Scottish Cyber Coordination Centre

Daily Threat Bulletin

18 November 2025

Vulnerabilities

Google Issues Security Fix for Actively Exploited Chrome V8 Zero-Day Vulnerability

The Hacker News - 18 November 2025 11:14

The vulnerability in question is CVE-2025-13223 (CVSS score: 8.8), a type confusion vulnerability in the V8 JavaScript and WebAssembly engine that could be exploited to achieve arbitrary code execution or program crashes.

Microsoft: Windows bug blocks Microsoft 365 desktop app installs

BleepingComputer - 17 November 2025 10:54

Microsoft is working to resolve a known issue preventing users from installing the Microsoft 365 desktop apps on Windows devices.

Threat actors and malware

RondoDox botnet malware now hacks servers using XWiki flaw

BleepingComputer - 17 November 2025 18:41

The RondoDox botnet malware is now exploiting a critical remote code execution (RCE) flaw in XWiki Platform tracked as CVE-2025-24893.

Microsoft: Azure hit by 15 Tbps DDoS attack using 500,000 IP addresses

BleepingComputer - 17 November 2025 13:13

Microsoft said today that the Aisuru botnet hit its Azure network with a 15.72 terabits per second (Tbps) DDoS attack, launched from over 500,000 IP addresses.

New EVALUSION ClickFix Campaign Delivers Amatera Stealer and NetSupport RAT

The Hacker News - 17 November 2025 23:23

Cybersecurity researchers have discovered malware campaigns using the now-prevalent ClickFix social engineering tactic to deploy Amatera Stealer and NetSupport RAT.

Kraken Uses Benchmarking to Enhance Ransomware Attacks

Infosecurity Magazine - 17 November 2025 17:45

Cisco Talos has observed overlaps between Kraken and the earlier HelloKitty cartel through attack tactics using SMB flaws for big-game hunting and double extortion.