



Daily Threat Bulletin

19 December 2025

Vulnerabilities

[HPE warns of maximum severity RCE flaw in OneView software](#)

BleepingComputer - 18 December 2025 07:35

Hewlett Packard Enterprise (HPE) has patched a maximum-severity vulnerability in its HPE OneView software that enables attackers to execute arbitrary code remotely.

[Cisco Warns of Active Attacks Exploiting Unpatched 0-Day in AsyncOS Email Security Appliances](#)

The Hacker News - 18 December 2025 10:40

Cisco has alerted users to a maximum-severity zero-day flaw in Cisco AsyncOS software that has been actively exploited by a China-nexus advanced persistent threat (APT) actor codenamed UAT-9686 in attacks targeting Cisco Secure Email Gateway and Cisco Secure Email and Web Manager.

[CISA Warns of Exploited Flaw in Asus Update Tool](#)

SecurityWeek - 18 December 2025 14:27

Tracked as CVE-2025-59374, the issue is a software backdoor implanted in Asus Live Update in a supply chain attack.

[UEFI Vulnerability in Major Motherboards Enables Early-Boot Attacks](#)

SecurityWeek - 18 December 2025 16:30

ASRock, Asus, Gigabyte, and MSI motherboards are vulnerable to early-boot DMA attacks.

Threat actors and malware

[New password spraying attacks target Cisco, PAN VPN gateways](#)

BleepingComputer - 18 December 2025 13:27

An automated campaign is targeting multiple VPN platforms, with credential-based attacks being observed on Palo Alto Networks GlobalProtect and Cisco SSL VPN.

[Kimsuky Spreads DocSwap Android Malware via QR Phishing Posing as Delivery App](#)

The Hacker News - 18 December 2025 14:13

The North Korean threat actor known as Kimsuky has been linked to a new campaign that distributes a new variant of Android malware called DocSwap via QR codes hosted on phishing sites.



Scottish
Cyber
Coordination
Centre

GhostPairing campaign abuses WhatsApp device linking to hijack accounts

Security Affairs - 18 December 2025 09:47

Attackers are exploiting WhatsApp's device-linking feature to hijack accounts using pairing codes in a campaign dubbed GhostPairing, without requiring authentication.

Clop ransomware targets Gladinet CentreStack in data theft attacks

BleepingComputer - 18 December 2025 16:16

The Clop ransomware gang is targeting Internet-exposed Gladinet CentreStack file servers in a new data theft extortion campaign.

Amazon blocked 1,800 suspected North Korean scammers seeking jobs

The Register - 19 December 2025 00:39

Even Amazon isn't immune to North Korean scammers who try to score remote jobs at tech companies so they can funnel their wages to Kim Jong Un's coffers.

UK incidents

NHS tech supplier probes cyberattack on internal systems

The Register - 18 December 2025 14:02

An NHS tech supplier is investigating a cyberattack that affected its systems in the early hours of Sunday, around 2,000 GP practices use its products.