Scottish Cyber Coordination Centre

Daily threat bulletin

28 October 2024

Vulnerabilities

U.S. CISA adds Cisco ASA and FTD, and RoundCube Webmail bugs to its Known Exploited Vulnerabilities catalog

Security Affairs - 25 October 2024 08:40

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Cisco ASA and FTD, and RoundCube Webmail bugs to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the following vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog:

Researchers Uncover OS Downgrade Vulnerability Targeting Microsoft Windows Kernel

The Hacker News - 28 October 2024 11:59

A new attack technique could be used to bypass Microsoft's Driver Signature Enforcement (DSE) on fully patched Windows systems, leading to operating system (OS) downgrade attacks.

Researchers Discover Command Injection Flaw in Wi-Fi Alliance's Test Suite

The Hacker News - 25 October 2024 20:11

A security flaw impacting the Wi-Fi Test Suite could enable unauthenticated local attackers to execute arbitrary code with elevated privileges.The CERT Coordination Center (CERT/CC) said the vulnerability, tracked as CVE-2024-41992, said the susceptible code from the Wi-Fi Alliance has been found deployed on Arcadyan FMIMG51AX000J routers.

Apple Opens PCC Source Code for Researchers to Identify Bugs in Cloud AI Security

The Hacker News - 25 October 2024 18:55

Apple has publicly made available its Private Cloud Compute (PCC) Virtual Research Environment (VRE), allowing the research community to inspect and verify the privacy and security guarantees of its offering.

Threat actors and malware

Fog ransomware targets SonicWall VPNs to breach corporate networks

BleepingComputer - 27 October 2024 11:17

Fog and Akira ransomware operators have increased their exploitation efforts of CVE-2024-40766, a critical access control flaw that allows unauthorized access to resources on the SSL VPN feature of SonicWall SonicOS firewalls. [...]

Scottish Cyber Coordination Centre

AWS Seizes Domains Used by Russia's APT29

SecurityWeek - 25 October 2024 10:55

AWS announced the seizure of domains used by Russian hacker group APT29 in phishing attacks targeting Ukraine and other countries.

New Cisco ASA and FTD features block VPN brute-force password attacks

BleepingComputer - 26 October 2024 11:31

Cisco has added new security features that significantly mitigate brute-force and password spray attacks on Cisco ASA and Firepower Threat Defense (FTD), helping protect the network from breaches and reducing resource utilization on devices.

Black Basta ransomware poses as IT support on Microsoft Teams to breach networks

BleepingComputer - 25 October 2024 17:55

The BlackBasta ransomware operation has moved its social engineering attacks to Microsoft Teams, posing as corporate help desks contacting employees to assist them with an ongoing spam attack.

MacOS-Focused Ransomware Attempts Leverage LockBit Brand

Infosecurity Magazine - 25 October 2024 09:00

An unidentified threat actor has attempted to develop ransomware targeting macOS devices, posing as LockBit