Scottish
Cyber
Coordination
Centre

Daily threat bulletin

3 February 2025

Vulnerabilities

Broadcom Patches VMware Aria Flaws – Exploits May Lead to Credential Theft

The Hacker News - 31 January 2025 12:19

Broadcom has released security updates to patch five security flaws impacting VMware Aria Operations and Aria Operations for Logs, warning customers that attackers could exploit them to gain elevated access or obtain sensitive information.

DeepSeek's Flagship AI Model Under Fire for Security Vulnerabilities

Infosecurity Magazine - 31 January 2025 11:37

Cyber reports exposed major security flaws in DeepSeek's R1 LLM

Threat actors and malware

WhatsApp disrupted a hacking campaign targeting journalists with Paragon spyware

Security Affairs - 02 February 2025 15:04

Meta announced the disruption of a malware campaign via WhatsApp that targeted journalists with the Paragon spyware. Meta announced that discovered and dismantled a malware campaign via WhatsApp that targeted journalists and civil society members with the Paragon spyware (aka Graphite).

ClickFix vs. traditional download in new DarkGate campaign

Malwarebytes - 01 February 2025 00:43

Social engineering methods are being put to the test to distribute malware.

Threat Actors Target Public-Facing Apps for Initial Access

Infosecurity Magazine - 31 January 2025 15:30

Cisco Talos found that exploitation of public-facing applications made up 40% of incidents it observed in Q4 2024, marking a notable shift in initial access techniques

In Other News: Browser Syncjacking, Fake AWS Hack, Google Blocked 2M Bad Apps

SecurityWeek - 31 January 2025 18:10

Noteworthy stories that might have slipped under the radar: stealing browser data via Syncjacking, hackers falsely claim AWS breach, Google prevented 2 million bad apps from reaching Google Play.

Scottish
Cyber
Coordination
Centre