Scottish Cyber Coordination Centre

Daily Threat Bulletin

26 February 2025

Vulnerabilities

CISA Adds Microsoft and Zimbra Flaws to KEV Catalog Amid Active Exploitation

The Hacker News - 26 February 2025 11:03

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Tuesday placed two security flaws impacting Microsoft Partner Center and Synacor Zimbra Collaboration Suite (ZCS) to its Known Exploited Vulnerabilities (KEV) catalog, based on evidence of active exploitation.The vulnerabilities in question are as follows -CVE-2024-49035 (CVSS score: 8.7).

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).

Max Severity RCE Vuln in All Versions of MITRE Caldera

darkreading - 25 February 2025 22:42

In the wrong hands, the popular red-teaming tool can be made to access networks, escalate privileges, conduct reconnaissance, and disguise malicious activity as a simulated exercise.

Threat actors and malware

5 Active Malware Campaigns in Q1 2025

The Hacker News - 25 February 2025 17:30

The first quarter of 2025 has been a battlefield in the world of cybersecurity. Cybercriminals continued launching aggressive new campaigns and refining their attack methods.Below is an overview of five notable malware families, accompanied by analyses conducted in controlled environments.

Industrial System Cyberattacks Surge as OT Stays Vulnerable

darkreading - 25 February 2025 12:00

Nearly a third of organizations have an operational system connected to the Internet with a known exploited vulnerability, as attacks by state and non-state actors increase.

Southern Water takes the fifth over alleged $750K Black Basta ransom offer

The Register - 25 February 2025 10:30

Scottish Cyber Coordination Centre

Leaked chats and spilled secrets as AI helps decode circa 200K private talks Southern Water neither confirms nor denies offering Black Basta a $750,000 ransom payment following its ransomware attack in 2024.

Chinese Botnet Powered by 130,000 Devices Targets Microsoft 365 Accounts

SecurityWeek - 25 February 2025 18:10

A China-linked botnet powered by 130,000 hacked devices has targeted Microsoft 365 accounts with password spraying attacks.

Leader of North Korean Hackers Sanctioned by EU

SecurityWeek - 25 February 2025 14:45

The EU has announced new sanctions against entities aiding Russia's war against Ukraine, including an individual who leads North Korean hackers.