2025-66562** Aiql tuui

TUUI is a desktop MCP client designed as a tool unitary utility integration. Prior to 1.3.4, a critical Remote Code Execution (RCE) vulnerability exists in Tuui due to an unsafe Cross-Site Scripting (XSS) flaw in the Markdown rendering component. Tuui allows t

9.8 **CVE-2025-12374**

The Email Verification, Email OTP, Block Spam Email, Passwordless login, Hide Login, Magic Login – User Verification plugin for WordPress is vulnerable to authentication bypass in all versions up to, and including, 2.0.44. This is due to the plugin not properl

9.6 **CVE-2025-64054** Fanvil x210 firmware

A reflected Cross Site Scripting (XSS) vulnerability on Fanvil x210 2.12.20 devices allows attackers to cause a denial of service or potentially execute arbitrary commands via crafted POST request to the /cgi-bin/webconfig?page=upload&action=submit endpoint.

10.0 **CVE-2025-66570** Yhirose cpp-httplib

cpp-httplib is a C++11 single-file header-only cross platform HTTP/HTTPS library. Prior to 0.27.0, a vulnerability allows attacker-controlled HTTP headers to influence server-visible metadata, logging, and authorization decisions. An attacker can inject header

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.