Scottish Cyber Coordination Centre

Daily threat bulletin

12 July 2024

Vulnerabilities

Signal downplays encryption key flaw, fixes it after X drama

BleepingComputer - 11 July 2024 17:49

Signal is finally tightening its desktop client's security by changing how it stores plain text encryption keys for the data store after downplaying the issue since 2018.

Palo Alto Networks Patches Critical Flaw in Expedition Migration Tool

The Hacker News - 11 July 2024 21:49

Palo Alto Networks has released security updates to address five security flaws impacting its products, including a critical bug that could lead to an authentication bypass. Cataloged as CVE-2024-5910 (CVSS score: 9.3), the vulnerability has been described as a case of missing authentication in its Expedition migration tool that could lead to an admin account takeover.

OpenSSH bug leaves RHEL 9 and the RHELatives vulnerable

The Register - 11 July 2024 20:13

Newly discovered flaw affects OpenSSH 8.7 and 8.8 daemon The founder of Openwall has discovered a new signal handler race condition in the core sshd daemon used in RHEL 9.x and its various offshoots.

CISA, FBI Urge Immediate Action on OS Command Injection Vulnerabilities in Network Devices

SecurityWeek - 11 July 2024 12:24

In response to recent intrusions, CISA and the FBI are urging businesses and device manufacturers to eliminate OS command injection vulnerabilities at the source.

Threat actors and malware

CRYSTALRAY hacker expands to 1,500 breached systems using SSH-Snake tool

BleepingComputer - 11 July 2024 12:09

A new threat actor known as CRYSTALRAY has significantly broadened its targeting scope with new tactics and exploits, now counting over 1,500 victims whose credentials were stolen and cryptominers deployed.

60 New Malicious Packages Uncovered in NuGet Supply Chain Attack

The Hacker News - 11 July 2024 21:36

Scottish Cyber Coordination Centre

Threat actors have been observed publishing a new wave of malicious packages to the NuGet package manager as part of an ongoing campaign that began in August 2023, while also adding a new layer of stealth to evade detection.

Chinese APT41 Upgrades Malware Arsenal with DodgeBox and MoonWalk

The Hacker News - 11 July 2024 19:01

The China-linked advanced persistent threat (APT) group codenamed APT41 is suspected to be using an “advanced and upgraded version” of a known malware called StealthVector to deliver a previously undocumented backdoor dubbed MoonWalk. The new variant of StealthVector which is also referred to as DUSTPAN has been designated DodgeBox by Zscaler ThreatLabz.

Akira Ransomware: Lightning-Fast Data Exfiltration in 2-Ish Hours

darkreading - 11 July 2024 22:38

The gang’s time from initial access to draining data out of a Veeam server is shockingly fast; after which the attackers went on to deploy actual ransomware in less than a day.

Ransomware Surges Annually Despite Law Enforcement Takedowns

Infosecurity Magazine - 11 July 2024 10:45

Symantec figures suggest a 9% annual increase claimed ransomware attacks