Scottish Cyber Coordination Centre

Daily threat bulletin

2 October 2024

Vulnerabilities

Zimbra RCE Vuln Under Attack Needs Immediate Patching

darkreading - 01 October 2024 22:41

The bug gives attackers a way to run arbitrary code on affected servers and take control of them.

Organizations Warned of Exploited SAP, Gpac and D-Link Vulnerabilities

SecurityWeek - 01 October 2024 13:19

CISA warns that years-old vulnerabilities in SAP Commerce, Gpac framework, and D-Link DIR-820 routers are exploited in the wild.

Arc browser launches bug bounty program after fixing RCE bug

BleepingComputer - 01 October 2024 19:33

The Browser Company has introduced an Arc Bug Bounty Program to encourage security researchers to report vulnerabilities to the project and receive rewards. [...]

Threat actors and malware

AI-Powered Rhadamanthys Stealer Targets Crypto Wallets with Image Recognition

The Hacker News - 01 October 2024 23:04

The threat actors behind the Rhadamanthys information stealer have added new advanced features to the malware, including using artificial intelligence (AI) for optical character recognition (OCR) as part of what's called "Seed Phrase Image Recognition."

Free Sniper Dz Phishing Tools Fuel 140,000+ Cyber Attacks Targeting User Credentials

The Hacker News - 01 October 2024 13:02

More than 140,000 phishing websites have been found linked to a phishing-as-a-service (PhaaS) platform named Sniper Dz over the past year, indicating that it's being used by a large number of cybercriminals to conduct credential theft.

Cyberattackers Use HR Targets to Lay More_Eggs Backdoor

darkreading - 01 October 2024 18:21

The FIN6 group is the likely culprit behind a spear-phishing campaign that demonstrates a shift in tactics, from targeting job seekers to going after those who hire.

Scottish Cyber Coordination Centre

More LockBit Hackers Arrested, Unmasked as Law Enforcement Seizes Servers

SecurityWeek - 01 October 2024 16:06

Previously seized LockBit websites have been used to announce more arrests, charges and infrastructure disruptions.

Evil Corp hit with new sanctions, BitPaymer ransomware charges

BleepingComputer - 01 October 2024 13:30

The Evil Corp cybercrime syndicate has been hit with new sanctions by the United States, United Kingdom, and Australia. The US also indicted one of its members for conducting BitPaymer ransomware attacks. [...]