Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

25 April 2025

Vulnerabilities

Highest-Risk Security Flaw Found in Commvault Backup Solutions

Infosecurity Magazine - 24 April 2025 15:00

A new critical vulnerability has been found in Commvault, illustrating that backup and replication solutions are highly sought after by cyber threat actors due to their crucial role in data management.

159 CVEs Exploited in Q1 2025 — 28.3% Within 24 Hours of Disclosure

The Hacker News - 24 April 2025 19:25

As many as 159 CVE identifiers have been flagged as exploited in the wild in the first quarter of 2025, up from 151 in Q4 2024.

Cisco Confirms Some Products Impacted by Critical Erlang/OTP Flaw

SecurityWeek - 24 April 2025 09:05

Cisco is investigating the impact of the Erlang/OTP remote code execution vulnerability CVE-2025-32433 on its products.

Microsoft fixes machine learning bug flagging Adobe emails as spam

BleepingComputer - 24 April 2025 16:02

Microsoft says it mitigated a known issue in one of its machine learning (ML) models that mistakenly flagged Adobe emails in Exchange Online as spam.

Threat actors and malware

Hackers abuse OAuth 2.0 workflows to hijack Microsoft 365 accounts

BleepingComputer - 24 April 2025 17:24

Russian threat actors have been abusing legitimate OAuth 2.0 authentication workflows to hijack Microsoft 365 accounts of employees of organizations related to Ukraine and human rights.

Linux io_uring PoC Rootkit Bypasses System Call-Based Threat Detection Tools

The Hacker News - 24 April 2025 19:28

Cybersecurity researchers have demonstrated a proof-of-concept (PoC) rootkit dubbed Curing that leverages a Linux asynchronous I/O mechanism called io_uring to bypass traditional system call monitoring.

Emulating the Hellish Helldown Ransomware

Security Boulevard - 24 April 2025 19:48

AttackIQ has released a new attack graph emulating the behaviors exhibited by Helldown ransomware since its emergence in August 2024. Helldown is operated by the eponymous and still largely undocumented adversary, which employs double extortion tactics by exfiltrating sensitive data prior to encrypting victim systems and threatening to leak the data on its Dedicated Leak Site (DLS).

AI-Powered Polymorphic Phishing Is Changing the Threat Landscape

SecurityWeek - 24 April 2025 12:00

Combined with AI, polymorphic phishing emails have become highly sophisticated, creating more personalized and evasive messages that result in higher attack success rates.