Scottish Cyber Coordination Centre

Daily threat bulletin

16 December 2024

Vulnerabilities

Cleo MFT Zero-Day Exploits Are About Escalate, Analysts Warn

darkreading - 13 December 2024 22:56

Defenders running the Cleo managed file transfer are urged to be on the lookout for the Cleopatra backdoor and other indicators of an ongoing ransomware campaign, as patching details remain foggy, and no CVE has been issued.

Critical OpenWrt Vulnerability Exposes Devices to Malicious Firmware Injection

The Hacker News - 13 December 2024 23:18

A security flaw has been disclosed in OpenWrt's Attended Sysupgrade (ASU) feature that, if successfully exploited, could have been abused to distribute malicious firmware packages.The vulnerability, tracked as CVE-2024-54143, carries a CVSS score of 9.3 out of a maximum of 10, indicating critical severity.

Microsoft Patches Vulnerabilities in Windows Defender, Update Catalog

SecurityWeek - 13 December 2024 12:40

Microsoft has patched potentially critical vulnerabilities in Update Catalog and Windows Defender on the server side.

Critical Vulnerabilities Found in Ruijie Reyee Cloud Management Platform

SecurityWeek - 13 December 2024 16:46

Researchers warn about critical vulnerabilities in Ruijie Networks' Reyee cloud management platform and Reyee OS network devices.

390,000+ WordPress Credentials Stolen via Malicious GitHub Repository Hosting PoC Exploits

The Hacker News - 14 December 2024 02:30

A now-removed GitHub repository that advertised a WordPress tool to publish posts to the online content management system (CMS) is estimated to have enabled the exfiltration of over 390,000 credentials.

Threat actors and malware

Researchers Discover Malware Used by Nation-Sates to Attack Industrial Systems

Infosecurity Magazine - 13 December 2024 12:15

IOCONTROL, a custom-built IoT/OT malware, was used by Iran-affiliated groups to attack Israel- and US-based OT/IoT devices, according to Claroty

Experts discovered the first mobile malware families linked to Russia's Gamaredon

Security Affairs - 13 December 2024 08:23

The Russia-linked APT Gamaredon used two new Android spyware tools called BoneSpy and PlainGnome against former Soviet states. Lookout researchers linked the BoneSpy and PlainGnome Android surveillance families to the Russian APT group Gamaredon (a.k.a. Armageddon, Primitive Bear, and ACTINIUM).

Citrix shares mitigations for ongoing Netscaler password spray attacks

BleepingComputer - 13 December 2024 18:10

Citrix Netscaler is the latest target in widespread password spray attacks targeting edge networking devices and cloud platforms this year to breach corporate networks. [...]

Winnti hackers target other threat actors with new Glutton PHP backdoor

BleepingComputer - 15 December 2024 11:19

The Chinese Winnti hacking group is using a new PHP backdoor named 'Glutton' in attacks on organizations in China and the U.S., and also in attacks on other cybercriminals. [...]

Akira and RansomHub Surge as Ransomware Claims Reach All-Time High

Infosecurity Magazine - 13 December 2024 14:00

Claims on ransomware groups' data leak sites reached an all-time high in November, with 632 reported victims, according to Corvus Insurance