Scottish
Cyber
Coordination
Centre

Daily threat bulletin

2 August 2024

Vulnerabilities

Over 20,000 internet-exposed VMware ESXi instances vulnerable to CVE-2024-37085

Security Affairs - 01 August 2024 20:58

Shadowserver researchers reported that over 20,000 internet-exposed VMware ESXi instances are affected by the actively exploited flaw CVE-2024-37085. Researchers at the Shadowserver Foundation reported that approximately 20,000 VMware ESXi servers exposed online appear impacted by the exploited vulnerability CVE-2024-37085. Microsoft this week warned that multiple ransomware gangs are exploiting the recently patched vulnerability CVE-2024-37085 (CVSS […]

Recent Vulnerabilities in Cybersecurity: July 2024 CVE Roundup

Security Boulevard - 02 August 2024 01:33

Recent cybersecurity vulnerabilities reported on the National Institute of Standards and Technology (NIST)'s National Vulnerability Database pose significant risks to organizations worldwide. Without mitigation, data breaches and system compromises are possible.

Homebrew Security Audit Finds 25 Vulnerabilities

SecurityWeek - 01 August 2024 12:08

Vulnerabilities in Homebrew could have allowed attackers to load executable code and modify binary builds, security audit finds..

Threat actors and malware

Hackers abuse free TryCloudflare to deliver remote access malware

BleepingComputer - 01 August 2024 15:33

Researchers are warning of threat actors increasingly abusing the Cloudflare Tunnel service in malware campaigns that usually deliver remote access trojans (RATs). […]

Sitting Ducks DNS attacks let hackers hijack over 35,000 domains

BleepingComputer - 01 August 2024 14:10

Threat actors have hijacked more than 35,000 registered domains in so-called Sitting Ducks attacks that allow claiming a domain without having access to the owner's account at the DNS provider or registrar. […]

Hackers Distributing Malicious Python Packages via Popular Developer Q&A Platform

The Hacker News - 01 August 2024 20:02

In yet another sign that threat actors are always looking out for new ways to trick users into downloading malware, it has come to light that the question-and-answer (Q&A) platform known as Stack Exchange has been abused to direct unsuspecting developers to bogus Python packages capable of draining their cryptocurrency wallets.

Attacks on Bytecode Interpreters Conceal Malicious Injection Activity

darkreading - 01 August 2024 22:32

By injecting malicious bytecode into interpreters for VBScript, Python, and Lua, researchers found they can circumvent malicious code detection.

Black Basta Develops Custom Malware in Wake of Qakbot Takedown

darkreading - 01 August 2024 20:06

The prolific ransomware group has shifted away from phishing as the method of entry into corporate networks, and is now using initial access brokers as well as its own tools to optimize its most recent attacks.

How “professional” ransomware variants boost cybercrime groups

Securelist - 01 August 2024 11:00

Kaspersky researchers investigated three ransomware groups that tapped newly built malware samples based on Babuk, Lockbit, Chaos and others, while lacking professional resources.