Scottish Cyber Coordination Centre

Daily threat bulletin

10 December 2024

Vulnerabilities

OpenWrt Sysupgrade flaw let hackers push malicious firmware images

BleepingComputer - 09 December 2024 18:33

A flaw in OpenWrt's Attended Sysupgrade feature used to build custom, on-demand firmware images could have allowed for the distribution of malicious firmware packages. [...]

QNAP Patches Vulnerabilities Exploited at Pwn2Own

SecurityWeek - 09 December 2024 14:24

QNAP has released patches for multiple high-severity QTS and QuTS Hero vulnerabilities disclosed at the Pwn2Own Ireland 2024 hacking contest.

Researchers Uncover Prompt Injection Vulnerabilities in DeepSeek and Claude AI

The Hacker News - 09 December 2024 18:25

Details have emerged about a now-patched security flaw in the DeepSeek artificial intelligence (AI) chatbot that, if successfully exploited, could permit a bad actor to take control of a victim's account by means of a prompt injection attack.

Threat actors and malware

Attackers Can Use QR Codes to Bypass Browser Isolation

darkreading - 09 December 2024 20:42

Researchers demonstrate a proof-of-concept cyberattack vector that gets around remote, on-premises, and local versions of browser isolation security technology to send malicious communications from an attacker-controlled server.

Black Basta Ransomware Evolves with Email Bombing, QR Codes, and Social Engineering

The Hacker News - 10 December 2024 00:14

The threat actors linked to the Black Basta ransomware have been observed switching up their social engineering tactics, distributing a different set of payloads such as Zbot and DarkGate since early October 2024.

Unmasking Termite, the Ransomware Gang Claiming the Blue Yonder Attack

Infosecurity Magazine - 09 December 2024 13:35

Scottish Cyber Coordination Centre

This new ransomware group is likely a new variant of Babuk, said Cyble threat intelligence analysts