Scottish
Cyber
Coordination
Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

8 January 2023

Vulnerabilities

Ivanti patches critical flaw in its EPM software

SC Magazine US - January 5 2024

Ivanti on 4 Jan. patched a critical vulnerability (CVSS 9.6) in its endpoint manager (EPM) software that could have let an attacker with internal access launch a remote code execution (RCE). The vulnerability — CVE-2023-39336 — if exploited, could let an attacker leverage an unspecified SQL injection to execute arbitrary SQL queries and retrieve output without the need for authentication.

Hackers target Apache RocketMQ servers vulnerable to RCE attacks

BleepingComputer.com - January 5 2024

Security researchers are detecting hundreds of IP addresses on a daily basis that scan or attempt to exploit Apache RocketMQ services vulnerable to a remote command execution flaw identified as CVE-2023-33246 and CVE-2023-37582.

CISA Advisory: Critical Vulnerabilities Found in Rockwell, Mitsubishi, and Unitronics Devices

The Cyber Express - January 5 2024

The Cybersecurity and Infrastructure Security Agency (CISA) has published three advisories addressing security issues, vulnerabilities, and potential exploits in Industrial Control Systems (ICS).

Ransomware

Diving deep into Phobos ransomware. [Research Saturday]

The CyberWire - January 6 2024

Guilherme Venere from Cisco Talos joins to discuss their research on "A deep dive into Phobos ransomware, recently deployed by 8Base group."

TLP CLEAR: Disclosure is not limited

Malware and threat actors

Turkish Sea Turtle APT targets Dutch IT and Telecom firms

Security Affairs - January 7 2024

Sea Turtle cyber espionage group targeted telco, media, ISPs, IT service providers, and Kurdish websites in the Netherlands. Researchers from Dutch security firm Hunt & Hackett observed Sea Turtle cyber espionage group (aka Teal Kurma, Marbled Dust, SILICON and Cosmic Wolf) targeting telco, media, ISPs, IT service providers, and Kurdish websites in the Netherlands.

Experts spotted a new macOS Backdoor named SpectralBlur linked to North Korea

Security Affairs - January 6 2024

Researchers discovered a macOS backdoor, called SpectralBlur, which shows similarities with a North Korean APT's malware family. Security researcher Greg Lesnewich discovered a backdoor, called SpectralBlur, that targets Apple macOS.

Stealthy AsyncRAT malware attacks targets US infrastructure for 11 months

BleepingComputer.com - January 7 2024

A campaign delivering the AsyncRAT malware to select targets has been active for at least the past 11 months, using hundreds of unique loader samples and more than 100 domains.