Scottish Cyber Coordination Centre

Daily threat bulletin

5 August 2024

Vulnerabilities

Avtech camera vulnerability actively exploited in the wild, CISA warns

Security Affairs - 02 August 2024 14:55

CISA warned that an Avtech camera vulnerability, which is still unpatched, is being actively exploited in the wild. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) published an advisory to warn of a vulnerability, tracked as CVE-2024-7029 (CVSS base score of 8.8), in Avtech camera that has been exploited in the wild.

Critical Flaw in Rockwell Automation Devices Allows Unauthorized Access

The Hacker News - 05 August 2024 12:37

A high-severity security bypass vulnerability has been disclosed in Rockwell Automation ControlLogix 1756 devices that could be exploited to execute common industrial protocol (CIP) programming and configuration commands. The flaw, which is assigned the CVE identifier CVE-2024-6242, carries a CVSS v3.1 score of 8.4.

Threat actors and malware

Surge in Magniber ransomware attacks impact home users worldwide

BleepingComputer - 04 August 2024 11:17

Linux kernel impacted by new SLUBStick cross-cache attack

BleepingComputer - 03 August 2024 12:17

A novel Linux Kernel cross-cache attack named SLUBStick has a 99% success in converting a limited heap vulnerability into an arbitrary memory read-and-write capability, letting the researchers elevate privileges or escape containers.

Chinese StormBamboo APT compromised ISP to deliver malware

Security Affairs - 04 August 2024 16:55

A China-linked APT, tracked as StormBamboo, compromised an internet service provider (ISP) to poison software update mechanisms with malware. Volexity researchers reported that a China-linked APT group, tracked as StormBamboo (aka Evasive Panda, Daggerfly, and StormCloud), successfully compromised an undisclosed internet service provider (ISP) in order to poison DNS responses for target organizations.

New Android Trojan “BlankBot” Targets Turkish Users’ Financial Data

The Hacker News - 05 August 2024 11:24

Cybersecurity researchers have discovered a new Android banking trojan called BlankBot targeting Turkish users with an aim to steal financial information."BlankBot features a range of malicious capabilities, which include customer injections, keylogging, screen recording and it communicates with a control server over a WebSocket connection," Intel 471 said in an analysis published last week.

Mirai Botnet targeting OFBiz Servers Vulnerable to Directory Traversal

The Hacker News - 02 August 2024 17:22

Enterprise Resource Planning (ERP) Software is at the heart of many enterprising supporting human resources, accounting, shipping, and manufacturing. These systems can become very complex and difficult to maintain. They are often highly customized, which can make patching difficult. However, critical vulnerabilities keep affecting these systems and put critical business data at risk.

Cloudflare Tunnels Abused for Malware Delivery

SecurityWeek - 02 August 2024 10:39

Threat actors are abusing Cloudflare's TryCloudflare feature to create one-time tunnels for the distribution of remote access trojans.The post Cloudflare Tunnels Abused for Malware Delivery appeared first on SecurityWeek.

UK related

NCSC Unveils Advanced Cyber Defence 2.0 to Combat Evolving Threats

Infosecurity Magazine - 02 August 2024 10:50

The UK's NCSC is launching ACD 2.0, an advanced suite of cybersecurity tools and services designed to protect businesses from evolving cyber threats