Scottish Cyber Coordination Centre

Daily threat bulletin

10 October 2024

Vulnerabilities

CISA says critical Fortinet RCE flaw now exploited in attacks

BleepingComputer - 09 October 2024 19:07

Today, CISA revealed that attackers actively exploit a critical FortiOS remote code execution (RCE) vulnerability in the wild. [...]

Mozilla fixes Firefox zero-day actively exploited in attacks

BleepingComputer - 09 October 2024 14:34

Mozilla has issued an emergency security update for the Firefox browser to address a critical use-after-free vulnerability that is currently exploited in attacks. [...]

Palo Alto fixed critical flaws in PAN-OS firewalls that allow for full compromise of the devices

Security Affairs - 10 October 2024 06:24

Palo Alto fixed critical flaws in PAN-OS firewalls, warning that attackers could chain these vulnerabilities to hijack the devices. Palo Alto Networks addressed multiple vulnerabilities that an attacker can chain to hijack PAN-OS firewalls.

Researchers Uncover Major Security Vulnerabilities in Industrial MMS Protocol Libraries

The Hacker News - 09 October 2024 22:03

Details have emerged about multiple security vulnerabilities in two implementations of the Manufacturing Message Specification (MMS) protocol that, if successfully exploited, could have severe impacts in industrial environments.

3 More Ivanti Cloud Vulns Exploited in the Wild

darkreading - 09 October 2024 19:47

The security bugs were found susceptible to exploitation in connection to the previously disclosed, critical CVE-2024-8963 vulnerability in the security vendor's Cloud Services Appliance (CSA).

Apple's iPhone Mirroring Flaw Exposes Employee Privacy Risks

Infosecurity Magazine - 09 October 2024 17:15

The privacy flaw in Apple's iPhone mirroring feature enables personal apps on an iPhone to be listed in a company's software inventory when the feature is used on work computers

Scottish Cyber Coordination Centre

Threat actors and malware

Microsoft Detects Growing Use of File Hosting Services in Business Email Compromise Attacks

The Hacker News - 09 October 2024 10:52

Microsoft is warning of cyber attack campaigns that abuse legitimate file hosting services such as SharePoint, OneDrive, and Dropbox that are widely used in enterprise environments as a defense evasion tactic.

Hackers Hide Remcos RAT in GitHub Repository Comments

darkreading - 09 October 2024 22:03

The tack highlights bad actors' interest in trusted development and collaboration platforms — and their users.

Awaken Likho APT group targets Russian government with a new implant

Security Affairs - 09 October 2024 15:00

A threat actor tracked as Awaken Likho is targeting Russian government agencies and industrial entities, reported cybersecurity firm Kaspersky. A recent investigation by Kaspersky researchers into the APT group Awaken Likho (aka Core Werewolf and PseudoGamaredon) uncovered a new campaign from June to August 2024, showing a shift from UltraVNC to the MeshCentral platform.

N. Korean Hackers Use Fake Interviews to Infect Developers with Cross-Platform Malware

The Hacker News - 09 October 2024 20:03

Threat actors with ties to North Korea have been observed targeting job seekers in the tech industry to deliver updated versions of known malware families tracked as BeaverTail and InvisibleFerret.The activity cluster, tracked as CL-STA-0240, is part of a campaign dubbed Contagious Interview that Palo Alto Networks Unit 42 first disclosed in November 2023.