Scottish Cyber Coordination Centre

Daily Threat Bulletin

29 April 2025

Vulnerabilities

Over 1,200 SAP NetWeaver servers vulnerable to actively exploited flaw

BleepingComputer - 28 April 2025 13:46

Over 1,200 internet-exposed SAP NetWeaver instances are vulnerable to an actively exploited maximum severity unauthenticated file upload vulnerability that allows attackers to hijack servers. [...]

Attackers chained Craft CMS zero-days attacks in the wild

Security Affairs - 28 April 2025 09:34

Orange Cyberdefense's CSIRT reported that threat actors exploited two vulnerabilities in Craft CMS to breach servers and steal data. Orange Cyberdefense's CSIRT warns that threat actors chained two Craft CMS vulnerabilities in recent attacks. Orange experts discovered the flaws while investigating a server compromise.

CISA Adds Actively Exploited Broadcom and Commvault Flaws to KEV Database

The Hacker News - 29 April 2025 10:51

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added two high-severity security flaws impacting Broadcom Brocade Fabric OS and Commvault Web Server to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation in the wild.

Critical Vulnerabilities Found in Planet Technology Industrial Networking Products

SecurityWeek - 28 April 2025 12:09

Planet Technology industrial switches and network management products are affected by several critical vulnerabilities.

Threat actors and malware

Hitachi Vantara takes servers offline after Akira ransomware attack

BleepingComputer - 28 April 2025 16:39

Hitachi Vantara, a subsidiary of Japanese multinational conglomerate Hitachi, was forced to take servers offline over the weekend to contain an Akira ransomware attack. [...]

Earth Kurma APT is actively targeting government and telecommunications orgs in Southeast Asia

Scottish Cyber Coordination Centre

Security Affairs - 28 April 2025 20:44

Earth Kurma APT carried out a sophisticated campaign against government and telecommunications sectors in Southeast Asia. Trend Research exposed the Earth Kurma APT campaign targeting Southeast Asia's government and telecom sectors. Threat actors use custom malware, rootkits, and cloud storage for espionage, credential theft, and data exfiltration, posing a high business risk with advanced evasion [...]

WooCommerce Users Targeted by Fake Patch Phishing Campaign Deploying Site Backdoors

The Hacker News - 28 April 2025 14:36

Cybersecurity researchers are warning about a large-scale phishing campaign targeting WooCommerce users with a fake security alert urging them to download a "critical patch" but deploy a backdoor instead.

Ukrainian state and banking services restored after data center outage

The Record from Recorded Future News - 28 April 2025 15:20

UK related

M&S customers in limbo as cyber attack chaos continues

BBC News - 28 April 2025 14:04

The retail giant's online business remains suspended with no indication yet when it will be restored.