Scottish Cyber Coordination Centre

Daily Threat Bulletin

23 August 2024

Vulnerabilities

Slack Patches AI Bug That Let Attackers Steal Data From Private Channels

darkreading - 22 August 2024 16:36

A prompt injection flaw in the AI feature of the workforce collaboration suite makes malicious queries of data sources appear legitimate.

Chinese Hackers Exploit Zero-Day Cisco Switch Flaw to Gain System Control

The Hacker News - 22 August 2024 22:43

Details have emerged about a China-nexus threat group's exploitation of a recently disclosed, now-patched security flaw in Cisco switches as a zero-day to seize control of the appliances and evade detection. The activity, attributed to Velvet Ant, was observed early this year and involved the weaponization of CVE-2024-20399 (CVSS score: 6.0) to deliver bespoke malware and gain extensive control.

New 'ALBeast' Vulnerability Exposes Weakness in AWS Application Load Balancer

The Hacker News - 22 August 2024 21:33

As many as 15,000 applications using Amazon Web Services' (AWS) Application Load Balancer (ALB) for authentication are potentially susceptible to a configuration-based issue that could expose them to sidestep access controls and compromise applications.

8 vulnerabilities found in macOS operating system Microsoft apps

Security Magazine - 22 August 2024 09:00

Researchers discovered 8 vulnerabilities in macOS operating system Microsoft apps, and security leaders are sharing their insights.

Google Chrome Update Fixes Flaw Exploited in the Wild

darkreading - 22 August 2024 19:38

New Chrome release set to roll out over the next few days addresses 38 security issues in the browser.

SolarWinds fixes hardcoded credentials flaw in Web Help Desk

BleepingComputer - 22 August 2024 12:01

SolarWinds has released a hotfix for a critical Web Help Desk vulnerability that allows attackers to log into unpatched systems using hardcoded credentials.

Scottish Cyber Coordination Centre

Threat actors and malware

New macOS Malware "Cthulhu Stealer" Targets Apple Users' Data

The Hacker News - 23 August 2024 11:31

Cybersecurity researchers have uncovered a new information stealer that's designed to target Apple macOS hosts and harvest a wide range of information, underscoring how threat actors are increasingly setting their sights on the operating system. Dubbed Cthulhu Stealer, the malware has been available under a malware-as-a-service (MaaS) model for $500 a month from late 2023.

NFC Traffic Stealer Targets Android Users &amp; Their Banking Info

darkreading - 22 August 2024 21:30

The malware builds on a near-field communication tool in combination with phishing and social engineering to steal cash.

Qilin ransomware caught stealing credentials stored in Google Chrome

Threat Research – Sophos News - 22 August 2024 11:45

During a recent investigation of a Qilin ransomware breach, the Sophos X-Ops team identified attacker activity leading to en-masse theft of credentials stored in Google Chrome browsers

Understanding the ‘Morphology’ of Ransomware: A Deeper Dive

SecurityWeek - 22 August 2024 14:12

Ransomware isn't just about malware. It's about brands, trust, and the shifting allegiances of cybercriminals.