Scottish Cyber Coordination Centre

Daily threat bulletin

10 January 2025

Vulnerabilities

Ivanti zero-day attacks infected devices with custom malware

BleepingComputer - 09 January 2025 12:11

Hackers exploiting the critical Ivanti Connect Secure zero-day vulnerability disclosed yesterday installed on compromised VPN appliances new malware called 'Dryhook' and 'Phasejam' that is not currently associated with any threat group. [...]

GFI KerioControl Firewall Vulnerability Exploited in the Wild

SecurityWeek - 09 January 2025 13:58

Threat actors are exploiting a recent GFI KerioControl firewall vulnerability that leads to remote code execution.

Palo Alto Networks Patches High-Severity Vulnerability in Retired Migration Tool

SecurityWeek - 09 January 2025 12:53

Palo Alto Networks has released patches for multiple vulnerabilities in the Expedition migration tool, which was retired on December 31, 2024.

SonicWall Patches Authentication Bypass Vulnerabilities in Firewalls

SecurityWeek - 09 January 2025 13:40

SonicWall has released patches for multiple vulnerabilities in SonicOS, including high-severity authentication bypass flaws.

Microsoft fixes OneDrive bug causing macOS app freezes

BleepingComputer - 09 January 2025 14:29

Microsoft has fixed a known issue causing macOS applications to freeze when opening or saving files in OneDrive. [...]

Threat actors and malware

Banshee 2.0 Malware Steals Apple's Encryption to Hide on Macs

darkreading - 09 January 2025 23:47

The most recent iteration of the open source infostealer skates by antivirus programs on Macs, using an encryption mechanism stolen from Apple's own antivirus product.

Google Chrome AI extensions deliver info-stealing malware in broad attack

Scottish Cyber Coordination Centre

Malwarebytes - 09 January 2025 17:35

At least 36 Google Chrome extensions for AI and VPN tools have begun delivering info-stealing malware in a widespread attack.

Fake CrowdStrike job offer emails target devs with crypto miners

BleepingComputer - 09 January 2025 17:30

CrowdStrike is warning that a phishing campaign is impersonating the cybersecurity company in fake job offer emails to trick targets into infecting themselves with a Monero cryptocurrency miner (XMRig). [...]

Chinese-linked Hackers May Be Exploiting Latest Ivanti Vulnerability

Security Boulevard - 09 January 2025 21:41

Software maker Ivanti, which for more than a year has been plagued by security flaws in its appliance, unveiled two new ones this week, with Mandiant researchers saying that one likely is being activity exploited by China-linked threat groups.The post Chinese-linked Hackers May Be Exploiting Latest Ivanti Vulnerability appeared first on Security Boulevard.

Japan Faces Prolonged Cyber-Attacks Linked to China's MirrorFace

Infosecurity Magazine - 09 January 2025 17:30

Cyber-attacks by China-linked MirrorFace targeted Japan's national security information in major campaigns operating since 2019

UK related

Government Launches £1.9m Initiative to Boost UK's Cyber Resilience

Infosecurity Magazine - 09 January 2025 11:30

The UK government has pledged nearly £2m to 30 new Cyber Local projects designed to enhance cyber resilience