Scottish Cyber Coordination Centre

Daily threat bulletin

8 October 2024

Vulnerabilities

Critical Apache Avro SDK RCE flaw impacts Java applications

Security Affairs - 07 October 2024 12:04

A critical vulnerability, tracked as CVE-2024-47561, in the Apache Avro Java Software Development Kit (SDK) could allow the execution of arbitrary code on vulnerable instances.

Qualcomm Urges OEMs to Patch Critical DSP and WLAN Flaws Amid Active Exploits

The Hacker News - 08 October 2024 10:37

Qualcomm has rolled out security updates to address nearly two dozen flaws spanning proprietary and open-source components, including one that has come under active exploitation in the wild.

Single HTTP Request Can Exploit 6M WordPress Sites

darkreading - 07 October 2024 10:45

The popular LiteSpeed Cache plug-in is vulnerable to unauthenticated privilege escalation via a dangerous XSS flaw.

Okta Tells Users to Check for Potential Exploitation of Newly Patched Vulnerability

SecurityWeek - 07 October 2024 11:28

Okta has resolved a vulnerability that could have allowed attackers to bypass sign-on policies and gain access to applications.

Threat actors and malware

New Gorilla Botnet Launches Over 300,000 DDoS Attacks Across 100 Countries

The Hacker News - 07 October 2024 20:22

Cybersecurity researchers have discovered a new botnet malware family called Gorilla (aka GorillaBot) that draws its inspiration from the leaked Mirai botnet source code. Cybersecurity firm NSFOCUS, which identified the activity last month, said the botnet “issued over 300,000 attack commands, with a shocking attack density” between September 4 and September 27, 2024.

Advanced Threat Group GoldenJackal Exploits Air-Gapped Systems

Infosecurity Magazine - 07 October 2024 16:30

Scottish Cyber Coordination Centre

GoldenJackal targeted air-gapped government systems from May 2022 to March 2024, ESET found.

Recently spotted Trinity ransomware spurs federal warning to healthcare industry

The Record from Recorded Future News - 07 October 2024 20:44

At least one U.S. healthcare entity has fallen victim to a new ransomware strain called Trinity, according to a report from federal officials.

A Modern Playbook for Ransomware

Security Boulevard - 07 October 2024 23:58

SOC teams need every advantage against ransomware. Learn how a SOAR playbook can streamline incident response, saving time and minimizing the impact of attacks.