Scottish Cyber Coordination Centre

Daily threat bulletin

4 February 2025

Vulnerabilities

Google fixes Android kernel zero-day exploited in attacks

BleepingComputer - 03 February 2025 16:10

The February 2025 Android security updates patch 48 vulnerabilities, including a zero-day kernel vulnerability that has been exploited in the wild. [...]

Microsoft Patches Critical Azure AI Face Service Vulnerability with CVSS 9.9 Score

The Hacker News - 04 February 2025 11:38

Microsoft has released patches to address two Critical-rated security flaws impacting Azure AI Face Service and Microsoft Account that could allow a malicious actor to escalate their privileges under certain conditions.The flaws are listed below -CVE-2025-21396 (CVSS score: 7.5) - Microsoft Account Elevation of Privilege VulnerabilityCVE-2025-21415 (CVSS score: 9.9) - Azure AI Face Service

CISA Warns of Backdoor Vulnerability in Contec Patient Monitors

Infosecurity Magazine - 03 February 2025 18:15

CISA has identified a backdoor in Contec CMS8000 devices that could allow unauthorized access to patient data and disrupt monitoring functions

Microsoft SharePoint Connector Flaw Could've Enabled Credential Theft Across Power Platform

The Hacker News - 04 February 2025 10:59

Cybersecurity researchers have disclosed details of a now-patched vulnerability impacting the Microsoft SharePoint connector on Power Platform that, if successfully exploited, could allow threat actors to harvest a user's credentials and stage follow-on attacks.

Amazon Redshift gets new default settings to prevent data breaches

BleepingComputer - 03 February 2025 17:37

Amazon has announced key security enhancements for Redshift, a popular data warehousing solution, to help prevent data exposures due to misconfigurations and insecure default settings. [...]

768 CVEs Exploited in the Wild in 2024

Infosecurity Magazine - 03 February 2025 15:00

VulnCheck observed 768 public reports of CVEs exploited in the wild for the first time in 2024, a 20% rise compared to 2023

Scottish Cyber Coordination Centre

Threat actors and malware

Web Skimmer found on at least 17 websites, including Casio UK

Security Affairs - 03 February 2025 23:02

Casio Website Infected With Skimmer A threat actor has installed a web skimmer on all pages of the Casio UK's website, except the checkout page. Jscrambler researchers uncovered a web skimmer campaign targeting multiple websites, including Casio one (casio.co.uk).

Coyote Malware Expands Reach: Now Targets 1,030 Sites and 73 Financial Institutions

The Hacker News - 03 February 2025 18:09

Brazilian Windows users are the target of a campaign that delivers a banking malware known as Coyote."Once deployed, the Coyote Banking Trojan can carry out various malicious activities, including keylogging, capturing screenshots, and displaying phishing overlays to steal sensitive credentials,"

DeepSeek AI tools impersonated by infostealer malware on PyPI

BleepingComputer - 03 February 2025 12:33

Threat actors are taking advantage of the rise in popularity of the DeepSeek to promote two malicious infostealer packages on the Python Package Index (PyPI), where they impersonated developer tools for the AI platform. [...]

1-Click Phishing Campaign Targets High-Profile X Accounts

darkreading - 03 February 2025 16:45

In an attack vector that's been used before, threat actors aim to commit crypto fraud by hijacking highly followed users, thus reaching a broad audience of secondary victims.

DeepSeek Security: System Prompt Jailbreak, Details Emerge on Cyberattacks

SecurityWeek - 03 February 2025 13:03

Researchers found a jailbreak method that exposed DeepSeek's system prompt, while others have analyzed the DDoS attacks aimed at the new gen-AI.

Ransomware Groups Weathered Raids, Profited in 2024

darkreading - 03 February 2025 22:20

Cybercriminals posted nearly 6,000 breaches to data-leak sites last year — and despite significant takedowns, they continued to thrive in a record-breaking year for ransomware.

UK related

UK Announces "World-First" AI Security Standard

Scottish Cyber Coordination Centre

Infosecurity Magazine - 03 February 2025 10:30

The UK government has launched a new AI security code of practice it believes will become an ETSI standard