Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

11 December 2023

Vulnerabilities

Syrus4 IoT Gateway Vulnerability Could Allow Code Execution on Thousands of Vehicles, Simultaneously (CVE-2023-6248)

SOCRadar - December 8 2023

A significant vulnerability affecting Syrus4 IoT Gateway has emerged, posing a serious threat to the worldwide automotive industry. This vulnerability, capable of giving hackers control over a fleet of vehicles and potentially shutting them down, has been left unattended by the vendor for an extended period.

Update Your Microsoft Edge Now! Critical Vulnerabilities Patched

InfoTech News - RSS - December 8 2023

Microsoft has released a critical security update for its Edge browser. This update addresses multiple vulnerabilities that could be exploited by attackers to gain access to your system, steal sensitive information, or even take control of your computer. What are the vulnerabilities? The update patches three vulnerabilities: CVE-2023-38174 (CVSS score of 4.3): This vulnerability could allow attackers to disclose limited information about your system.

SLAM Attack: New Spectre-based Vulnerability Impacts Intel, AMD, and Arm CPUs

The Hacker News - December 9 2023

Researchers from the Vrije Universiteit Amsterdam have disclosed a new side-channel attack called SLAM that could be exploited to leak sensitive information from kernel memory on current and upcoming CPUs from Intel, AMD, and Arm.

Malware and threat actors

SpyLoan Scandal: 18 Malicious Loan Apps Defraud Millions of Android Users

The Hacker News - December 11 2023

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Cybersecurity researchers have discovered 18 malicious loan apps for Android on the Google Play Store that have been collectively downloaded over 12 million times. "Despite their attractive appearance, these services are in fact designed to defraud users by offering them high-interest-rate loans endorsed with deceitful descriptions.

Analyzing AsyncRAT's Code Injection into Aspnet_Compiler[.]exe Across Multiple Incident Response Cases

Trend Micro Research News Perspectives - December 11 2023

This blog entry delves into MxDR's unraveling of the AsyncRAT infection chain across multiple cases, shedding light on the misuse of aspnet_compiler[.]exe, a legitimate Microsoft process originally designed for precompiling ASP[.]NET web applications.