Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

02 May 2025

Vulnerabilities

SonicWall Flags Two More Vulnerabilities as Exploited

SecurityWeek - 01 May 2025 11:00

SonicWall has updated the advisories for two vulnerabilities to warn that they are being exploited in the wild.

Commvault Confirms Hackers Exploited CVE-2025-3928 as Zero-Day in Azure Breach

The Hacker News - 01 May 2025 14:41

Enterprise data backup platform Commvault has revealed that an unknown nation-state threat actor breached its Microsoft Azure environment by exploiting CVE-2025-3928 but emphasized there is no evidence of unauthorized data access.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. CVE-2024-38475 Apache HTTP Server Improper Escaping of Output Vulnerability & CVE-2023-44221 SonicWall SMA100 Appliances OS Command Injection Vulnerability.

Threat actors and malware

Fake Security Plugin on WordPress Enables Remote Admin Access for Attackers

The Hacker News - 01 May 2025 22:17

Cybersecurity researchers have shed light on a new campaign targeting WordPress sites that disguises the malware as a security plugin.The plugin, which goes by the name “WP-antymalwary-bot.php,” comes with a variety of features to maintain access, hide itself from the admin dashboard, and execute remote code.

Pro-Russia hacktivist group NoName057(16) is targeting Dutch organizations

Security Affairs - 02 May 2025 00:08

This week, several Dutch and European organizations faced large-scale DDoS attacks launched by Pro-Russia hacktivists, including the NoName057(16) group. Threat actors target organizations across public and private sectors.

DarkWatchman, Sheriff Malware Hit Russia and Ukraine with Stealth and Nation-Grade Tactics

The Hacker News - 01 May 2025 15:57

Russian companies have been targeted as part of a large-scale phishing campaign that's designed to deliver a known malware called DarkWatchman. Targets of the attacks include entities in the media, tourism, finance and insurance, manufacturing, retail, energy, telecom, transport, and biotechnology sectors.

Claude AI Exploited to Operate 100+ Fake Political Personas in Global Influence Campaign

The Hacker News - 01 May 2025 17:32

Artificial intelligence (AI) company Anthropic has revealed that unknown threat actors leveraged its Claude chatbot for an "influence-as-a-service" operation to engage with authentic accounts across Facebook and X.

UK incidents

Harrods the next UK retailer targeted in a cyberattack

BleepingComputer - 01 May 2025 15:33

London's iconic department store, Harrods, has confirmed it was targeted in a cyberattack, becoming the third major UK retailer to report cyberattacks in a week following incidents at M&S and the Co-op.

ICO: No Further Action on British Library Ransomware Breach

Infosecurity Magazine - 01 May 2025 10:45

The ICO has decided not to fine the British Library for a 2023 ransomware breach