Scottish
Cyber
Coordination
Centre

Daily Threat Bulletin

10 March 2025

Vulnerabilities

Mirai-based botnets exploit CVE-2025-1316 zero-day in Edimax IP cameras

Security Affairs - 07 March 2025 20:18

Mirai-based botnets are exploiting a zero-day flaw, tracked as CVE-2025-1316, in Edimax IP cameras, to achieve remote command execution. US CISA warns that multiple botnets are exploiting a recently disclosed vulnerability, tracked as CVE-2025-1316 (CVSS score of 9.8), in Edimax IC-7100 IP cameras.

In Other News: EntrySign AMD Flaw, Massive Attack Targets ISPs, ENISA Report

SecurityWeek - 07 March 2025 18:01

Noteworthy stories that might have slipped under the radar: Google discloses AMD CPU flaw named EntrySign, ISPs in the US and China targeted in massive attack, ENISA report on NIS2 Directive.

Software bug at firm left NHS data ‘vulnerable to hackers’

BBC News - 10 March 2025 02:24

The NHS is looking into claims that a software flaw at Medefer left patient data vulnerable.

Threat actors and malware

Microsoft: North Korean hackers join Qilin ransomware gang

BleepingComputer - 07 March 2025 08:10

Microsoft says a North Korean hacking group tracked as Moonstone Sleet has deployed Qilin ransomware payloads in a limited number of attacks. [...]

Akira ransomware gang used an unsecured webcam to bypass EDR

Security Affairs - 08 March 2025 22:42

The Akira ransomware gang exploited an unsecured webcam to bypass EDR and launch encryption attacks on a victim’s network. Cybersecurity researchers at S-RM team discovered a novel attack technique used by the Akira ransomware gang. The ransomware group used an unsecured webcam to encrypt systems within a target’s network, bypassing Endpoint Detection and Response (EDR). The [...]

International law enforcement operation seized the domain of the Russian crypto exchange Garantex

Security Affairs - 07 March 2025 11:18

The U.S. Secret Service and global law enforcement seized the domain of sanctioned Russian crypto exchange Garantex. An international law enforcement operation led by U.S. Secret Service seized the website ("garantex[.]org") of the sanctioned Russian crypto exchange Garantex. In April 2022, the US Treasury Department sanctioned the virtual currency exchange. Garantex has been active since 2019, [...]

Medusa Ransomware targeted over 40 organizations in 2025

Security Affairs - 07 March 2025 09:42

Medusa ransomware has claimed nearly 400 victims since January 2023, with attacks increasing by 42% between 2023 and 2024. The Symantec Threat Hunter Team reported that the Medusa ransomware operators have claimed nearly 400 victims since January 2023. Experts observed a 42% increase in attacks carried out by the group between 2023 and 2024. Experts [...]

SilentCryptoMiner Infects 2,000 Russian Users via Fake VPN and DPI Bypass Tools

The Hacker News - 10 March 2025 10:42

A new mass malware campaign is infecting users with a cryptocurrency miner named SilentCryptoMiner by masquerading it as a tool designed to circumvent internet blocks and restrictions around online services.Russian cybersecurity company Kaspersky said the activity is part of a larger trend where cybercriminals are increasingly leveraging Windows Packet Divert (WPD) tools to distribute malware