Scottish
Cyber
Coordination
Centre

Daily threat bulletin

7 January 2025

Vulnerabilities

Vulnerable Moxa devices expose industrial networks to attacks

BleepingComputer - 06 January 2025 13:15

Industrial networking and communications provider Moxa is warning of a high-severity and a critical vulnerability that impact various models of its cellular routers, secure routers, and network security appliances. [...]

MediaTek rings in the new year with a parade of chipset vulns

The Register - 06 January 2025 15:28

Manufacturers should have had ample time to apply the fixes MediaTek kicked off the first full working week of the new year by disclosing a bevy of security vulnerabilities, including a critical remote code execution bug affecting 51 chipsets.

Threat actors and malware

EAGERBEE, with updated and novel components, targets the Middle East

Securelist - 06 January 2025 09:00

Kaspersky researchers analyze EAGERBEE backdoor modules, revealing a possible connection to the CoughingDown APT actor.

New Infostealer Campaign Uses Discord Videogame Lure

Infosecurity Magazine - 06 January 2025 12:10

Threat actors are tricking victims into downloading malware with the promise of testing a new videogame

China-linked Salt Typhoon APT compromised more US telecoms than previously known

Security Affairs - 06 January 2025 10:32

China-linked Salt Typhoon group that breached multiple US telecoms compromised more firms than previously known, WSJ says. The China-linked cyberespionage group Salt Typhoon targeted more US telecoms than previously known, as The Wall Street Journal reported. According to WSJ, wich cited people familiar with the matter, the Chinese cyberspies also compromised Charter Communications and Windstream. [...]

⚡ THN Weekly Recap: Top Cybersecurity Threats, Tools and Tips [6 Jan]

The Hacker News - 06 January 2025 18:35

Every tap, click, and swipe we make online shapes our digital lives, but it also opens doors—some we never meant to unlock. Extensions we trust, assistants we rely on, and even the codes we scan are turning into tools for attackers.