Scottish Cyber Coordination Centre

Daily Threat Bulletin

24 September 2024

Vulnerabilities

ESET fixed two privilege escalation flaws in its products

Security Affairs - 23 September 2024 18:43

ESET addressed two local privilege escalation vulnerabilities in security products for Windows and macOS operating systems. Cybersecurity firm ESET released security patches for two local privilege escalation vulnerabilities impacting Windows and macOS products.

Critical Flaw in Microchip ASF Exposes IoT Devices to Remote Code Execution Risk

The Hacker News - 23 September 2024 16:28

A critical security flaw has been disclosed in the Microchip Advanced Software Framework (ASF) that, if successfully exploited, could lead to remote code execution. The vulnerability, tracked as CVE-2024-7490, carries a CVSS score of 9.5 out of a maximum of 10.0.

Vulnerabilities Found in Popular Houzez Theme and Plugin

Infosecurity Magazine - 23 September 2024 16:30

The flaws are dangerous as the Houzez theme and Login Register plugin could allow privilege escalation by unauthenticated users

Threat actors and malware

New Mallox ransomware Linux variant based on leaked Kryptina code

BleepingComputer - 23 September 2024 15:29

An affiliate of the Mallox ransomware operation, also known as TargetCompany, was spotted using a slightly modified version of the Kryptina ransomware to attack Linux systems.

Android malware 'Necro' infects 11 million devices via Google Play

BleepingComputer - 23 September 2024 12:15

A new version of the Necro malware loader for Android was installed on 11 million devices through Google Play in malicious SDK supply chain attacks.

Meet UNC1860: Iran's Low-Key Access Broker for State Hackers

darkreading - 24 September 2024 06:30

The group has used more than 30 custom tools to target high-value government and telecommunications organizations on behalf of Iranian intelligence services.

Scottish Cyber Coordination Centre

Microsoft Trims Cloud Cyberattack Surface in Security Push

darkreading - 23 September 2024 22:23

The company has jettisoned hundreds of thousands of unused apps and millions of unused tenants as part of its Secure Future Initiative.