Scottish Cyber Coordination Centre

Daily threat bulletin

13 January 2025

Vulnerabilities

Researchers disclosed details of a now-patched Samsung zero-click flaw

Security Affairs - 10 January 2025 15:45

Researchers at Google Project Zero disclosed a now-patched zero-click vulnerability that affects Samsung devices. Google Project Zero researchers disclosed details about a now-patched zero-click vulnerability, tracked as CVE-2024-49415 (CVSS score: 8.1), in Samsung devices. The flaw is an out-of-bound write issue in libsaped.so prior to SMR Dec-2024 Release 1, it allows remote attackers to execute arbitrary code. [...]

Fake PoC Exploit Targets Security Researchers with Infostealer

Infosecurity Magazine - 10 January 2025 10:15

Trend Micro detailed how attackers are using a fake proof-of-concept for a critical Microsoft vulnerability, designed to steal sensitive data from security researchers

Threat actors and malware

Phishing texts trick Apple iMessage users into disabling protection

BleepingComputer - 12 January 2025 15:31

Cybercriminals are exploiting a trick to turn off Apple iMessage's built-in phishing protection for a text and trick users into re-enabling disabled phishing links. [...]

PayPal Phishing Campaign Employs Genuine Links to Take Over Accounts

SecurityWeek - 10 January 2025 12:50

Fortinet warns of a phishing campaign that uses legitimate links to take over the victims' PayPal accounts.

Banshee macOS Malware Expands Targeting

SecurityWeek - 10 January 2025 13:25

The latest version of the Banshee macOS information stealer no longer checks if the infected systems have the Russian language installed.

AI-Driven Ransomware FunkSec Targets 85 Victims Using Double Extortion Tactics

The Hacker News - 10 January 2025 18:28

Cybersecurity researchers have shed light on a nascent artificial intelligence (AI) assisted ransomware family called FunkSec that sprang forth in late 2024, and has claimed more than

85 victims to date."The group uses double extortion tactics, combining data theft with encryption to pressure victims into paying ransoms," Check Point Research said in a new report shared with The Hacker News. "