Scottish Cyber Coordination Centre

Daily Threat Bulletin

25 February 2025

Vulnerabilities

Exploits for unpatched Parallels Desktop flaw give root on Macs

BleepingComputer - 24 February 2025 11:48

Two different exploits for an unpatched Parallels Desktop privilege elevation vulnerability have been publicly disclosed, allowing users to gain root access on impacted Mac devices. [...]

Two Actively Exploited Security Flaws in Adobe and Oracle Products Flagged by CISA

The Hacker News - 25 February 2025 10:40

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added two security flaws impacting Adobe ColdFusion and Oracle Agile Product Lifecycle Management (PLM) to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation. The vulnerabilities in question are listed below - CVE-2017-3066 (CVSS score: 9.8).

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2017-3066 Adobe ColdFusion Deserialization Vulnerability; CVE-2024-20953 Oracle Agile Product Lifecycle Management (PLM) Deserialization Vulnerability.

Threat actors and malware

OpenAI bans ChatGPT accounts used by North Korean hackers

BleepingComputer - 24 February 2025 17:35

OpenAI says it blocked several North Korean hacking groups from using its ChatGPT platform to research future targets and find ways to hack into their networks. [...]

A large botnet targets M365 accounts with password spraying attacks

Security Affairs - 24 February 2025 21:51

A botnet of 130,000+ devices is attacking Microsoft 365 accounts via password-spraying, bypassing MFA by exploiting basic authentication. SecurityScorecard researchers discovered a botnet of over 130,000 devices that is conducting password-spray attacks against Microsoft 365 (M365) accounts worldwide.

SpyLend Android malware found on Google Play enabled financial cyber crime and extortion

Scottish Cyber Coordination Centre

Security Affairs - 24 February 2025 09:57

CYFIRMA researchers discovered that the SpyLend Android malware was downloaded 100,000 times from the official app store Google Play. CYFIRMA researchers discovered an Android malware, named SpyLend, which was distributed through Google Play as Finance Simplified.

New Malware Campaign Uses Cracked Software to Spread Lumma and ACR Stealer

The Hacker News - 24 February 2025 23:28

Cybersecurity researchers are warning of a new campaign that leverages cracked versions of software as a lure to distribute information stealers like Lumma and ACR Stealer. The AhnLab Security Intelligence Center (ASEC) said it has observed a spike in the distribution volume of ACR Stealer since January 2025.