Midterm Report

Investigating the security vulnerabilities of a low-cost consumer security camera

Silvia Horga, Agile Astapoviciute, Anna Smolko

December 2025

1 Introduction

In this project, we analyze a wireless security camera sold on Amazon. The device is manufactured by Z-IOT and pairs with a mobile application named "Z-IOT CAM" that enables users to view the camera's video stream. Our goal is to identify potential vulnerabilities in both the camera and its associated mobile app.

2 Vulnerabilities we identified

2.1 Research on camera and Z-IOT

We began our investigation by researching the manufacturer. We found no publicly available documentation regarding the device's security architecture, protocols, or firmware. This lack of information and transparency suggests potential weaknesses. Additionally, user reviews of the Z-IOT app highlighted several security-related issues, including reports of weak authentication mechanisms and indications that login procedures can be bypassed. This further reinforced our suspicion that the device may contain exploitable vulnerabilities.

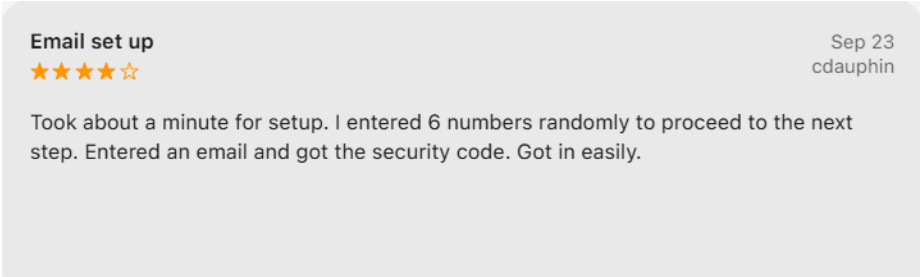

Figure 1: Enter Caption

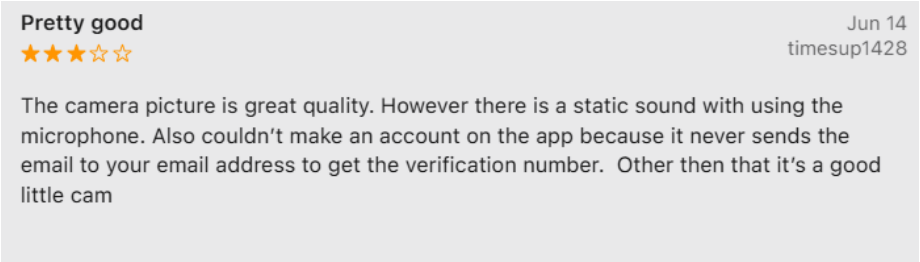

Figure 2: User Review

2.2 Testing

After receiving the camera, we evaluated different usage scenarios without employing any active exploitation methods.

When powered on without prior Wi-Fi configuration, the camera creates its own open Wi-Fi network. The AP has the following characteristics:

- It is an unauthenticated access point, meaning that the Wi-Fi network has no password and that any nearby user can join during setup. However,the app requires the creation of a user account.
- The camera supports two distinct modes of operation: a **single-client mode** and a **multi-client mode**. In single-client mode, only one device can be connected to the camera's access point at a time. When we attempted to join the AP with a second device while a streaming session was active, the legitimate client was forcibly disconnected.
- The app also gave us more information into some aspects of the camera, such that it only supports 2.4GHz Wifi connection, suggesting a minimal and potentially outdated wireless implementation. It probably doesn't support modern, more secure protocols like WPA3, and might only use older ones like WPA, or a weak implementation of WPA2.

2.3 Network Mapping

After connecting a laptop to the camera's access point, an Nmap scan revealed one open TCP port: 7070/tcp ("realserver"). All other common services (HTTP, RTSP, Telnet, SSH) are closed. By connecting to port 7070 using ncat, we confirmed that the service accepts TCP connections without authentication and that it does not respond to plaintext input or malformed binary payloads. This strongly suggests a structured binary protocol used exclusively by the vendor app. We conclude that exploiting this channel may give us access to sensitive information, since these are signs that the port is intended for sending configuration messages, retrieving device information and completing the initial pairing process

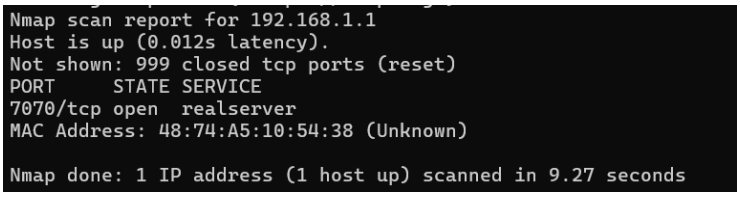

Figure 3: Nmap Scan

3 Planned Exploits

Based on the vulnerabilities we identified during our analysis, we have come up with the following ideas of exploiting our camera:

- **Setup Hijacking via the Open Access Point.** Since the camera's AP is open and supports only one client at a time mode, we could connect to it before the legitimate user. By doing so, we could take control of the configuration process and prevent the victim from pairing the device during its initial setup.
- **Device Impersonation and Hijacking.** The access point only supports one client at a time mode and connecting as a second client forcibly disconnects the legitimate user. This behaviour could be abused to repeatedly kick users off the camera and perform configuration steps in their place. We havent tested this extensively, but it is a promising vulnerability.
- **Man-in-the-Middle Attacks on the Mobile App.** The app's communication with the device during pairing appears to lack authentication and may lack integrity protection. We will therefore try to inject or modify configuration packets, alter the camera's network configuration.
- **Unauthorized Device Configuration.** The binary protocol on port 7070 accepts unauthenticated TCP connections. With further reverse engineering, we could build configuration messages and adjust device settings without using the official app.
- **Denial-of-Service During Setup.** By maintaining a connection to the AP or repeatedly initiating new connections, we could prevent any legitimate device from completing the setup process. This form of denial-of-service would render the camera unusable until reset.
- **Cloud Account Takeover Risks (Indirect).** Users must register an account in the Z-IOT mobile app, but the app ecosystem has been reported to contain weak authentication flows. The reported bugs seem to have been fixed in the most recent version, but we are planning on further testing the functionality of the app.