Scottish Cyber Coordination Centre

Daily threat bulletin

25 November 2024

Vulnerabilities

Experts warn of Palo Alto firewall exploitation after 2,000 compromises spotted

The Record from Recorded Future News - 22 November 2024 21:17

Windows 10 KB5046714 update fixes bug preventing app uninstalls

BleepingComputer - 22 November 2024 18:32

Microsoft has released the optional KB5046714 Preview cumulative update for Windows 10 22H2 with six bug fixes, including a fix for a bug preventing users from uninstalling or updating packaged applications. [...]

QNAP pulls buggy QTS firmware causing widespread NAS issues

BleepingComputer - 22 November 2024 16:49

QNAP has pulled a recently released firmware update after widespread customer reports that it's breaking connectivity and, in some cases, locking users out of their devices. [...]

400,000 Systems Potentially Exposed to 2023's Most Exploited Flaws

SecurityWeek - 22 November 2024 12:00

VulnCheck finds hundreds of thousands of internet-accessible hosts potentially vulnerable to 2023's top frequently exploited flaws.

Threat actors and malware

Hackers abuse Avast anti-rootkit driver to disable defenses

BleepingComputer - 23 November 2024 11:07

A new malicious campaign is using a legitimate but old and vulnerable Avast Anti-Rootkit driver to evade detection and take control of the target system by disabling security components. [...]

Russian Cyber Spies Target Organizations with HatVibe and CherrySpy Malware

Infosecurity Magazine - 22 November 2024 14:00

Russian-aligned TAG-110 uses custom tools to spy on governments, human rights groups and educational institutions in Europe and Asia

Google Exposes GLASSBRIDGE: A Pro-China Influence Network of Fake News Sites

Scottish Cyber Coordination Centre

The Hacker News - 23 November 2024 18:40

Government agencies and non-governmental organizations in the United States have become the target of a nascent China state threat actor known as Storm-2077.The adversary, believed to be active since at least January 2024, has also conducted cyber attacks against the Defense Industrial Base (DIB), aviation, telecommunications, and financial and legal services across the world, Microsoft said.

Five Ransomware Groups Responsible for 40% of Cyber-Attacks in 2024

Infosecurity Magazine - 22 November 2024 11:45

Corvus Insurance highlighted the growing complexity and competition within the ransomware ecosystem, with the threat level remaining elevated

Manufacturing Sector in the Crosshairs of Advanced Email Attacks

Infosecurity Magazine - 22 November 2024 10:15

Phishing attacks, business email compromise and vendor email compromise attacks on manufacturing have surged in the past 12 months