Vulnerability Report – iSmartAlarm App (Android)

Description

The android version of the iSmartAlarm application stores the user password in cleartext in the configuration file (iSmartAlermData.xml).

Platform

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

- Samsung Galaxy Edge 6, Android OS 6.0.1
    - iSmartAlarm App – Version 2.0.8

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 iSmartAlarm application.

In the configuration file the user password is stored in cleartext.

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