Scottish
Cyber
Coordination
Centre

Daily threat bulletin

17 June 2024

Vulnerabilities

CISA warns of Windows bug exploited in ransomware attacks

BleepingComputer - 14 June 2024 13:39

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added a high-severity Windows vulnerability abused in ransomware attacks as a zero-day to its catalog of actively exploited security bugs. [...]

ASUS fixed critical remote authentication bypass bug in several routers

Security Affairs - 16 June 2024 08:44

Taiwanese manufacturer giant ASUS addressed a critical remote authentication bypass vulnerability impacting several router models. ASUS addresses a critical remote authentication bypass vulnerability, tracked as CVE-2024-3080 (CVSS v3.1 score: 9.8), impacting seven router models. The flaw is an authentication bypass issue that a remote attacker can exploit to log into the device without authentication.

CISA adds Android Pixel, Microsoft Windows, Progress Telerik Report Server bugs to its Known Exploited Vulnerabilities catalog

Security Affairs - 14 June 2024 10:46

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds Android Pixel, Microsoft Windows, Progress Telerik Report Server bugs to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the following vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog: CVE-2024-32896 is an elevation of privilege vulnerability in the Pixel Firmware.

ZKTeco Biometric System Found Vulnerable to 24 Critical Security Flaws

The Hacker News - 14 June 2024 14:39

An analysis of a hybrid biometric access system from Chinese manufacturer ZKTeco has uncovered two dozen security flaws that could be used by attackers to defeat authentication, steal biometric data, and even deploy malicious backdoors

Rockwell Automation Patches High-Severity Vulnerabilities in FactoryTalk View SE

SecurityWeek - 14 June 2024 11:17

Rockwell Automation has patched three high-severity vulnerabilities in its FactoryTalk View SE HMI software.The post Rockwell Automation Patches High-Severity Vulnerabilities in FactoryTalk View SE appeared first on SecurityWeek.

Threat actors and malware

New ARM 'TIKTAG' attack impacts Google Chrome, Linux systems

BleepingComputer - 16 June 2024 11:16

A new speculative execution attack named "TIKTAG" targets ARM's Memory Tagging Extension (MTE) to leak data with over a 95% chance of success, allowing hackers to bypass the security feature. [...]

New Linux malware is controlled through emojis sent from Discord

BleepingComputer - 15 June 2024 14:08

A newly discovered Linux malware dubbed 'DISGOMOJI' uses the novel approach of utilizing emojis to execute commands on infected devices in attacks on government agencies in India. [...]

Scattered Spider hackers switch focus to cloud apps for data theft

BleepingComputer - 14 June 2024 12:04

The Scattered Spider gang has started to steal data from software-as-a-service (SaaS) applications and establish persistence through creating new virtual machines. [...]

NiceRAT Malware Targets South Korean Users via Cracked Software

The Hacker News - 17 June 2024 11:41

Threat actors have been observed deploying a malware called NiceRAT to co-opt infected devices into a botnet. The attacks, which target South Korean users, are designed to propagate the malware under the guise of cracked software, such as Microsoft Windows, or tools that purport to offer license verification for Microsoft Office.