Scottish Cyber Coordination Centre

Daily Threat Bulletin

16 January 2026

Vulnerabilities

Cisco Patches Zero-Day RCE Exploited by China-Linked APT in Secure Email Gateways

The Hacker News - 16 January 2026 12:08

Cisco on Thursday released security updates for a maximum-severity security flaw impacting Cisco AsyncOS Software for Cisco Secure Email Gateway and Cisco Secure Email and Web Manager, nearly a month after the company disclosed that it had been exploited as a zero-day by a China-nexus advanced persistent threat (APT) actor codenamed UAT-9686.

Hackers exploit Modular DS WordPress plugin flaw for admin access

BleepingComputer - 15 January 2026 16:49

Hackers are actively exploiting a maximum severity flaw in the Modular DS WordPress plugin that allows them to bypass authentication remotely and access the vulnerable sites with admin-level privileges.

Palo Alto Networks addressed a GlobalProtect flaw, PoC exists

Security Affairs - 15 January 2026 12:26

Palo Alto Networks addressed a high-severity vulnerability, tracked as CVE-2026-0227 (CVSS score: 7.7), affecting GlobalProtect Gateway and Portal, for which a proof-of-concept (PoC) exploit exists.

Critical WhisperPair flaw lets hackers track, eavesdrop via Bluetooth audio devices

BleepingComputer - 15 January 2026 12:13

A critical vulnerability in Google's Fast Pair protocol can allow attackers to hijack Bluetooth audio accessories like wireless headphones and earbuds, track users, and eavesdrop on their conversations.

CodeBuild Flaw Put AWS Console Supply Chain At Risk

Infosecurity Magazine - 15 January 2026 16:00

A critical AWS CodeBuild misconfiguration has exposed core repositories to potential attack

Scottish Cyber Coordination Centre

Threat actors and malware

Researchers Reveal Reprompt Attack Allowing Single-Click Data Exfiltration From Microsoft Copilot

The Hacker News - 15 January 2026 21:39

Cybersecurity researchers have disclosed details of a new attack method dubbed Reprompt that could allow bad actors to exfiltrate sensitive data from artificial intelligence (AI) chatbots like Microsoft Copilot in a single click, while bypassing enterprise security controls entirely.

New 'StackWarp' Attack Threatens Confidential VMs on AMD Processors

SecurityWeek - 15 January 2026 19:00

Researchers have disclosed technical details on a new AMD processor attack that allows remote code execution inside confidential VMs.

Hackers Increasingly Shun Encryption in Favour of Pure Data Theft and Extortion

Infosecurity Magazine - 15 January 2026 16:45

While 'traditional' ransomware attacks remain stable, some gangs are shifting towards exploiting zero-days and supply chains to go straight to stealing data

UK incidents

Microsoft taps UK courts to dismantle cybercrime host RedVDS

The Register - 15 January 2026 12:32

Redmond says cheap virtual desktops powered a global wave of phishing and fraud Microsoft has taken its cybercrime fight to the UK in its first major civil action outside the US, moving to shut down RedVDS, a virtual desktop service used to power phishing and fraud at global scale.