Scottish Cyber Coordination Centre

Daily threat bulletin

14 May 2024

Vulnerabilities

Apple backports fix for RTKit iOS zero-day to older iPhones

BleepingComputer - 13 May 2024 18:47

Apple has backported security patches released in March to older iPhones and iPads, fixing an iOS Kernel zero-day tagged as exploited in attacks. [...]

Severe Vulnerabilities in Cinterion Cellular Modems Pose Risks to Various Industries

The Hacker News - 13 May 2024 16:42

Cybersecurity researchers have disclosed multiple security flaws in Cinterion cellular modems that could be potentially exploited by threat actors to access sensitive information and achieve code execution.

Two F5 BIG-IP Next Central Manager Flaws Allow Device Takeover

Security Boulevard - 13 May 2024 19:23

F5, a multi-cloud security and application delivery vendor, has recently patched two high-risk vulnerabilities in its BIG-IP Next Central Manager.

Threat actors and malware

FCC reveals Royal Tiger, its first tagged robocall threat actor

BleepingComputer - 13 May 2024 17:45

The Federal Communications Commission (FCC) has named its first officially designated robocall threat actor ‘Royal Tiger,’ a move aiming to help international partners and law enforcement more easily track individuals and entities behind repeat robocall campaigns. [...]

Botnet sent millions of emails in LockBit Black ransomware campaign

BleepingComputer - 13 May 2024 16:08

Since April, millions of phishing emails have been sent through the Phorpiex botnet to conduct a large-scale LockBit Black ransomware campaign. [...]

Hackers use DNS tunneling for network scanning, tracking victims

BleepingComputer - 13 May 2024 14:50

Threat actors are using Domain Name System (DNS) tunneling to track when their targets open phishing emails and click on malicious links, and to scan networks for potential vulnerabilities. [...]

MITRE Unveils EMB3D: A Threat-Modeling Framework for Embedded Devices

The Hacker News - 13 May 2024 20:59

The MITRE Corporation has officially made available a new threat-modeling framework called EMB3D for makers of embedded devices used in critical infrastructure environments. ”The model provides a cultivated knowledge base of cyber threats to embedded devices, providing a common understanding of these threats with the security mechanisms required to mitigate them,” the non-profit said.

Mallox Ransomware Deployed Via MS-SQL Honeypot Attack

Infosecurity Magazine - 13 May 2024 16:30

Analyzing Mallox samples, Sekoia identified two distinct affiliates using different approaches.

CISA and Partners Release Advisory on Black Basta Ransomware

CISA Advisories -

Today, CISA, in partnership with the Federal Bureau of Investigation (FBI), the Department of Health and Human Services (HHS), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) released joint Cybersecurity Advisory (CSA) #StopRansomware: Black Basta to provide cybersecurity defenders tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) used by known Black Basta ransomware affiliates and identified through FBI investigations and third-party reporting.Black Basta is a ransomware-as-a-service (RaaS) variant, first identified in April 2022. Black Basta affiliates have targeted over 500 private industry and critical infrastructure entities, including healthcare organizations, in North America, Europe, and Australia.