Scottish Cyber Coordination Centre

Daily threat bulletin

22 January 2025

Vulnerabilities

7-Zip fixes bug that bypasses Windows MoTW security warnings, patch now

BleepingComputer - 21 January 2025 12:05

A high-severity vulnerability in the 7-Zip file archiver allows attackers to bypass the Mark of the Web (MotW) Windows security feature and execute code on users' computers when extracting malicious files from nested archives. [...]

Imperva Protects Against the Exploited CVEs in the Cleo Data Theft Attacks

Security Boulevard - 21 January 2025 22:01

The Clop ransomware group has once again demonstrated its ability to exploit vulnerabilities to compromise sensitive systems. As Cleo—a managed file transfer provider for businesses—grapples with the aftermath of Clop's targeted attack on their systems, the spotlight turns to CVE-2024-50623 and CVE-2024-55956, two critical vulnerabilities that enabled these breaches.

Patch procrastination leaves 50,000 Fortinet firewalls vulnerable to zero-day

The Register - 21 January 2025 19:45

Seven days after disclosure and little action taken, data shows Fortinet customers need to get with the program and apply the latest updates as nearly 50,000 management interfaces are still vulnerable to the latest zero-day exploit.

Oracle To Address 320 Vulnerabilities in January Patch Update

Infosecurity Magazine - 21 January 2025 13:45

Critical flaws include those in Oracle Supply Chain products

Threat actors and malware

New Mirai botnet variant Murdoc Botnet targets AVTECH IP cameras and Huawei HG532 routers

Security Affairs - 21 January 2025 17:41

Researchers warn of a campaign exploiting AVTECH IP cameras and Huawei HG532 routers to create a Mirai botnet variant called Murdoc Botnet. Murdoc Botnet is a new Mirai botnet variant that targets vulnerabilities in AVTECH IP cameras and Huawei HG532 routers, the Qualys Threat Research Unit reported.

Cloudflare mitigated a record-breaking 5.6 Tbps DDoS attack

Scottish Cyber Coordination Centre

BleepingComputer - 21 January 2025 17:04

The largest distributed denial-of-service (DDoS) attack to date peaked at 5.6 terabits per second and came from a Mirai-based botnet with 13,000 compromised devices. [...]

Ransomware gangs pose as IT support in Microsoft Teams phishing attacks

BleepingComputer - 21 January 2025 11:59

Ransomware gangs are increasingly adopting email bombing followed by posing as tech support in Microsoft Teams calls to trick employees into allowing remote control and install malware that provides access to the company network. [...]

Two-factor authentication phishing kit targets Microsoft 365 accounts

Security Magazine - 21 January 2025 12:00

New research from has unveiled a phishing-as-a-service kit, and security leaders are sharing their insights.

Phishing Risks Rise as Zendesk Subdomains Facilitate Attacks

Infosecurity Magazine - 21 January 2025 16:45

A CloudSEK report revealed Zendesk's platform can be exploited for phishing and investment scams

Fake Homebrew Google ads target Mac users with malware

BleepingComputer - 21 January 2025 15:58

Hackers are once again abusing Google ads to spread malware, using a fake Homebrew website to infect Macs and Linux devices with an infostealer that steals credentials, browser data, and cryptocurrency wallets. [...]

UK related

UK's New Digital IDs Raise Security and Privacy Fears

Infosecurity Magazine - 21 January 2025 17:25

Security experts have outlined security and privacy concerns around the UK government's GOV.UK Wallet, which will allow citizens to store all their ID documents in a single place