Scottish Cyber Coordination Centre

Daily Threat Bulletin

19 January 2026

Vulnerabilities

Microsoft releases OOB Windows updates to fix shutdown, Cloud PC bugs

BleepingComputer - 18 January 2026 14:16

Microsoft has released multiple emergency, out-of-band updates for Windows 10, Windows 11, and Windows Server to fix two issues caused by the January Patch Tuesday updates. [...]

Actively exploited critical flaw in Modular DS WordPress plugin enables admin takeover

Security Affairs - 16 January 2026 09:26

A critical Modular DS WordPress flaw (CVE-2026-23550) is actively exploited, enabling unauthenticated privilege escalation. Threat actors are actively exploiting a critical Modular DS WordPress vulnerability tracked as CVE-2026-23550 (CVSS score of 10).

Security Bug in StealC Malware Panel Let Researchers Spy on Threat Actor Operations

The Hacker News - 19 January 2026 13:23

Cybersecurity researchers have disclosed a cross-site scripting (XSS) vulnerability in the web-based control panel used by operators of the StealC information stealer, allowing them to gather crucial insights on one of the threat actors using the malware in their operations.

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.

RondoDox Botnet Targets HPE OneView Vulnerability in Exploitation Wave

Infosecurity Magazine - 16 January 2026 10:15

Check Point Research has reported a surge in attacks on a vulnerability in HPE OneView, driven by the Linux-based RondoDox botnet

Threat actors and malware

Credential-stealing Chrome extensions target enterprise HR platforms

BleepingComputer - 17 January 2026 12:19

Malicious Chrome extensions on the Chrome Web Store masquerading as productivity and security tools for enterprise HR and ERP platforms were discovered stealing authentication credentials or blocking management pages used to respond to security incidents. [...]

China-linked hackers exploited Sitecore zero-day for initial access

BleepingComputer - 16 January 2026 13:10

An advanced threat actor tracked as UAT-8837 and believed to be linked to China has been focusing on critical infrastructure systems in North America, gaining access by exploiting both known and zero-day vulnerabilities. [...]

China-linked APT UAT-9686 abused now patched maximum severity AsyncOS bug

Security Affairs - 16 January 2026 11:17

Cisco fixed a maximum severity AsyncOS flaw in Secure Email products, previously exploited as a zero-day by China-linked APT group UAT-9686. Cisco fixed a critical AsyncOS flaw, tracked as CVE-2025-20393 (CVSS score of 10.0), affecting Secure Email Gateway and Email and Web Manager, previously exploited as a zero-day by China-linked APT group UAT-9686. Cisco detected attacks [...]

Black Basta Ransomware Leader Added to EU Most Wanted and INTERPOL Red Notice

The Hacker News - 17 January 2026 22:56

Ukrainian and German law enforcement authorities have identified two Ukrainians suspected of working for the Russia-linked ransomware-as-a-service (RaaS) group Black Basta.In addition, the group's alleged leader, a 35-year-old Russian national named Oleg Evgenievich Nefedov (Нефедов Олег Евгеньевич), has been added to the European Union's Most Wanted and INTERPOL's Red Notice lists.