Daily brief, Monday, December 29, 2025

Dec 28, 7:00 PM to Dec 29, 7:00 PM ET

Generated Nov 9, 2026, 2:08 AM ET

0	1	0	15	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 15 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

7.5 **CVE-2025-14847** MongoDB MongoDB and MongoDB Server CISA KEV DETECTION

MongoDB Server contains an improper handling of length parameter inconsistency vulnerability in Zlib compressed protocol headers. This vulnerability may allow a read of uninitialized heap memory by an unauthenticated client.

New public exploit code

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

New critical CVEs

15

9.8 **CVE-2025-68706** Kuwfi ac900 firmware

A stack-based buffer overflow exists in the GoAhead-Webs HTTP daemon on KuWFi 4G LTE AC900 devices with firmware 1.0.13. The /goform/formMultiApnSetting handler uses sprintf() to copy the user-supplied pincode parameter into a fixed 132-byte stack buffer with

9.8 **CVE-2025-15194** Dlink dir-600 firmware

A vulnerability was found in D-Link DIR-600 up to 2.15WWb02. Affected by this vulnerability is an unknown functionality of the file hedwig.cgi of the component HTTP Header Handler. The manipulation of the argument Cookie results in stack-based buffer overflow.

9.8 **CVE-2025-15226** Sun.Net wmpro

WMPro developed by Sunnet has a Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.

9.8 **CVE-2025-15228** Welltend bpmflowwebkit

BPMFlowWebkit developed by WELLTEND TECHNOLOGY has a Arbitrary File Upload vulnerability, allowing unauthenticated remote attackers to upload and execute web shell backdoors, thereby enabling arbitrary code execution on the server.

9.8 **CVE-2025-68860**

Authentication Bypass Using an Alternate Path or Channel vulnerability in Mobile Builder Mobile builder mobile-builder allows Authentication Abuse.This issue affects Mobile builder: from n/a through <= 1.4.2.

9.8 **CVE-2025-65570** Jsish jsish

A type confusion in jsish 2.0 allows incorrect control flow during execution of the OP_NEXT opcode. When an “instanceof” expression uses an array element access as the left-hand operand inside a for-in loop, the instructions implementation leaves an additional

9.8 **CVE-2025-56333** Pangolin pangolin

An issue in Fossorial fosrl/pangolin v.1.6.2 and before allows a remote attacker to escalate privileges via the 2FA component

9.0 **CVE-2025-68929** Frappe frappe

Frappe is a full-stack web application framework. Prior to versions 14.99.6 and 15.88.1, an authenticated user with specific permissions could be tricked into accessing a specially crafted link. This could lead to a malicious template being executed on the ser

9.8 **CVE-2025-69201** Quenary tugtainer

Tugtainer is a self-hosted app for automating updates of docker containers. In versions prior to 1.15.1, arbitary arguments can be injected in tugtainer-agent `POST api/command/run`. Version 1.15.1 fixes the issue.

9.8 **CVE-2025-57460** Machsol machpanel

File upload vulnerability in machsol machpanel 8.0.32 allows attacker to gain a webshell.

9.9 **CVE-2025-68562**

Unrestricted Upload of File with Dangerous Type vulnerability in RomanCode MapSVG allows Upload a Web Shell to a Web Server.This issue affects MapSVG: from n/a through 8.7.3.

9.8 **CVE-2024-25182** Vvveb vvvebjs

givanz VvvebJs 1.7.2 suffers from a File Upload vulnerability via save.php.

9.8 **CVE-2024-27480** Vvveb vvvebjs

givanz VvvebJs 1.7.2 is vulnerable to Insecure File Upload.

9.9 **CVE-2025-68897**

Improper Control of Generation of Code ('Code Injection') vulnerability in Mohammad I. Okfie IF AS Shortcode if-as-shortcode allows Code Injection.This issue affects IF AS Shortcode: from n/a through <= 1.2.

9.1 **CVE-2024-25181** Vvveb vvvebjs

A critical vulnerability has been identified in givanz VvvebJs 1.7.2, which allows both Server-Side Request Forgery (SSRF) and arbitrary file reading. The vulnerability stems from improper handling of user-supplied URLs in the "file_get_contents" function with

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.