Scottish Cyber Coordination Centre

Daily threat bulletin

30 August 2024

Vulnerabilities

Cisco Patches Multiple NX-OS Software Vulnerabilities

SecurityWeek - 29 August 2024 12:35

Cisco on Wednesday announced NX-OS software updates that resolve multiple vulnerabilities, including a high-severity DoS bug.

Malware exploits 5-year-old zero-day to infect end-of-life IP cameras

BleepingComputer - 29 August 2024 12:46

The Corona Mirai-based malware botnet is spreading through a 5-year-old remote code execution (RCE) zero-day in AVTECH IP cameras, which have been discontinued for years and will not receive a patch. [...]

Threat actors and malware

US Sees Iranian Hackers Working Closely With Ransomware Groups

SecurityWeek - 29 August 2024 08:42

Iranian state-sponsored APT Lemon Sandstorm is working closely with ransomware groups on monetizing network intrusions.

Iranian Hackers Use New Tickler Malware for Intelligence Gathering on Critical Infrastructure

SecurityWeek - 29 August 2024 10:41

The Iran-linked state-sponsored hacker group tracked as Peach Sandstorm has started using a new backdoor in attacks aimed at the US and UAE.

Russian APT29 hackers use iOS, Chrome exploits created by spyware vendors

BleepingComputer - 29 August 2024 10:04

The Russian state-sponsored APT29 hacking group has been observed using the same iOS and Android exploits created by commercial spyware vendors in a series of cyberattacks between November 2023 and July 2024. [...]

North Korean Hackers Target Developers with Malicious npm Packages

The Hacker News - 30 August 2024 12:55

Threat actors with ties to North Korea have been observed publishing a set of malicious packages to the npm registry, indicating “coordinated and relentless” efforts to target

developers with malware and steal cryptocurrency assets.The latest wave, which was observed between August 12 and 27, 2024, involved packages named temp-etherscan-api, ethersscan-api, telegram-con, helmet-validate.

BlackByte Adopts New Tactics, Targets ESXi Hypervisors

Infosecurity Magazine - 29 August 2024 16:30

BlackByte, linked to the Conti group, exploited VMware ESXi CVE-2024-37085 to control virtual machines.

#StopRansomware: RansomHub Ransomware

CISA Advisories -

SummaryNote: This joint Cybersecurity Advisory is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors.