Scottish Cyber Coordination Centre

Daily threat bulletin

13 December 2024

Vulnerabilities

Cleo patches critical zero-day exploited in data theft attacks

BleepingComputer - 12 December 2024 13:03

Cleo has released security updates for a zero-day flaw in its LexiCom, VLTransfer, and Harmony software, currently exploited in data theft attacks. [...]

Researchers Uncover Symlink Exploit Allowing TCC Bypass in iOS and macOS

The Hacker News - 12 December 2024 19:05

Details have emerged about a now-patched security vulnerability in Apple's iOS and macOS that, if successfully exploited, could sidestep the Transparency, Consent, and Control (TCC) framework and result in unauthorized access to sensitive information. The flaw, tracked as CVE-2024-44131 (CVSS score: 5.3), resides in the FileProvider component.

Apache issues patches for critical Struts 2 RCE bug

The Register - 12 December 2024 14:31

More details released after devs allowed weeks to apply fixes We now know the remote code execution vulnerability in Apache Struts 2 disclosed back in November carries a near-maximum severity rating following the publication of the CVE....

Update now! Apple releases new security patches for vulnerabilities in iPhones, Macs, and more

Malwarebytes - 12 December 2024 16:14

Apple has released security patches for most of its operating systems, including iOS, Mac, iPadOS, Safari, and visionOS.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-49138 Microsoft Windows Common Log File System (CLFS) Driver Heap-Based Buffer Overflow Vulnerability.

Threat actors and malware

New stealthy Pumakit Linux rootkit malware spotted in the wild

BleepingComputer - 12 December 2024 18:35

A new Linux rootkit malware called Pumakit has been discovered that uses stealth and advanced privilege escalation techniques to hide its presence on systems. [...]

New IOCONTROL malware used in critical infrastructure attacks

BleepingComputer - 12 December 2024 16:46

Iranian threat actors are utilizing a new malware named IOCONTROL to compromise Internet of Things (IoT) devices and OT/SCADA systems used by critical infrastructure in Israel and the United States. [...]

Remcos RAT Malware Evolves with New Techniques

Infosecurity Magazine - 12 December 2024 17:30

Cyber-attacks involving Remcos RAT surged in Q3 2024, enabling attackers to control victim machines remotely, steal data and carry out espionage

IoT Cloud Cracked by ‘Open Sesame’ Over-the-Air Attack

darkreading - 12 December 2024 21:47

Researchers demonstrate how to hack Ruijie Reyee access points without Wi-Fi credentials or even physical access to the device.