Scottish Cyber Coordination Centre

Daily Threat Bulletin

23 April 2025

Vulnerabilities

Windows 10 KB5055612 preview update fixes a GPU bug in WSL2

BleepingComputer - 22 April 2025 16:25

Microsoft has released the optional KB5055612 preview cumulative update for Windows 10 22H2 with two changes, including a fix for a GPU paravirtualization bug in Windows Subsystem for Linux 2 (WSL2).

GCP Cloud Composer Bug Let Attackers Elevate Access via Malicious PyPI Packages

The Hacker News - 22 April 2025 20:36

Cybersecurity researchers have detailed a now-patched vulnerability in Google Cloud Platform (GCP) that could have enabled an attacker to elevate their privileges in the Cloud Composer workflow orchestration service that's based on Apache Airflow.

CVE-2025-3248: RCE vulnerability in Langflow

Security Boulevard - 22 April 2025 19:56

CVE-2025-3248, a critical remote code execution (RCE) vulnerability with a CVSS score of 9.8, has been discovered in Langflow, an open-source platform for visually composing AI-driven agents and workflows.

Threat actors and malware

Docker Malware Exploits Teneo Web3 Node to Earn Crypto via Fake Heartbeat Signals

The Hacker News - 22 April 2025 23:16

Cybersecurity researchers have detailed a malware campaign that's targeting Docker environments with a previously undocumented technique to mine cryptocurrency.

Cookie-Bite attack PoC uses Chrome extension to steal session tokens

BleepingComputer - 22 April 2025 12:02

A proof-of-concept attack called "Cookie-Bite" uses a browser extension to steal browser session cookies from Azure Entra ID to bypass multi-factor authentication (MFA) protections and maintain access to cloud services like Microsoft 365, Outlook, and Teams.

Scottish Cyber Coordination Centre

Many Malware Campaigns Linked to Proton66 Network

SecurityWeek - 22 April 2025 12:31

Security researchers detail various malware campaigns that use bulletproof services linked to Proton66 ASN.

Legacy Google Service Abused in Phishing Attacks

SecurityWeek - 22 April 2025 12:14

A sophisticated phishing campaign abuses weakness in Google Sites to spoof Google no-reply addresses and bypass protections.

UK incidents

British retailer M&S confirms being hit by 'cyber incident' amid store delays

The Record from Recorded Future News - 22 April 2025 16:05

British retailer Marks and Spencer (M&S) announced on Tuesday it "has been managing a cyber incident over the past few days" following a slew of customer complaints on social media.