Scottish Cyber Coordination Centre

Daily Threat Bulletin

19 February 2025

Vulnerabilities

New OpenSSH flaws expose SSH servers to MiTM and DoS attacks

BleepingComputer - 18 February 2025 13:07

OpenSSH has released security updates addressing two vulnerabilities, a man-in-the-middle (MitM) and a denial of service flaw, with one of the flaws introduced over a decade ago. [...]

Juniper Networks fixed a critical flaw in Session Smart Routers

Security Affairs - 18 February 2025 23:30

Juniper Networks has addressed a critical vulnerability, tracked as CVE-2025-21589, impacting the Session Smart Router. Juniper Networks addressed a critical authentication bypass vulnerability, tracked as CVE-2025-21589 (CVSS score of 9.8), affecting its Session Smart Router product.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2025-0108 Palo Alto PAN-OS Authentication Bypass Vulnerability, CVE-2024-53704 SonicWall SonicOS SSLVPN Improper Authentication Vulnerability.

Threat actors and malware

New FrigidStealer Malware Targets macOS Users via Fake Browser Updates

The Hacker News - 18 February 2025 19:30

Cybersecurity researchers are alerting to a new campaign that leverages web injects to deliver a new Apple macOS malware known as FrigidStealer.The activity has been attributed to a previously undocumented threat actor known as TA2727, with the information stealers for other platforms such as Windows (Lumma Stealer or DeerStealer) and Android (Marcher).

Evolving Snake Keylogger Variant Targets Windows Users

Infosecurity Magazine - 18 February 2025 15:00

A new Snake Keylogger variant, responsible for over 280 million blocked infection attempts worldwide, has been identified targeting Windows users

Chinese Hackers Exploit MAVInject.exe to Evade Detection in Targeted Cyber Attacks

Scottish Cyber Coordination Centre

The Hacker News - 18 February 2025 21:39

The Chinese state-sponsored threat actor known as Mustang Panda has been observed employing a novel technique to evade detection and maintain control over infected systems.This involves the use of a legitimate Microsoft Windows utility called Microsoft Application Virtualization Injector (MAVInject.exe) to inject the threat actor's malicious payload into an external process, waitfor.exe,

BlackLock On Track to Be 2025's Most Prolific Ransomware Group

Infosecurity Magazine - 18 February 2025 14:00

The BlackLock or Eldorado ransomware gang could be the year's fastest-growing ransomware-as-a-service group