TREEL_TPMS 2W kit(Bike)- Valve Type Sensor

Reported By:
Amir Saiyad
Sr. Security Researcher
FEV India Pvt Ltd.
saiyad_a@fev.com

Table of Contents

1. Introduction

1.1. Overview

This document describes the vulnerabilities observed from the security research conducted on BLE communication between TPMS and Mobile Application **(Smart Tyre Car & Bike).**

The purpose of this research was to identify any potential vulnerabilities in the BLE communication between TPMS and Mobile Application **(Smart Tyre Car & Bike).**

1.2. Research Team

The security research was conducted by:

Amir Saiyad, Senior Security Researcher, FEV India Pvt Ltd.

Amir Saiyad a is a Senior Security Researcher, holding a B. Tech degree in electronics and communication and have embedded system course certificate from vector India institute. With over four years of dedicated experience in wireless, IVN, hardware security. And have one year of experience in development of router firmware with cyber security.

1.3. Methodology

Black Box testing approach was taken to make sure the BLE communication between TPMS and Mobile Application **(Smart Tyre Car & Bike)** was assessed against vulnerabilities from all possible security perspectives.

2. Summary

The following table is the summary of vulnerabilities and findings, which summaries the overall risks identified during the penetration testing.

Total of **01** risks were identified during the test.

Target	**Total Vulnerabilities**				
	Critical	**High**	**Medium**	**Low**	**Info**
Counts	0	1	0	0	0

The following graph summarizes the distribution of the risks identified by vulnerability rating.

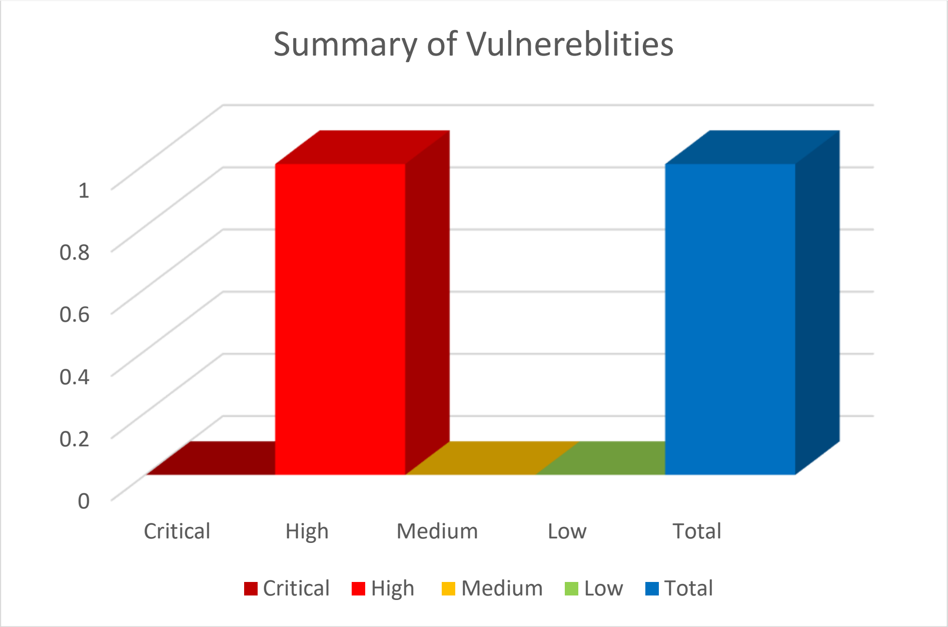


Figure 1: Vulnerability Risk Summary Graph

Vulnerability ID	Vulnerability	Severity
BLE_VUL_01	TPMS Data Manipulation over BLE	HIGH

3. Detailed Description of the Vulnerabilities and findings

3.1. Vulnerabilities:

3.1.1. TPMS Data Manipulation over BLE.

Reconnaissance:

Vulnerability Description:

During the observation and enumeration of BLE communication between TPMS and Mobile Application **(Smart Tyre Car & Bike)**, found that TPMS advertises data without including time stamp and TAG id is configured with same MAC address. It allows an attacker to enumerate service UUID, manufacture data, Type, etc. and send random data over BLE to application.

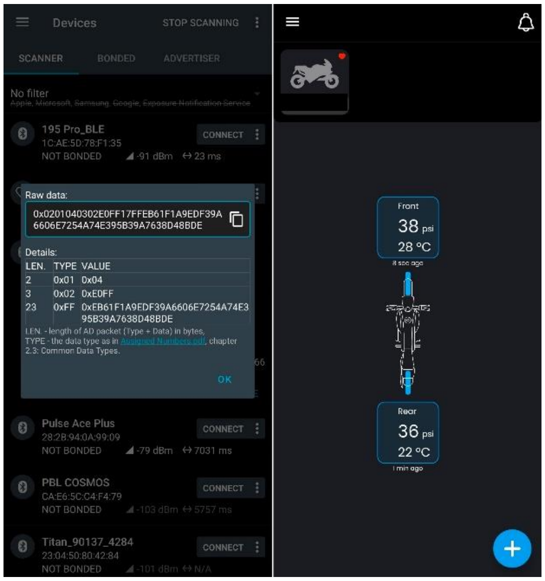
Technical Impact:

By exploiting this vulnerability an attacker can send a random data to application and can raise false warning for tire pressure, temperature and battery percentage with in between 50 to 80 meters.

Test Methodology:

Note: We have demonstrated by sending the random data to a specific device but the same can be performed on all the registered devices under the applications environment.

Prerequisite: Using BLE scanner scan near by all BLE device and identify TPMS and it's MAC Address. This you can easily identify because TPMS will advertisement after every 2 Min.



Devices
STOP SCANNING
SCANNER
BONDED
ADVERTISER
No filter
~~Apple, Microsoft, Samsung, Google, Exposure Notification Service~~

195 Pro_BLE
1C:AE:5D:78:F1:35
NOT BONDED -91 dBm ↔ 23 ms

Raw data:
0x0201040302E0FF17FFEB61F1A9EDF39A6606E7254A74E395B39A7638D48BDE

Details:

LEN.	TYPE	VALUE
2	0x01	0x04
3	0x02	0xE0FF
23	0xFF	0xEB61F1A9EDF39A6606E7254A74E395B39A7638D48BDE

LEN. - length of AD packet (Type + Data) in bytes,
TYPE - the data type as in Assigned Numbers.pdf, chapter 2.3: Common Data Types.

Pulse Ace Plus
28:2B:94:0A:99:09
NOT BONDED -79 dBm ↔ 7031 ms

PBL COSMOS
CA:E6:5C:C4:F4:79
NOT BONDED -103 dBm ↔ 5757 ms

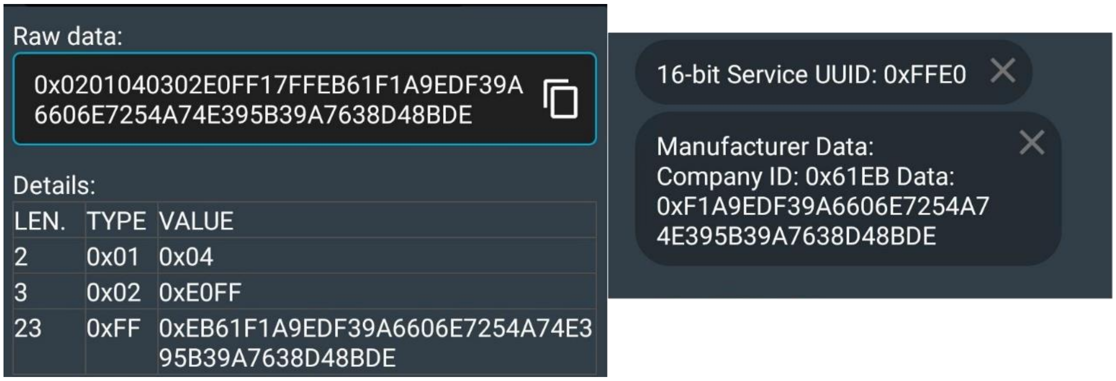
Titan_90137_4284
23:04:50:80:42:84
NOT BONDED -101 dBm ↔ N/A

Front
38 psi
28 °C
8 sec ago

Rear
36 psi
22 °C
1 min ago

TPMS Advertainment and actual data in application.

1. First scan for TPMS BLE advertisement and decode and understand type, value, length of data, service UUID, company ID and data.



Raw data:
0x0201040302E0FF17FFEB61F1A9EDF39A6606E7254A74E395B39A7638D48BDE

Details:

LEN.	TYPE	VALUE
2	0x01	0x04
3	0x02	0xE0FF
23	0xFF	0xEB61F1A9EDF39A6606E7254A74E395B39A7638D48BDE

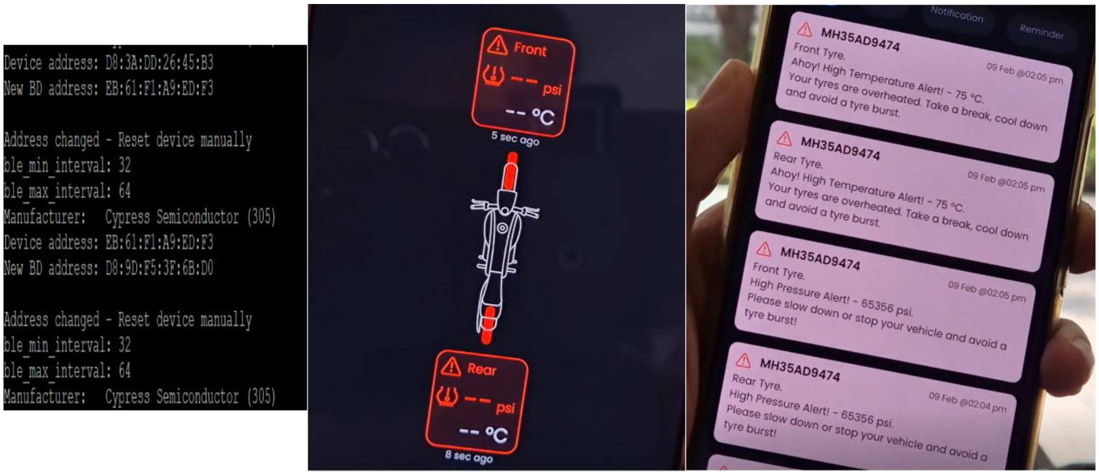
16-bit Service UUID: 0xFFE0

Manufacturer Data:
Company ID: 0x61EB Data:
0xF1A9EDF39A6606E7254A74E395B39A7638D48BDE

TPMS data

2. Write an own code, which will change mac address of own device (**NOTE**: I used raspberry-pi but by using BLE dongle can also do this) as per TPMS MAC address and start BLE advertisement with same type, service UUID, Value, company ID and random data.

3. As soon as advertisement start User get false data and warning of TPMS even existence sensor is in range with user.



```
Device address: D8:3A:DD:26:45:B3
New BD address: EB:61:F1:A9:ED:F3

Address changed - Reset device manually
ble_min_interval: 32
ble_max_interval: 64
Manufacturer:   Cypress Semiconductor (305)
Device address: EB:61:F1:A9:ED:F3
New BD address: D8:9D:F5:3F:6B:D0

Address changed - Reset device manually
ble_min_interval: 32
ble_max_interval: 64
Manufacturer:   Cypress Semiconductor (305)
```

MH35AD9474
Front Tyre.
09 Feb @02:05 pm
Ahoy! High Temperature Alert! - 75 °C.
Your tyres are overheated. Take a break, cool down and avoid a tyre burst.

MH35AD9474
Rear Tyre.
09 Feb @02:05 pm
Ahoy! High Temperature Alert! - 75 °C.
Your tyres are overheated. Take a break, cool down and avoid a tyre burst.

MH35AD9474
Front Tyre.
09 Feb @02:05 pm
High Pressure Alert! - 65356 psi.
Please slow down or stop your vehicle and avoid a tyre burst!

MH35AD9474
Rear Tyre.
09 Feb @02:04 pm
High Pressure Alert! - 65356 psi.
Please slow down or stop your vehicle and avoid a tyre burst!

After attack observation

Remediation:

Include time-stamp also in advertisement and check time-stamp at application end, if match then only accept data. And try to add mechanism where manufacture data and service UUID can be hide.

CVSS Score:

CVSS-v3.1 score (NVD - CVSS v3 Calculator (nist.gov))for this vulnerability is provided below.

CVSS Base Vector:	AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H	**Base Score: 8.3**

About Us

FEV is a globally leading engineering provider in the automotive industry and internationally recognized leader of innovation across different sectors, supplying solutions and strategy consulting to the world's largest automotive OEMs and Tier 1 companies through the entire transportation and mobility ecosystem.
FEV India commenced its operations in 2006, today, we have strong team of over 950+ adept and specialized engineers working from FEV offices located at major automotive hubs of India: Pune (Talegaon, Baner, Chinchwad) | Chennai | Delhi | Jaipur.

FEV Secure Lab is one of FEV India's verticals where innovation meets security in IOT/OT and automotive cybersecurity. FEV Secure Lab is committed to securing the future of connected vehicles and IoT devices by providing cutting-edge penetration testing solutions. Our skilled professionals have unrivalled expertise in identifying and addressing vulnerabilities, ensuring the resilience of IOT/OT and automotive systems against cyber threats. FEV Secure Lab is a trusted partner in securing the road ahead, with a passion for excellence and a commitment to advancing cybersecurity in the automotive, defense, railways and IOT industry.

For more information about our services, you can contact us fev_india@fev.com
Website: FEV Asia | India