Scottish Cyber Coordination Centre

Daily Threat Bulletin

18 December 2025

Vulnerabilities

Cisco warns of unpatched AsyncOS zero-day exploited in attacks

BleepingComputer - 17 December 2025 14:45

Cisco warned customers today of an unpatched, maximum-severity Cisco AsyncOS zero-day actively exploited in attacks targeting Secure Email Gateway (SEG) and Secure Email and Web Manager (SEWM) appliances.

SonicWall warns of actively exploited flaw in SMA 100 AMC

Security Affairs - 17 December 2025 20:36

SonicWall urged customers to address a vulnerability, tracked as CVE-2025-40602, in the SMA1000 Appliance Management Console that was exploited as a zero-day in attacks in the wild.

Critical Fortinet Flaws Under Active Attack

darkreading - 17 December 2025 23:44

Attackers targeted admin accounts, and once authenticated, exported device configurations including hashed credentials and other sensitive information.

Motors WordPress Vulnerability Exposes Sites to Takeover

Infosecurity Magazine - 17 December 2025 17:45

A critical flaw in the Motors WordPress theme affecting more than 20,000 installations allows low-privileged users to gain full control of websites

Two Chrome flaws could be triggered by simply browsing the web: Update now

Malwarebytes - 17 December 2025 17:02

Google's patched two flaws in Chrome, both of which can be triggered remotely when a user loads specially crafted web content.

Threat actors and malware

WhatsApp device linking abused in account hijacking attacks

BleepingComputer - 17 December 2025 15:14

Threat actors are abusing the legitimate device-linking feature to hijack WhatsApp accounts via pairing codes in a campaign dubbed GhostPairing.

Scottish Cyber Coordination Centre

Kimwolf Botnet Hijacks 1.8 Million Android TVs, Launches Large-Scale DDoS Attacks

The Hacker News - 18 December 2025 00:39

A new distributed denial-of-service (DDoS) botnet known as Kimwolf has enlisted a massive army of no less than 1.8 million infected devices comprising Android-based TVs, set-top boxes, and tablets, and may be associated with another botnet known as AISURU.

GhostPoster Firefox Extensions Hide Malware in Icons

SecurityWeek - 17 December 2025 11:40

The malware hijacks purchase commissions, tracks users, removes security headers, injects hidden iframes, and bypasses CAPTCHA.

Chinese Ink Dragon Group Hides in European Government Networks

Infosecurity Magazine - 17 December 2025 10:30

China’s Ink Dragon is using European government networks to hide its espionage activity