AV-TEST Analysis of Fitbit Vulnerabilities

In June 2015, AV-TEST published a report about security issues in fitness trackers. The discovered issues were reported to the respective vendors. Subsequently we started to work with the vendors to resolve the issues.

Fitbit responded immediately after publication of the results and asked for more information. AV-TEST then provided detailed information and supported Fitbit by testing the fixes before they were released to the general public.

Details about the findings are listed below.

Date of analysis: May/June 2015

Initial Report to Fitbit: June 10th 2015 (via Fitbit's German Press agency)

Publication of sanitized results: June 22nd 2015

Incoming Inquiry from Fitbit Security Team: June 23rd 2015

Fixed by Fitbit: September 23rd for certain products, December 8th for the complete set of products

Publication of details: April 2016

Fitbit were initially notified via their German Press Agency due to the lack of a published security contact on their website. Fitbit now publish information about how to contact their security department on their website https://www.fitbit.com/security

Vulnerability 1

Fitbit Charge with firmware version 106 and lower allows non-authenticated smartphones to be treated as authenticated if an authenticated smartphone is in range or has been in range recently.

- (According to Fitbit) a successful authentication of a smartphone sets an authentication flag on tracker.
- The reset of this flag does not happen (in time) under certain circumstances after an authorized smartphone is disconnected.
- As long as the flag is not reset, all connections are considered authorised

As a result of this, an attacker in the vicinity of an affected tracker could read live fitness data and receive updates on fitness data.

- Reading characteristic 558dfa01-4fa8-4105-9f02-4eaa93e62980 and enabling notifications for this characteristic is possible without re-authentication
- Because of this, an attacker is able to tracking a user's activity metrics in (almost) real-time by getting notified whenever user fitness data is updated

This issue was resolved in version 110 of Fitbit Charge.

Vulnerability 2

Fitbit Charge with firmware version 106 and lower allows attackers to replay the tracker synchronization process. The attacker is thereby able to restore tracker system functions like alarm timers, system date and fitness data back to an earlier value.

- Attackers who are able to capture communications between a fitness tracker and client are able to replay a valid synchronisation sequence and thereby manipulate the system status of the tracker
- Synchronized data is encrypted and/or secured by check sums, i.e. imitation of synchronisation process (if at all) only possible with considerable efforts in reverse engineering
- But simple replay works, i.e. security mechanisms with at least a time-dependent factor are not present

This issue was resolved in version 110 of Fitbit Charge.