Scottish Cyber Coordination Centre

Daily Threat Bulletin

20 February 2025

Vulnerabilities

Palo Alto Networks warns that CVE-2025-0111 flaw is actively exploited in attacks

Security Affairs - 20 February 2025 07:32

Palo Alto Networks warns that threat actors are chaining the vulnerability CVE-2025-0111 with two other vulnerabilities, tracked as CVE-2025-0108 with CVE-2024-9474, to compromise PAN-OS firewalls.

Citrix Releases Security Fix for NetScaler Console Privilege Escalation Vulnerability

The Hacker News - 20 February 2025 11:06

Citrix has released security updates for a high-severity security flaw impacting NetScaler Console (formerly NetScaler ADM) and NetScaler Agent that could lead to privilege escalation under certain conditions. The vulnerability, tracked as CVE-2024-12284, has been given a CVSS v4 score of 8.8 out of a maximum of 10.0.

Microsoft Patches Actively Exploited Power Pages Privilege Escalation Vulnerability

The Hacker News - 20 February 2025 10:59

Microsoft has released security updates to address two Critical-rated flaws impacting Bing and Power Pages, including one that has come under active exploitation in the wild. The vulnerabilities are listed below - CVE-2025-21355 (CVSS score: 8.6) - Microsoft Bing Remote Code Execution Vulnerability & CVE-2025-24989 (CVSS score: 8.2) - Microsoft Power Pages Elevation of Privilege Vulnerability.

Chrome 133, Firefox 135 Updates Patch High-Severity Vulnerabilities

SecurityWeek - 19 February 2025 13:57

Google and Mozilla resolve high-severity memory safety vulnerabilities with the latest Chrome and Firefox security updates.

Threat actors and malware

Russian phishing campaigns exploit Signal's device-linking feature

BleepingComputer - 19 February 2025 07:59

Russian threat actors have been launching phishing campaigns that exploit the legitimate "Linked Devices" feature in the Signal messaging app to gain unauthorized access to accounts of interest.

Scottish Cyber Coordination Centre

Macs targeted by infostealers in new era of cyberthreats

Malwarebytes - 19 February 2025 13:51

Info stealers are thriving on Mac, with one specific variant accounting for 70% of all info stealer detections at the end of 2024.

#StopRansomware: Ghost (Cring) Ransomware

CISA Advisories -

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are releasing this joint advisory to disseminate known Ghost (Cring) - ("Ghost") - ransomware IOCs and TTPs identified through FBI investigation as recently as January 2025.

UK incidents

Medusa ransomware gang demands $2M from UK private health services provider

The Register - 20 February 2025 08:34

HCRG Care Group, a private health and social services provider, has seemingly fallen victim to the Medusa ransomware gang, which is threatening to leak what's claimed to be stolen internal records unless a substantial ransom is paid.