Scottish Cyber Coordination Centre

Daily threat bulletin

18 April 2024

Vulnerabilities

Cisco discloses root escalation flaw with public exploit code

BleepingComputer - 17 April 2024 14:25

Cisco has released patches for a high-severity Integrated Management Controller (IMC) vulnerability with public exploit code that can let local attackers escalate privileges to root.

Ivanti fixed two critical flaws in its Avalanche MDM

Security Affairs - 17 April 2024 11:49

Ivanti addressed two critical vulnerabilities in its Avalanche mobile device management (MDM) solution, that can lead to remote command execution. Ivanti addressed multiple flaws in its Avalanche mobile device management (MDM) solution, including two critical flaws, tracked as CVE-2024-24996 and CVE-2024-29204, that can lead to remote command execution. The MDM software allows administrators to configure.

Critical Atlassian Flaw Exploited to Deploy Linux Variant of Cerber Ransomware

The Hacker News - 17 April 2024 17:27

Threat actors are exploiting unpatched Atlassian servers to deploy a Linux variant of Cerber (aka C3RB3R) ransomware. The attacks leverage CVE-2023-22518(CVSS score: 9.1), a critical security vulnerability impacting the Atlassian Confluence Data Center and Server that allows an unauthenticated attacker to reset Confluence and create an administrator account.

Hackers Exploit Fortinet Flaw, Deploy ScreenConnect, Metasploit in New Campaign

The Hacker News - 17 April 2024 16:53

Cybersecurity researchers have discovered a new campaign that’s exploiting a recently disclosed security flaw in Fortinet FortiClient EMS devices to deliver ScreenConnect and Metasploit Powerfun payloads.The activity entails the exploitation of CVE-2023-48788 (CVSS score: 9.3), a critical SQL injection flaw that could permit an unauthenticated attacker to execute unauthorized code.

Active Kubernetes RCE Attack Relies on Known OpenMetadata Vulns

Scottish Cyber Coordination Centre

darkreading - 17 April 2024 20:14

Once attackers have control over a workload in the cluster, they can leverage access for lateral movement both inside the cluster and to external resources.

SoumniBot malware exploits Android bugs to evade detection

BleepingComputer - 17 April 2024 18:38

A new Android banking malware named 'SoumniBot' is using a less common obfuscation approach by exploiting weaknessesin the Android manifest extraction and parsing procedure.

Threat actors and malware

FIN7 targets American automaker's IT staff in phishing attacks

BleepingComputer - 17 April 2024 17:40

The financially motivated threat actor FIN7 targeted a large U.S. car maker with spear-phishing emails for employees in the IT department to infect systems withthe Anunak backdoor.

Russian APT Deploys New 'Kapeka' Backdoor in Eastern European Attacks

The Hacker News - 17 April 2024 20:02

A previously undocumented "flexible" backdoor called Kapeka has been "sporadically" observed in cyber attacks targeting Eastern Europe, including Estonia and Ukraine, since at least mid-2022.The findings come from Finnish cybersecurity firm WithSecure, which attributed the malware to the Russia-linked advanced persistent threat (APT) group tracked as Sandworm.

Various Botnets Pummel Year-Old TP-Link Flaw in IoT Attacks

darkreading - 17 April 2024 15:11

Moobot, Miori, AGoent, and a Gafgyt variant have joined the infamous Mirai botnet in attacking unpatched versions of vulnerable Wi-Fi routers.

North Korean Group Kimsuky Exploits DMARC and Web Beacons

Infosecurity Magazine - 17 April 2024 16:30

Proofpoint confirmed Kimsuky has directly contacted foreign policy experts since 2023 through seemingly benign email conversations