Scottish Cyber Coordination Centre

Daily threat bulletin

2 May 2024

Vulnerabilities

HPE Aruba Networking fixes four critical RCE flaws in ArubaOS

BleepingComputer - 01 May 2024 19:31

HPE Aruba Networking has issued its April 2024 security advisory detailing critical remote code execution (RCE) vulnerabilities impacting multiple versions of ArubaOS, its proprietary network operating system. [...]

CISA says GitLab account takeover bug is actively exploited in attacks

BleepingComputer - 01 May 2024 13:29

CISA warned today that attackers are actively exploiting a maximum-severity GitLab vulnerability that allows them to take over accounts via password resets. [...]

DBIR: Vulnerability Exploits Triple as Initial Access Point for Data Breaches

Infosecurity Magazine - 01 May 2024 12:00

The growth of software supply chain attacks pushed vulnerability exploits to the third most used initial access method, Verizon found.

Threat actors and malware

DropBox says hackers stole customer data, auth secrets from eSignature service

BleepingComputer - 01 May 2024 19:22

Cloud storage firm DropBox says hackers breached production systems for its DropBox Sign eSignature platform and gained access to authentication tokens, MFA keys, hashed passwords, and customer information. [...]

New Cuttlefish malware infects routers to monitor traffic for credentials

BleepingComputer - 01 May 2024 10:00

A new malware named 'Cuttlefish' has been spotted infecting enterprise-grade and small office/home office (SOHO) routers to monitor data that passes through them and steal authentication information. [...]

ZLoader Malware Evolves with Anti-Analysis Trick from Zeus Banking Trojan

The Hacker News - 01 May 2024 16:57

The authors behind the resurfaced ZLoader malware have added a feature that was originally present in the Zeus banking trojan that it's based on, indicating that it's being

actively developed."The latest version, 2.4.1.0, introduces a feature to prevent execution on machines that differ from the original infection," Zscaler ThreatLabz researcher Santiago

LockBit, Black Basta, Play Dominate Ransomware in Q1 2024

Infosecurity Magazine - 01 May 2024 17:00

The data from ReliaQuest also suggests LockBit faced a significant setback due to law enforcement action

NCSC's New Mobile Risk Model Aimed at "High-Threat" Firms

Infosecurity Magazine - 01 May 2024 09:45

The UK's National Cyber Security Centre claims its AMS model will protect firms from state-backed mobile threats