Scottish Cyber Coordination Centre

Daily threat bulletin

25 June 2024

Vulnerabilities

New attack uses MSC files and Windows XSS flaw to breach networks

BleepingComputer - 24 June 2024 16:03

A novel command execution technique dubbed 'GrimResource' uses specially crafted MSC (Microsoft Saved Console) and an unpatched Windows XSS flaw to perform code execution via the Microsoft Management Console. [...]

Google Introduces Project Naptime for AI-Powered Vulnerability Research

The Hacker News - 24 June 2024 21:33

Google has developed a new framework called Project Naptime that it says enables a large language model (LLM) to carry out vulnerability research with an aim to improve automated discovery approaches."

Ollama drama as 'easy-to-exploit' critical flaw found in open source AI server

The Register - 24 June 2024 21:34

About a thousand vulnerable instances still exposed online, we're told A now-patched vulnerability in Ollama – a popular open source project for running LLMs – can lead to remote code execution, according to flaw finders who warned that upwards of 1,000 vulnerable instances remain exposed to the internet.

Threat actors and malware

Experts observed approximately 120 malicious campaigns using the Rafel RAT

Security Affairs - 24 June 2024 14:15

Multiple threat actors are using an open-source Android remote administration tool called Rafel RAT to target Android Devices. Check Point Research identified multiple threat actors using Rafel, an open-source remote administration tool (RAT).

Multiple WordPress Plugins Compromised: Hackers Create Rogue Admin Accounts

The Hacker News - 25 June 2024 10:02

Multiple WordPress plugins have been backdoored to inject malicious code that makes it possible to create rogue administrator accounts with the aim of performing arbitrary actions.

StealC & Vidar Malware Campaign Identified

Security Boulevard - 24 June 2024 20:08

Scottish Cyber Coordination Centre

‘Mirai-like’ botnet observed attacking EOL Zyxel NAS devices

The Register - 24 June 2024 15:39

Seems like as good a time as any to upgrade older hardware There are early indications of active attacks targeting end-of-life Zyxel NAS boxes just a few weeks after details of three critical vulnerabilities were made public.

New SnailLoad Attack Relies on Network Latency Variations to Infer User Activity

SecurityWeek - 24 June 2024 17:07

New attack named SnailLoad allows a remote attacker to infer websites and videos viewed by a user without direct access to network traffic.The post New SnailLoad Attack Relies on Network Latency Variations to Infer User Activity appeared first on SecurityWeek.

Modular Malware Boolka’s BMANAGER Trojan Exposed

Infosecurity Magazine - 24 June 2024 17:15

The group has been observed exploiting vulnerabilities through SQL injection attacks since 2022.