مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Vulnerability in Ezviz Internet PT Camera

Tracking #:432316188

Date:27-08-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a critical vulnerability in the Ezviz Internet PT Camera that could be exploited to gain control of affected devices.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE ID:** CVE-2024-42531
- **CVSS Score:** 9.8 (Critical)
- A critical vulnerability exists in the Ezviz Internet PT Camera CS-CV246 (Model: CS-CV246) (B0-1C1WFR). This vulnerability allows unauthorized individuals to remotely access the camera's live video stream without requiring any authentication. This could lead to severe privacy breaches and security risks.
- The vulnerability stems from the camera's improper handling of RTSP requests. By crafting specific RTSP packets with malicious URLs, attackers can bypass the camera's security controls and hijack its live video feed.
- Successful exploitation of this vulnerability could grant attackers unauthorized access to the camera's live feed, potentially compromising sensitive information and activities. This could pose significant security risks, enabling attackers to plan physical breaches or other malicious actions.

Affected Devices:

- Ezviz Internet PT Camera CS-CV246 (Model: CS-CV246) (B0-1C1WFR) with Serial Number: D15655150 and Version: V5.3.0 build 191225

RECOMMENDATIONS:

- **Update Firmware:** Immediately update the firmware of Ezviz Internet PT Camera CS-CV246 to the latest version available from the manufacturer's website. This update should address the vulnerability and provide necessary security patches.
- **Change Default Credentials:** Change the default username and password for camera. Using strong, unique credentials can help prevent unauthorized access.
- **Limit Network Access:** Restrict network access to camera by configuring router to allow only authorized devices to connect. This can help reduce the risk of unauthorized access.
- **Monitor for Updates:** Keep an eye on the manufacturer's website for any additional security advisories or updates related to this vulnerability.
- **Consider Alternative Cameras:** If it is not possible to update the firmware or address the vulnerability in the current camera, consider replacing it with a more secure model.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2024-42531