Scottish
Cyber
Coordination
Centre

Daily threat bulletin

14 January 2025

Vulnerabilities

Cloud Attackers Exploit Max-Critical Aviatrix RCE Flaw

darkreading - 13 January 2025 21:44

The security vulnerability tracked as CVE-2024-50603, which rates 10 out of 10 on the CVSS scale, enables unauthenticated remote code execution on affected systems, which cyberattackers are using to plant malware.

Microsoft: macOS bug lets hackers install malicious kernel drivers

BleepingComputer - 13 January 2025 14:24

Apple recently addressed a macOS vulnerability that allows attackers to bypass System Integrity Protection (SIP) and install malicious kernel drivers by loading third-party kernel extensions. [...]

CISA Adds Second BeyondTrust Flaw to KEV Catalog Amid Active Attacks

The Hacker News - 14 January 2025 09:51

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a second security flaw impacting BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) products to the Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation in the wild.

Juniper Networks Fixes High-Severity Vulnerabilities in Junos OS

SecurityWeek - 13 January 2025 13:04

Juniper Networks has patched multiple high-severity vulnerabilities in Junos OS and its third-party components.

Threat actors and malware

Infostealer Masquerades as PoC Code Targeting Recent LDAP Vulnerability

SecurityWeek - 13 January 2025 15:23

A fake proof-of-concept (PoC) exploit for a recent LDAP vulnerability distributes information stealer malware..

Ransomware abuses Amazon AWS feature to encrypt S3 buckets

BleepingComputer - 13 January 2025 11:27

A new ransomware campaign encrypts Amazon S3 buckets using AWS's Server-Side Encryption with Customer Provided Keys (SSE-C) known only to the threat actor, demanding ransoms to receive the decryption key. [...]

Credit Card Skimmer campaign targets WordPress via database injection

Security Affairs - 13 January 2025 10:58

Stealthy credit card skimmer targets WordPress e-commerce sites, injecting malicious JavaScript into CMS database tables to evade detection. Sucuri researchers warn of a stealthy credit card skimmer campaign targeting WordPress e-commerce sites by injecting malicious JavaScript into CMS database tables.

Cyberattackers Hide Infostealers in YouTube Comments, Google Search Results

darkreading - 13 January 2025 18:26

Threat actors are targeting people searching for pirated or cracked software with fake downloaders that include infostealing malware such as Lumma and Vidar.

UK proposes banning hospitals and schools from making ransomware payments

The Record from Recorded Future News - 13 January 2025 20:08

UK related

UK domain registry Nominet confirms breach via Ivanti zero-day

BleepingComputer - 13 January 2025 12:50

Nominet, the official .UK domain registry and one of the largest country code registries, has confirmed that its network was breached two weeks ago using an Ivanti VPN zero-day vulnerability. [...]