Scottish
Cyber
Coordination
Centre

Daily threat bulletin

30 October 2024

Vulnerabilities

New Windows Themes zero-day gets free, unofficial patches

BleepingComputer - 29 October 2024 17:21

Free unofficial patches are now available for a new Windows Themes zero-day vulnerability that allows attackers to steal a target’s NTLM credentials remotely. [...]

Apple Patches Over 70 Vulnerabilities Across iOS, macOS, Other Products

SecurityWeek - 29 October 2024 10:30

Apple has released security updates for iOS 18 and macOS Sequoia 15 to address dozens of vulnerabilities.

QNAP fixes NAS backup software zero-day exploited at Pwn2Own

BleepingComputer - 29 October 2024 14:35

QNAP has fixed a critical zero-day vulnerability exploited by security researchers on Thursday to hack a TS-464 NAS device during the Pwn2Own Ireland 2024 competition. [...]

Fog and Akira ransomware attacks exploit SonicWall VPN flaw CVE-2024-40766

Security Affairs - 29 October 2024 12:51

Fog and Akira ransomware operators are exploiting SonicWall VPN flaw CVE-2024-40766 to breach enterprise networks. Fog and Akira ransomware operators are exploiting the critical SonicWall VPN vulnerability CVE-2024-40766 (CVSS v3 score: 9.3) to breach corporate networks via SSL VPN access. CVE-2024-40766 is an Improper Access Control Vulnerability impacting SonicWall SonicOS, the company addressed it in August [...]

Admins better Spring into action over latest critical open source vuln

The Register - 29 October 2024 15:33

Patch up: The Spring framework dominates the Java ecosystem If you’re running an application built using the Spring development framework, now is a good time to check it’s fully updated – a new, critical-severity vulnerability has just been disclosed.…

Threat actors and malware

Massive PSAUX ransomware attack targets 22,000 CyberPanel instances

BleepingComputer - 29 October 2024 16:15

Over 22,000 CyberPanel instances exposed online to a critical remote code execution (RCE) vulnerability were mass-targeted in a PSAUX ransomware attack that took almost all instances offline. [...]

New LightSpy Spyware Targets iOS with Enhanced Capabilities

Infosecurity Magazine - 29 October 2024 18:15

ThreatFabric researchers have discovered significant updates to the LightSpy spyware, featuring plugins designed to interfere with device functionality

China's 'Evasive Panda' APT Debuts High-End Cloud Hijacking

darkreading - 29 October 2024 22:05

A professional-grade tool set, appropriately dubbed "CloudScout," is infiltrating cloud apps like Microsoft Outlook and Google Drive, targeting sensitive info for exfiltration.

Russia's 'Midnight Blizzard' hackers target government workers in novel info-stealing campaign

The Record from Recorded Future News - 30 October 2024 02:25

Chenlun's Evolving Phishing Tactics Target Trusted Brands

Infosecurity Magazine - 29 October 2024 17:30

The phishing campaign targeted users via texts impersonating Amazon, linked to the threat actor Chenlun

31 new ransomware groups were discovered in 2024

Security Magazine - 29 October 2024 09:00

A report by Secureworks revealed a 30% year-over-year rise in active ransomware groups, which demonstrates fragmentation of an established criminal ecosystem.