Scottish Cyber Coordination Centre

Daily Threat Bulletin

24 February 2025

Vulnerabilities

CISA flags Craft CMS code injection flaw as exploited in attacks

BleepingComputer - 21 February 2025 11:57

The U.S. Cybersecurity & Infrastructure Security Agency (CISA) warns that a Craft CMS remote code execution flaw is being exploited in attacks.

U.S. CISA adds Microsoft Power Pages flaw to its Known Exploited Vulnerabilities catalog

Security Affairs - 23 February 2025 16:07

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added a Microsoft Power Pages vulnerability, tracked as CVE-2025-24989 (CVSS score: 8.2), to its Known Exploited Vulnerabilities (KEV) catalog.

Threat actors and malware

Beware: PayPal “New Address” feature abused to send phishing emails

BleepingComputer - 22 February 2025 17:01

An ongoing PayPal email scam exploits the platform’s address settings to send fake purchase notifications, tricking users into granting remote access to scammers.

SpyLend Android malware downloaded 100,000 times from Google Play

BleepingComputer - 21 February 2025 14:45

An Android malware app called SpyLend has been downloaded over 100,000 times from Google Play, where it masqueraded as a financial tool but became a predatory loan app.

Cisco Confirms Salt Typhoon Exploited CVE-2018-0171 to Target U.S. Telecom Networks

The Hacker News - 21 February 2025 14:08

Cisco has confirmed that a Chinese threat actor known as Salt Typhoon gained access by likely abusing a known security flaw tracked as CVE-2018-0171, and by obtaining legitimate victim login credentials as part of a targeted campaign aimed at major U.S. telecommunications companies.

Scottish Cyber Coordination Centre

North Korea's Lazarus Group Hacks Bybit, Steals $1.5 Billion in Crypto

Security Boulevard - 22 February 2025 19:33

North Korea's notorious Lazarus Group reportedly stole $1.5 billion in cryptocurrency from the Bybit exchange in what is being called the largest hack in the controversial market's history.

BlackBasta Ransomware Chatlogs Leaked Online

Infosecurity Magazine - 21 February 2025 12:15

Netherlands-based threat intelligence firm Prodaft revealed on February 20 that internal chatlogs from the BlackBasta ransomware gang have been leaked online.

UK incidents

Apple Pulls Advanced Data Protection for New UK Users Amid Backdoor Demand

SecurityWeek - 21 February 2025 16:56

Apple has pulled its privacy-themed Advanced Data Protection (ADP) feature from new users in the United Kingdom, a move clearly linked to UK government demands for a backdoor into encrypted cloud storage.