Scottish
Cyber
Coordination
Centre

Daily threat bulletin

19 December 2024

Vulnerabilities

Patch Alert: Critical Apache Struts Flaw Found, Exploitation Attempts Detected

The Hacker News - 18 December 2024 11:23

Threat actors are attempting to exploit a recently disclosed security flaw impacting Apache Struts that could pave the way for remote code execution.The issue, tracked as CVE-2024-53677, carries a CVSS score of 9.5 out of 10.0, indicating critical severity.

Over 25,000 SonicWall VPN Firewalls exposed to critical flaws

BleepingComputer - 17 December 2024 11:27

Over 25,000 publicly accessible SonicWall SSLVPN devices are vulnerable to critical severity flaws, with 20,000 using a SonicOS/OSX firmware version that the vendor no longer supports. [...]

Azure Data Factory Bugs Expose Cloud Infrastructure

darkreading - 17 December 2024 17:21

Three vulnerabilities in the service’s Apache Airflow integration could have allowed attackers to take shadow administrative control over an enterprise cloud infrastructure, gain access to and exfiltrate data, and deploy malware.

Cybercriminals Exploit Google Calendar to Spread Malicious Links

Infosecurity Magazine - 17 December 2024 16:45

Check Point research reveals cybercriminals are using Google Calendar and Drawings to send malicious links, bypassing traditional email security

Threat actors and malware

Attackers Exploit Microsoft Teams and AnyDesk to Deploy DarkGate Malware

The Hacker News - 17 December 2024 23:05

A new social engineering campaign has leveraged Microsoft Teams as a way to facilitate the deployment of a known malware called DarkGate.”An attacker used social engineering via a Microsoft Teams call to impersonate a user’s client and gain remote access to their system.

Hackers Exploit Webview2 to Deploy CoinLurker Malware and Evade Security Detection

The Hacker News - 17 December 2024 15:33

Bogus software update lures are being used by threat actors to deliver a new stealer malware called CoinLurker."Written in Go, CoinLurker employs cutting-edge obfuscation and anti-analysis techniques, making it a highly effective tool in modern cyber attacks," Morphisec researcher Nadav Lorber said in a technical report published Monday.

'Bitter' cyberspies target defense orgs with new MiyaRAT malware

BleepingComputer - 17 December 2024 18:29

A cyberespionage threat group known as 'Bitter' was observed targeting defense organizations in Turkey using a novel malware family named MiyaRAT. [...]

The Mask APT Resurfaces with Sophisticated Multi-Platform Malware Arsenal

The Hacker News - 17 December 2024 13:25

A little-known cyber espionage actor known as The Mask has been linked to a new set of attacks targeting an unnamed organization in Latin America twice in 2019 and 2022."The Mask APT is a legendary threat actor that has been performing highly sophisticated attacks since at least 2007," Kaspersky researchers Georgy Kucherin and Marc Rivero said in an analysis published last week.