Scottish Cyber Coordination Centre

Daily threat bulletin

16 May 2024

Vulnerabilities

Google patches third exploited Chrome zero-day in a week

BleepingComputer - 15 May 2024 19:36

Google has released a new emergency Chrome security update to address the third zero-day vulnerability exploited in attacks within a week. [...]

Flaw in Wi-Fi Standard Can Enable SSID Confusion Attacks

darkreading - 15 May 2024 22:32

Attackers can exploit the issue to trick users into connecting to insecure networks, but it works only under specific conditions.

D-Link Routers Vulnerable to Takeover Via Exploit for Zero-Day

darkreading - 15 May 2024 16:42

A vulnerability in the HNAP login request protocol that affects a family of devices gives unauthenticated users root access for command execution.

Intel Publishes 41 Security Advisories for Over 90 Vulnerabilities

SecurityWeek - 15 May 2024 14:58

Intel has published 41 new May 2024 Patch Tuesday advisories covering a total of more than 90 vulnerabilities. The post Intel Publishes 41 Security Advisories for Over 90 Vulnerabilities appeared first on SecurityWeek.

PDF Exploitation Targets Foxit Reader Users

Infosecurity Magazine - 15 May 2024 16:30

CPR said exploit builders in .NET and Python have been employed to deploy this malware

Threat actors and malware

Android 15, Google Play Protect get new anti-malware and anti-fraud features

BleepingComputer - 15 May 2024 16:53

Today, Google announced new security features coming to Android 15 and Google Play Protect that will help block scams, fraud, and malware apps on users' devices. [...]

Windows Quick Assist abused in Black Basta ransomware attacks

BleepingComputer - 15 May 2024 14:06

Financially motivated cybercriminals abuse the Windows Quick Assist feature in social engineering attacks to deploy Black Basta ransomware payloads on victims' networks. [...]

Threat Actors Abuse GitHub to Distribute Multiple Information Stealers

SecurityWeek - 15 May 2024 15:08

Russian-speaking threat actors are caught abusing a GitHub profile to distribute information stealers posing as legitimate software.The post Threat Actors Abuse GitHub to Distribute Multiple Information Stealers appeared first on SecurityWeek.

Unveiling common ransomware attack methods to secure your organization

Security Magazine - 15 May 2024 13:00

Instead of wondering whether or not they'll be hit with a ransomware attack, leaders need to be building a strategy for what to do when an attack is attempted on their business.

Banco Santander warns of a data breach exposing customer info

BleepingComputer - 15 May 2024 11:11

Banco Santander S.A. announced it suffered a data breach impacting customers after an unauthorized actor accessed a database hosted by one of its third-party service providers. [...]

FBI seize BreachForums hacking forum used to leak stolen data

BleepingComputer - 15 May 2024 11:44

The FBI has seized the notorious BreachForums hacking forum that leaked and sold stolen corporate data to other cybercriminals. [...]