Scottish Cyber Coordination Centre

Daily threat bulletin

8 May 2024

Vulnerabilities

Hackers exploit LiteSpeed Cache flaw to create WordPress admins

BleepingComputer - 07 May 2024 18:42

Hackers have been targeting WordPress sites with an outdated version of the LiteSpeed Cache plugin to create administrator users and gain control of the websites. [...]

RSAC: Log4J Still Among Top Exploited Vulnerabilities, Cato Finds

Infosecurity Magazine - 07 May 2024 17:22

A new report by Cato Networks found that exploiting old vulnerabilities in unpatched systems is one of threat actors' favorite initial access vectors

Exploits and vulnerabilities in Q1 2024

Securelist - 07 May 2024 11:00

The report provides vulnerability and exploit statistics, key trends, and analysis of interesting vulnerabilities discovered in Q1 2024.

Threat actors and malware

The UK Says a Huge Payroll Data Breach by a 'Malign Actor' Has Exposed Details of Military Personnel

SecurityWeek - 07 May 2024 19:41

The UK Ministry of Defense said a breach at a third-party payroll system exposed as many as 272,000 armed forces personnel and veterans. The post The UK Says a Huge Payroll Data Breach by a 'Malign Actor' Has Exposed Details of Military Personnel appeared first on SecurityWeek.

New attack leaks VPN traffic using rogue DHCP servers

BleepingComputer - 07 May 2024 15:46

A new attack dubbed "TunnelVision" can route traffic outside a VPN's encryption tunnel, allowing attackers to snoop on unencrypted traffic while maintaining the appearance of a secure VPN connection. [...]

APT42 Hackers Pose as Journalists to Harvest Credentials and Access Cloud Data

The Hacker News - 07 May 2024 19:55

The Iranian state-backed hacking outfit called APT42 is making use of enhanced social engineering schemes to infiltrate target networks and cloud environments.Targets of the attack include Western and Middle Eastern NGOs, media organizations, academia, legal services and activists, Google Cloud subsidiary Mandiant said in a report published last week."

China-Linked Hackers Used ROOTROT Webshell in MITRE Network Intrusion

The Hacker News - 07 May 2024 19:25

The MITRE Corporation has offered more details into the recently disclosed cyber attack, stating that the first evidence of the intrusion now dates back to December 31, 2023. The attack, which came to light last month, singled out MITRE's Networked Experimentation, Research, and Virtualization Environment (NERVE) through the exploitation of two Ivanti Connect Secure zero-days.