Scottish Cyber Coordination Centre

Daily Threat Bulletin

18 March 2025

Vulnerabilities

Critical RCE flaw in Apache Tomcat actively exploited in attacks

BleepingComputer - 17 March 2025 10:29

A critical remote code execution (RCE) vulnerability in Apache Tomcat tracked as CVE-2025-24813 is actively exploited in the wild, enabling attackers to take over servers with a simple PUT request. [...]

Unpatched Edimax Camera Flaw Exploited for Mirai Botnet Attacks Since Last Year

The Hacker News - 17 March 2025 19:42

An unpatched security flaw impacting the Edimax IC-7100 network camera is being exploited by threat actors to deliver Mirat botnet malware variants since at least May 2024.The vulnerability in question is CVE-2025-1316 (CVSS v4 score: 9.3)

Cybercriminals Exploit CSS to Evade Spam Filters and Track Email Users' Actions

The Hacker News - 17 March 2025 18:22

Malicious actors are exploiting Cascading Style Sheets (CSS), which are used to style and format the layout of web pages, to bypass spam filters and track users' actions.That's according to new findings from Cisco Talos, which said such malicious activities can compromise a victim's security and privacy.

8,000 New WordPress Vulnerabilities Reported in 2024

SecurityWeek - 17 March 2025 17:01

Nearly 8,000 new vulnerabilities affecting the WordPress ecosystem were reported last year, nearly all in plugins and themes.

Nvidia Patches Vulnerabilities That Could Let Hackers Exploit AI Services

SecurityWeek - 17 March 2025 12:16

Vulnerabilities in Nvidia Riva could allow hackers to abuse speech and translation AI services that are typically expensive.

Threat actors and malware

OKX suspends DEX aggregator after Lazarus hackers try to launder funds

BleepingComputer - 17 March 2025 15:23

OKX Web3 has decided to suspend its DEX aggregator services to implement security upgrades following reports of abuse by the notorious North Korean Lazarus hackers, who recently conducted a $1.5 billion crypto heist. [...]

Supply chain attack on popular GitHub Action exposes CI/CD secrets

BleepingComputer - 17 March 2025 12:24

A supply chain attack on the widely used 'tj-actions/changed-files' GitHub Action, used by 23,000 repositories, potentially allowed threat actors to steal CI/CD secrets from GitHub Actions build logs. [...]

Microsoft Warns of StilachiRAT: A Stealthy RAT Targeting Credentials and Crypto Wallets

The Hacker News - 18 March 2025 13:30

Microsoft is calling attention to a novel remote access trojan (RAT) named StilachiRAT that it said employs advanced techniques to sidestep detection and persist within target environments with an ultimate aim to steal sensitive data.

How Economic Headwinds Influence the Ransomware Ecosystem

darkreading - 17 March 2025 13:54

Inflation, cryptocurrency market volatility, and the ability to invest in defenses all influence the impact and severity of a ransomware attack, according to incident response efforts and ransomware negotiators.

Microsoft 365 Targeted in New Phishing, Account Takeover Attacks

SecurityWeek - 17 March 2025 13:48

Threat actors are abusing Microsoft 365 infrastructure in a BEC campaign, and target its users in two brand impersonation campaigns.

UK related

UK NHS API Flaw Exposes Critical Mobile Security Risks

Security Boulevard - 18 March 2025 00:28

A recent vulnerability discovered in an UK National Health Service HS API has once again highlighted the risks associated with insecure mobile application programming interfaces (APIs). The flaw reportedly allowed unauthorized access to sensitive patient data, raising serious concerns about the security of healthcare applications.

UK government to open £16B IT services competition after 6-month delay

The Register - 17 March 2025 11:27

Technology Services 4 framework expands by £4B, with procurement to begin this week UK government is set to crack open the pork barrel for up to £16 billion in contracts for a range of

Scottish Cyber Coordination Centre

IT services. The buying framework was delayed by six months and the total pot of spending is now potentially 25 percent bigger than the previous proposal....