Vulnerability Report – QBee Camera App (Android)

Description

The android version of the QBee Camera application stores the encrypted user password in the configuration file alongside the AES key for decryption (com.vestiacom.qbeecamera_preferences.xml).

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

Impact

CVSS v3 Severity and Metrics:

- Base Score: 6.4
- Vector: AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
- Impact Score: 5.9
- Exploitability Score: 0.5

Steps to reproduce

The vulnerability requires the attacker to have physical access to the user device in order to extract the configuration file from the QBee Camera application.

In the configuration file the user password is stored encrypted. However, the decryption key can be derived by combining a cleartext key with a hardcoded key present in the application APK.

Using the derived key, the attacker is able to decrypt the configuration file and extract the user password.

A proof of concept decryption script along with a configuration file extracted from the test phone is provided (crypto_dec.py). The script accepts a “com.vestiacom.qbeecamera_preferences.xml” file as input and outputs a decrypted version of the configuration in JSON format.

Recommendations

The application should use a token-based authentication system and only store the authorization token in the configuration.

Francesco Servida
University of Lausanne
In collaboration with Seculabs SA