Scottish Cyber Coordination Centre

Daily threat bulletin

26 September 2024

Vulnerabilities

Third Ivanti Bug Comes Under Active Exploit, CISA Warns

darkreading - 25 September 2024 19:03

Though the critical vulnerability was patched in August, Ivanti is reminding customers to update as soon as possible as attacks from unauthenticated threat actors start circulating.

Cybersecurity Researchers Warn of New Rust-Based Splinter Post-Exploitation Tool

The Hacker News - 25 September 2024 19:08

Cybersecurity researchers have flagged the discovery of a new post-exploitation red team tool called Splinter in the wild.Palo Alto Networks Unit 42 shared its findings after it discovered the program on several customers' systems.

ChatGPT macOS Flaw Could've Enabled Long-Term Spyware via Memory Function

The Hacker News - 25 September 2024 18:17

A now-patched security vulnerability in OpenAI's ChatGPT app for macOS could have made it possible for attackers to plant long-term persistent spyware into the artificial intelligence (AI) tool's memory. The technique, dubbed SpAIware, could be abused to facilitate "continuous data exfiltration of any information the user typed or responses received by ChatGPT, including any future chat sessions.

Threat Actors Continue to Exploit OT/ICS through Unsophisticated Means

CISA Advisories -

CISA continues to respond to active exploitation of internet-accessible operational technology (OT) and industrial control systems (ICS) devices, including those in the Water and Wastewater Systems (WWS) Sector. Exposed and vulnerable OT/ICS systems may allow cyber threat actors to use default credentials, conduct brute force attacks, or use other unsophisticated methods to access these devices and cause harm.

Threat actors and malware

China's 'Salt Typhoon' Cooks Up Cyberattacks on US ISPs

darkreading - 25 September 2024 21:41

The state-sponsored advanced persistent threat (APT) is going after high-value communications service provider networks in the US, potentially with a dual set of goals.

Google sees 68% drop in Android memory safety flaws over 5 years

BleepingComputer - 25 September 2024 14:00

The percentage of Android vulnerabilities caused by memory safety issues has dropped from 76% in 2019 to only 24% in 2024, representing a massive decrease of over 68% in five years. [...]

Security Firm Shows How Threat Actors Could Abuse Google's Gemini AI Assistant

SecurityWeek - 25 September 2024 14:35

HiddenLayer has discovered that Google Gemini for Workspace is prone to indirect prompt injection attacks.The post Security Firm Shows How Threat Actors Could Abuse Google's Gemini AI Assistant appeared first on SecurityWeek.

82% of Phishing Sites Now Target Mobile Devices

Infosecurity Magazine - 25 September 2024 16:30

82% of all phishing sites target mobile devices, with 76% using HTTPS to appear secure.

UK related

Cyber attack hits 20 UK railway stations

BBC – 25 September 2024

Network Rail confirmed that the wi-fi systems at stations including London Euston, Manchester Piccadilly, Liverpool Lime Street and Birmingham New Street were affected.