Scottish
Cyber
Coordination
Centre

Daily threat bulletin

18 October 2024

Vulnerabilities

Microsoft Reveals macOS Vulnerability that Bypasses Privacy Controls in Safari Browser

The Hacker News - 18 October 2024 12:12

Microsoft has disclosed details about a now-patched security flaw in Apple’s Transparency, Consent, and Control (TCC) framework in macOS that has likely come under exploitation to get around a user’s privacy preferences and access data.

F5 BIG-IP Updates Patch High-Severity Elevation of Privilege Vulnerability

SecurityWeek - 17 October 2024 13:51

F5 has released patches for a high-severity elevation of privilege vulnerability in BIG-IP and a medium-severity bug in BIG-IQ.

Cisco Patches High-Severity Vulnerabilities in Analog Telephone Adapters

SecurityWeek - 17 October 2024 12:52

Cisco has released patches for multiple vulnerabilities in ATA 190 series firmware, including two high-severity flaws.

WeChat devs introduced security flaws when they modded TLS, say researchers

The Register - 17 October 2024 09:31

No attacks possible, but enough issues to cause concern Messaging giant WeChat uses a network protocol that the app’s developers modified – and by doing so introduced security weaknesses, researchers claim.

Threat actors and malware

Fake Google Meet conference errors push infostealing malware

BleepingComputer - 17 October 2024 18:00

A new ClickFix campaign is luring users to fraudulent Google Meet conference pages showing fake connectivity errors that deliver info-stealing malware for Windows and macOS operating systems. […]

Russian RomCom Attacks Target Ukrainian Government with New SingleCamper RAT Variant

The Hacker News - 17 October 2024 22:43

The Russian threat actor known as RomCom has been linked to a new wave of cyber attacks aimed at Ukrainian government agencies and unknown Polish entities since at least late 2023.The intrusions are characterized by the use of a variant of the RomCom RAT dubbed SingleCamper (aka SnipBot or RomCom 5.0), said Cisco Talos, which is monitoring the activity cluster under the moniker UAT-5647.

SideWinder APT Strikes Middle East and Africa With Stealthy Multi-Stage Attack

The Hacker News - 17 October 2024 16:45

An advanced persistent threat (APT) actor with suspected ties to India has sprung forth with a flurry of attacks against high-profile entities and strategic infrastructures in the Middle East and Africa.The activity has been attributed to a group tracked as SideWinder, which is also known as APT-C-17, Baby Elephant, Hardcore Nationalist, Leafperforator, Rattlesnake, Razor Tiger, and T-APT-04.

Cicada3301 Ransomware Targets Critical Sectors in US and UK

Infosecurity Magazine - 17 October 2024 17:16

Cicada3301 ransomware has targeted critical sectors in US/UK, leaking data from 30 firms in three months

RansomHub Overtakes LockBit as Most Prolific Ransomware Group

Infosecurity Magazine - 17 October 2024 11:00

Symantec data reveals RansomHub claimed more attacks than any other group in Q3 2024

CISA, FBI, NSA, and International Partners Release Advisory on Iranian Cyber Actors Targeting Critical Infrastructure Organizations Using Brute Force

CISA Advisories -

Today, CISA—with the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and international partners—released joint Cybersecurity Advisory Iranian Cyber Actors Brute Force and Credential Access Activity Compromises Critical Infrastructure. This advisory provides known indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs) used by Iranian actors to impact organizations across multiple critical infrastructure sectors.

UK related

Firm hacked after accidentally hiring North Korean cyber criminal

BBC News – 16 October 2024

A company has been hacked after accidentally hiring a North Korean cyber criminal as a remote IT worker. The unidentified firm hired the technician after he faked his employment history and personal details.