Scottish Cyber Coordination Centre

Daily Threat Bulletin

28 April 2025

Vulnerabilities

Craft CMS RCE exploit chain used in zero-day attacks to steal data

BleepingComputer - 25 April 2025 16:44

Two vulnerabilities impacting Craft CMS were chained together in zero-day attacks to breach servers and steal data, with exploitation ongoing, according to CERT Orange Cyberdefense. [...]

SAP NetWeaver zero-day allegedly exploited by an initial access broker

Security Affairs - 25 April 2025 16:48

A zero-day in SAP NetWeaver is potentially being exploited, putting thousands of internet-facing applications at risk. Researchers warn that a zero-day vulnerability, tracked as CVE-2025-31324 (CVSS score of 10/10), in SAP NetWeaver is potentially being exploited. Thousands of internet-facing applications are potentially at risk.

Researchers Identify Rack::Static Vulnerability Enabling Data Breaches in Ruby Servers

The Hacker News - 25 April 2025 15:27

Cybersecurity researchers have disclosed three security flaws in the Rack Ruby web server interface that, if successfully exploited, could enable attackers to gain unauthorized access to files, inject malicious data, and tamper with logs under certain conditions.

Popular LLMs Found to Produce Vulnerable Code by Default

Infosecurity Magazine - 25 April 2025 10:30

Backslash Security found that naïve prompts resulted in code vulnerable to at least four of the of the 10 most common vulnerabilities across popular LLMs

Threat actors and malware

Coinbase fixes 2FA log error making people think they were hacked

BleepingComputer - 27 April 2025 15:21

Coinbase has fixed a confusing bug in its account activity logs that caused users to think their credentials were compromised. [...]

DragonForce expands ransomware model with white-label branding scheme

BleepingComputer - 26 April 2025 12:23

The ransomware scene is re-organizing, with one gang known as DragonForce working to gather other operations under a cartel-like structure. [...]

Mobile provider MTN says cyberattack compromised customer data

BleepingComputer - 25 April 2025 11:57

African mobile giant MTN Group announced that a cybersecurity incident has compromised the personal information of some of its subscribers in certain countries. [...]

Storm-1977 targets education sector with password spraying, Microsoft warns

Security Affairs - 27 April 2025 14:12

Microsoft warns that threat actor Storm-1977 is behind password spraying attacks against cloud tenants in the education sector. Over the past year, Microsoft Threat Intelligence researchers observed a threat actor, tracked as Storm-1977.

JPCERT warns of DslogdRAT malware deployed in Ivanti Connect Secure

Security Affairs - 25 April 2025 18:56

Researchers identified a new malware, named DslogdRAT, deployed after exploiting a now-patched flaw in Ivanti Connect Secure (ICS). JPCERT/CC researchers reported that a new malware, dubbed DslogdRAT, and a web shell were deployed by exploiting a zero-day vulnerability during attacks on Japanese organizations in December 2024.

UK related

Marks & Spencer pauses online orders after cyberattack

BleepingComputer - 25 April 2025 12:05

British retailer giant Marks & Spencer (M&S) has suspended online orders while working to recover from a recently disclosed cyberattack. [...]