Vulnerability Report – QBee Multi-Sensor Camera

Description

Cleartext transmission of session cookies between the phone application on android (“QBee Camera” or “Swisscom Home App”) and the camera.

An attacker with access to the local network is able to read and reuse the cookies in order to gain access to the camera settings, potentially disabling the camera.

In case the user solely relies on the Swisscom Home App for the camera management the attack can result in a complete denial of service of the camera (DoS).

Platform

The following devices and versions have been used during the test:

- Samsung Galaxy Edge 6, Android OS 6.0.1
  - QBee Camera App – Version 1.0.5
  - Swisscom Home App – Version 10.5.2
- QBee Camera
  - HW Version: 4.1 - Firmware Version: 4.16.4

Impact

CVSS v3 Severity and Metrics:

- Base Score: 6.4
- Vector: AV:A/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:H
- Impact Score: 4.7
- Exploitability Score: 1.6

Steps to reproduce

The vulnerability requires the attacker to have access to the local network and to be able to record the traffic between an authorized phone and the camera.

Once the user opens and uses the application the cookies are transmitted in cleartext over http to the camera.

The attacker can thus parse the cookies and reuse them in a custom script in order to gain access to the camera functions and settings.

A proof of concept script along with a network capture are provided alongside this report (qbee.py, pcap_parser.py & qbee_camera_network.pcap); in the capture file the traffic until 19:51 is generated by the “QBee Camera” application and that after 19:52 by the “Swisscom Home App”.

1. Intercept traffic between an authorized phone and the camera
2. Manually obtain the JSESSIONID, GC_ID and LD_ID from the pcap or parse the pcap with "pcap_parser.py" (eg. "python pcap_parser.py your_capture.pcap camera_ip")
3. Load the credentials and camera IP in qbee.py
4. Edit and run qbee.py to reflect the wanted status of the camera.

The demo video (qbee_vulnerability.mp4) included provides more insight on how the attack is carried out.

Recommendations

Encrypt all traffic between the phone and the camera with https.

Francesco Servida
University of Lausanne
In collaboration with Seculabs SA