POLAR H10 Heart rate monitor

Table of Contents

1. Introduction

1.1. Overview

This document describes the vulnerabilities observed from the security research conducted on BLE communication between Polar h10 heart rate sensor and Application.

The purpose of this research was to identify potential vulnerabilities in the BLE communication between Polar h10 heart rate sensor and Application (polar flow, polar beat).

1.2. Research Team

The security research was conducted by:

Sanyam Agarwal, Sr. Principal Security Researcher, FEV India Pvt Ltd.

Sanyam Agarwal is a Sr. Principal Security Researcher, holding a B. Tech degree in electronics and communication, has 10+ years of experience in Automotive/medical penetration testing. His core competencies lie in Penetration testing for Embedded device security, wireless security, and application security.

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's firmware with cyber security.

1.3. Methodology

Black Box testing approach was taken to make sure the BLE communication between Polar H10 heart rate sensor and application (polar flow, polar beat) was assessed against vulnerabilities from all possible security perspectives.

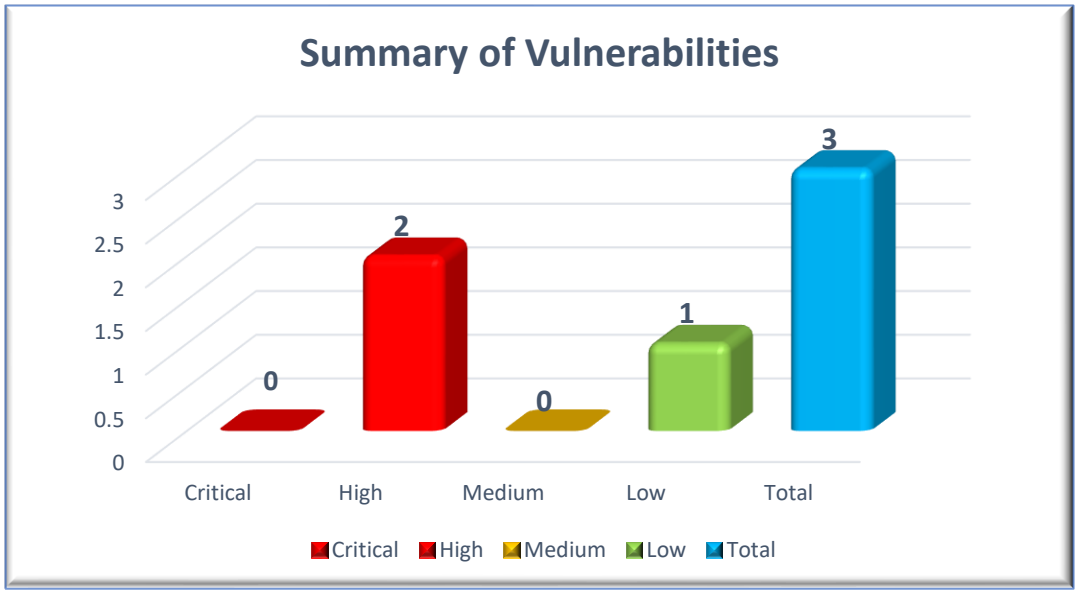
2. Summary

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

Total of **03** risks were identified during the test.

Target	Total Vulnerabilities				
	Critical	High	Medium	Low	Total
Counts	0	2	0	1	3

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



Vulnerability Risk Summary Graph

Vulnerability ID	Vulnerability	Severity
BLE_VUL_01	Polar h10 heart rate sensor Bluetooth services cloning.	**HIGH**
BLE_VUL_02	App connected with duplicate Bluetooth advertisement module.	**HIGH**
BLE_VUL_03	Polar beat App crashed by advertising data as Bluetooth name polar h10 name	**LOW**

3. Detailed Description of the Vulnerabilities and findings

3.1. Vulnerabilities:

3.1.1. Polar h10 heart rate sensor Bluetooth services Cloning.

Vulnerability Description:

During the observation and enumeration of BLE communication between Polar h10 heart rate sensor and application, found the service handler which is used to send ***"Heart rate"*** and ***"Battery Percentage"*** data. An attacker can easily clone this service handler, manufacturer data.

Technical Impact:

By exploiting this vulnerability an attacker can clone heart rate and battery percentage service and send the random heart rate and battery percentage.

Test Methodology:

Prerequisite: Using BLE scanner scan near by all BLE device and identify polar h10 heart rate module and it's MAC Address.

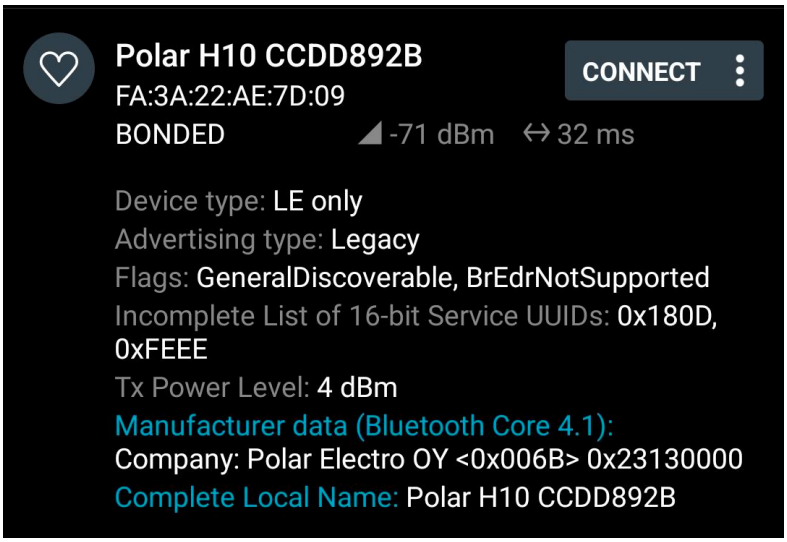


Figure 1: Scan nearby BLE device, Identify Polar H10 and Info

1. First scan for Polar H10 Heart Rate BLE Advertisement and try to connect it, once it connected with attacker tool, identify service handlers which send heart rate data and battery percentage data.

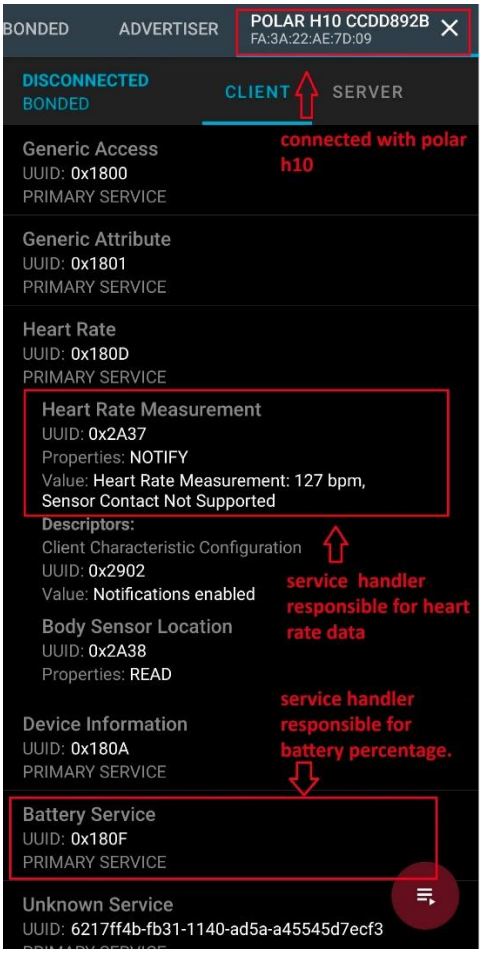


Figure 2: Connected with Polar H10 and Identify Services

2. Make a GATT server and add this heart rate and battery percentage services on server and add a manufacture data etc. Now start advertisement of this cloned module.

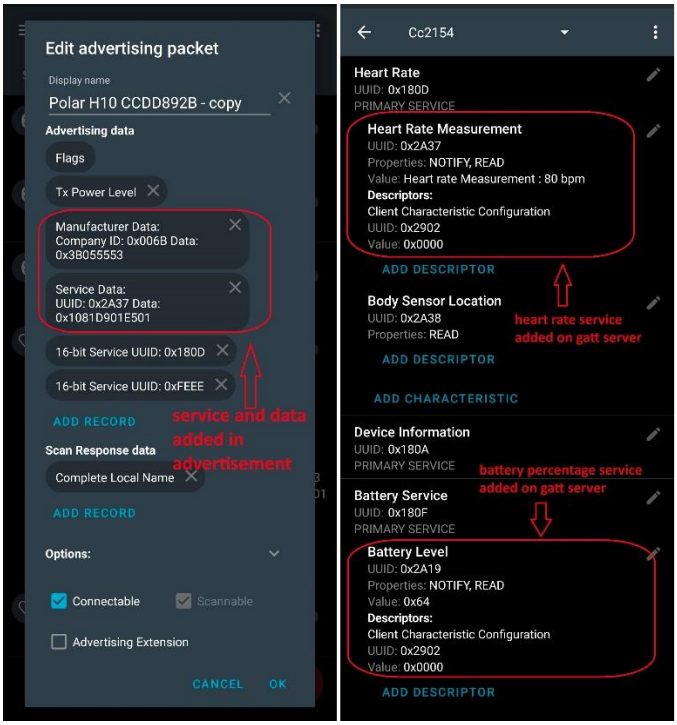


Figure 3: Clone Advertisement and Service Handle

3. As soon as advertisement starts, Attacker module name displayed in **Polar Flow** and **Polar Beat** Mobile Application.

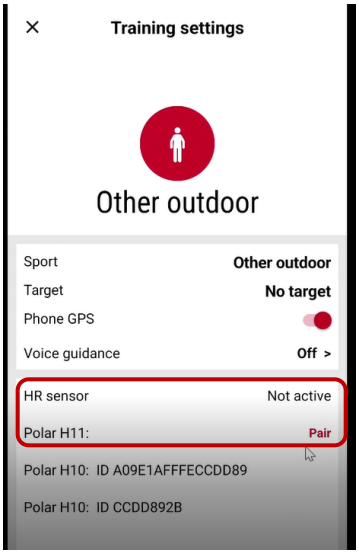


Figure 4: Attacker module name Polar H11

4. If user get paired to Attacker module. Attacker can send Fuzz/forged data over Bluetooth communication for Heart rate and Battery percentage.

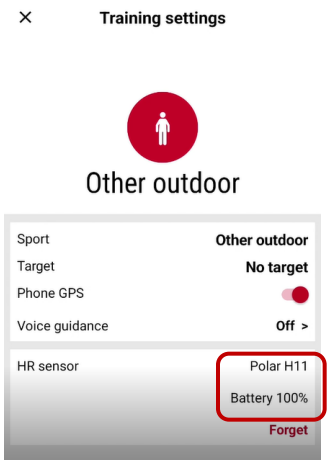


Figure 5: Mobile APp conencted with Fake GATT server with name Polar H11

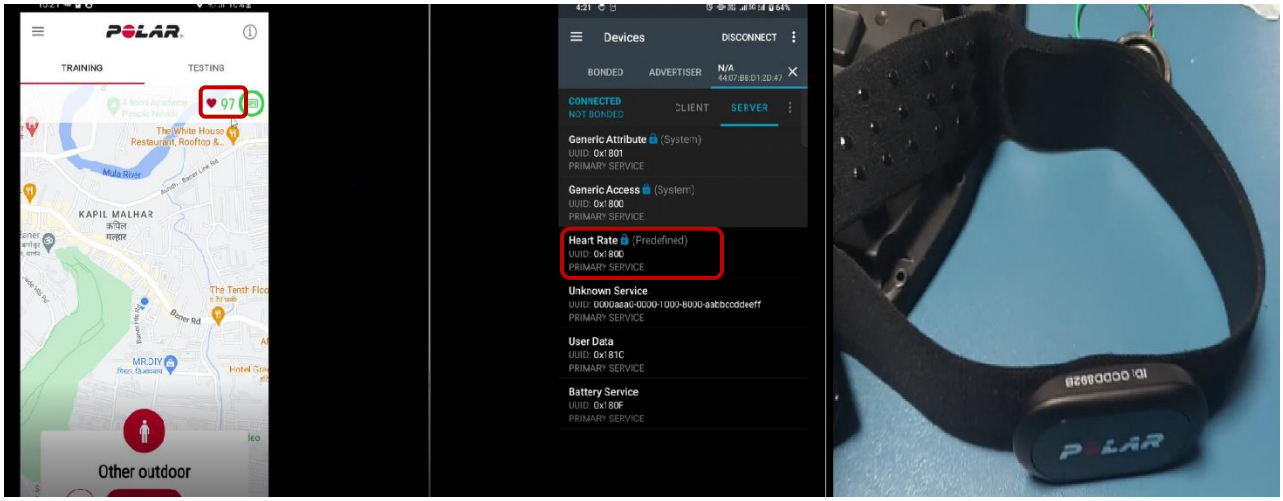


Figure 6: Left side Hear beat "97" crafted by an attacker by exploiting service handle. Attacker can send any forged data. Also at the Right side of the image Polar device is not connected as well as not stick to any human.

Remediation:

Add Authentication mechanism between Device and Mobile App.
Encrypt the communication between device and App.

CVSS Score:

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

CVSS Base Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H **Base Score: 8.0**

3.1.2. Mobile App connected with duplicate Bluetooth advertisement module.

Vulnerability Description:

During the observation and enumeration of BLE communication between Polar H10 Heart rate sensor and Mobile application. We found that if any BLE device have same MAC address and advertisement data then Mobile app doesn't have any authentication mechanism to find out whether device is duplicate or real.

Technical Impact:

By exploiting this vulnerability an attacker can create a duplicate device with same MAC address and create a GATT server with same Service Id and send random / fake data to the application (polar flow, polar beat).

Test Methodology:

Prerequisite: Using BLE scanner scan nearby all BLE device and identify Polar H10 heart rate module and it's MAC Address.

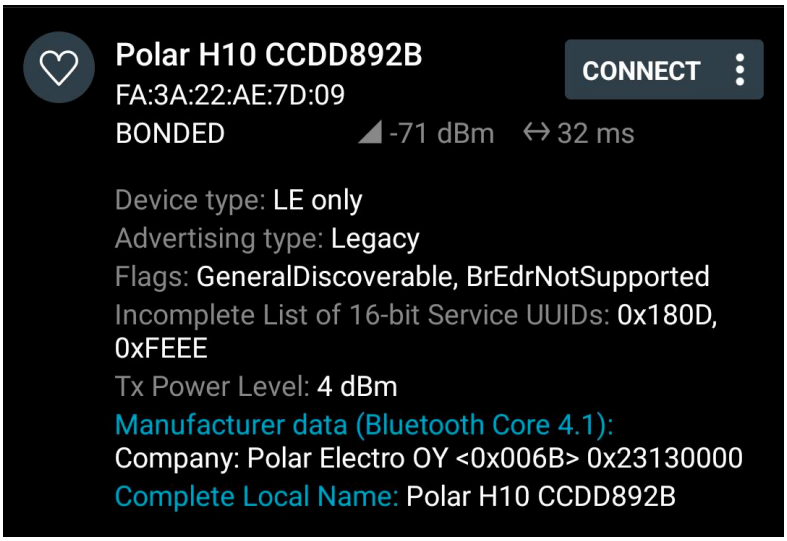


Figure 7: Scan Nearby BLE device and Identify Polar H10

1. First scan for Polar H10 BLE advertisement and decode/understand type, value, length of data, service UUID, Manufacturer details.

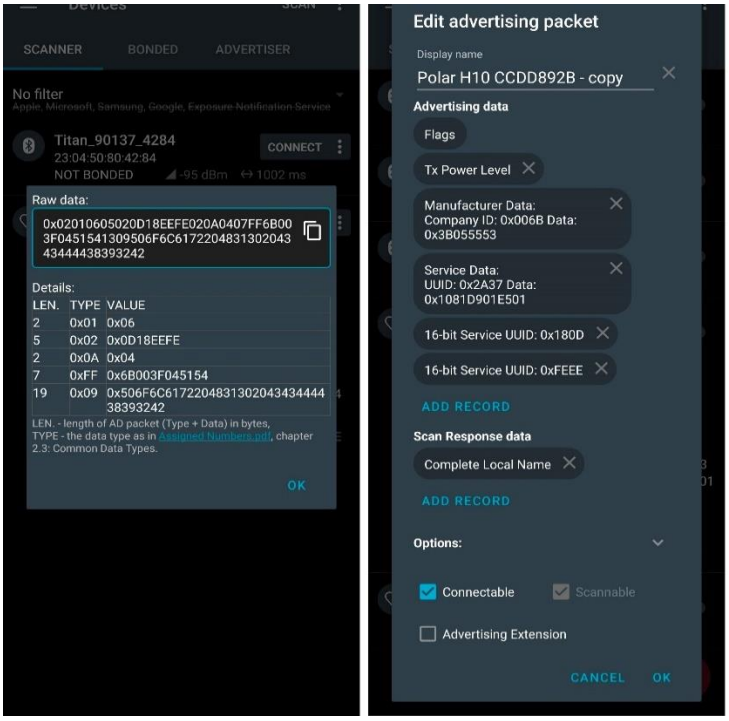


Figure 8: Observation

2. Created custom code and hardware. The objective is to have same MAC address (FA:3A:22:AE:7D:09) of the hardware as per Polar H10 MAC address and Device Name "**Polar H10**". Start BLE advertisement with same type, service UUID, Value, Manufacture data.

3. As soon as advertisement start User get duplicate module in scanning result of polar flow and polar beat application and user able to connect with this duplicate module too.

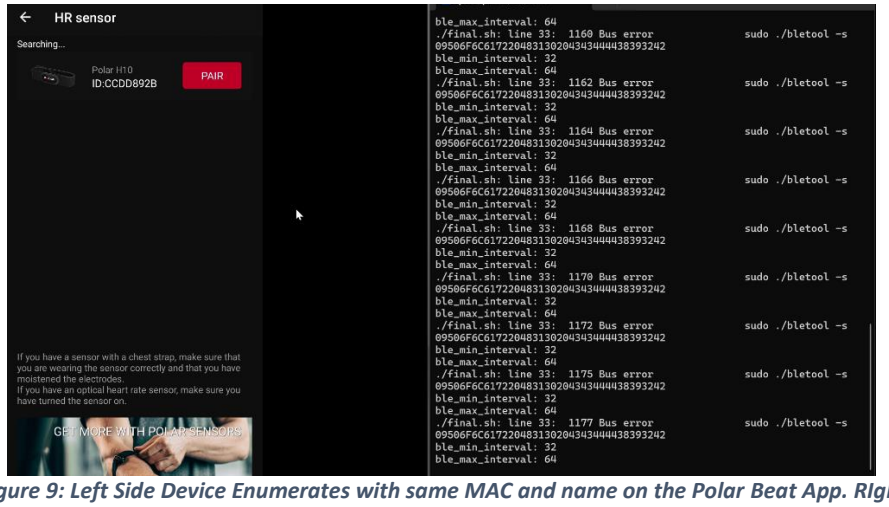


Figure 9: Left Side Device Enumerates with same MAC and name on the Polar Beat App. RIght side is the Custom code runs on BLE dongle which exploits Device name, MAC address and advertisement data

Remediation:

Add mechanism to hide the manufacture data and service UUID.
Add authentication mechanism between Mobile App and legitimate device.

CVSS Score:

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

CVSS Base Vector: AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H **Base Score: 8.0**

3.1.3. Polar beat App crashed by advertising data as Bluetooth name Polar H10 name.

Vulnerability Description:

During the observation and enumeration of BLE communication between Polar h10 heart rate sensor and application (Polar Beat). We identified the weakness related to Bluetooth name and MAC address. With different MAC address and same Bluetooth name as per Polar H10 device the "Polar Beat" app is getting crashed and not available for communication. if user try to connect with device through Polar Beat app then the app will get crashed

Technical Impact:

By exploiting this vulnerability an attacker can make Mobile App (Polar Beat) non-operational.

Test Methodology:

Prerequisite: Using BLE scanner scan nearby all BLE device and identify polar h10 heart rate module and it's MAC Address.

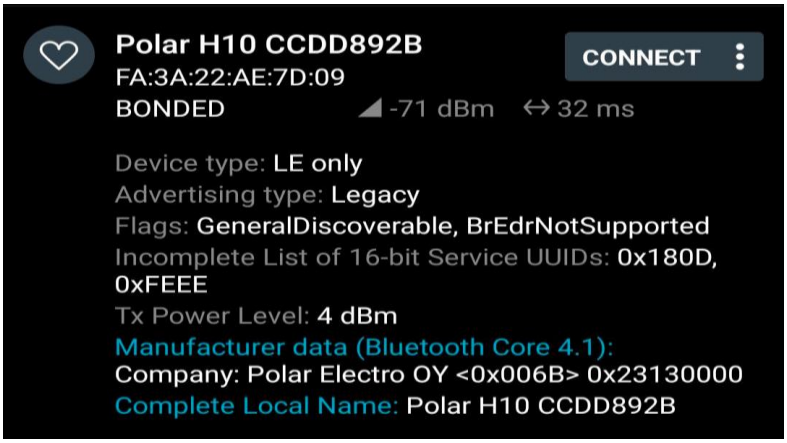


Figure 10: Scan nearby device and Idenfiy Polar H10 device

1. First scan for Polar H10 heart rate BLE advertisement and try to connect it, once it connected with attacker tool, clone the advertisement data.

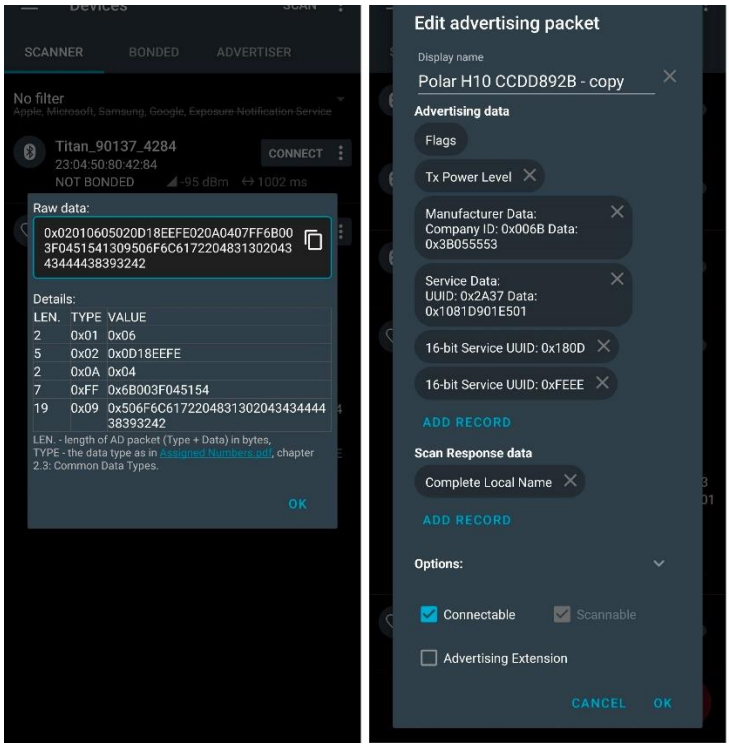


Figure 11: Clone Advertisement Data

2. Now change a Bluetooth name as a Polar H10 and start advertisement as soon as advertisement starts after that if any user tries to scan a device with Polar beat application, then polar beat application gets crashed.

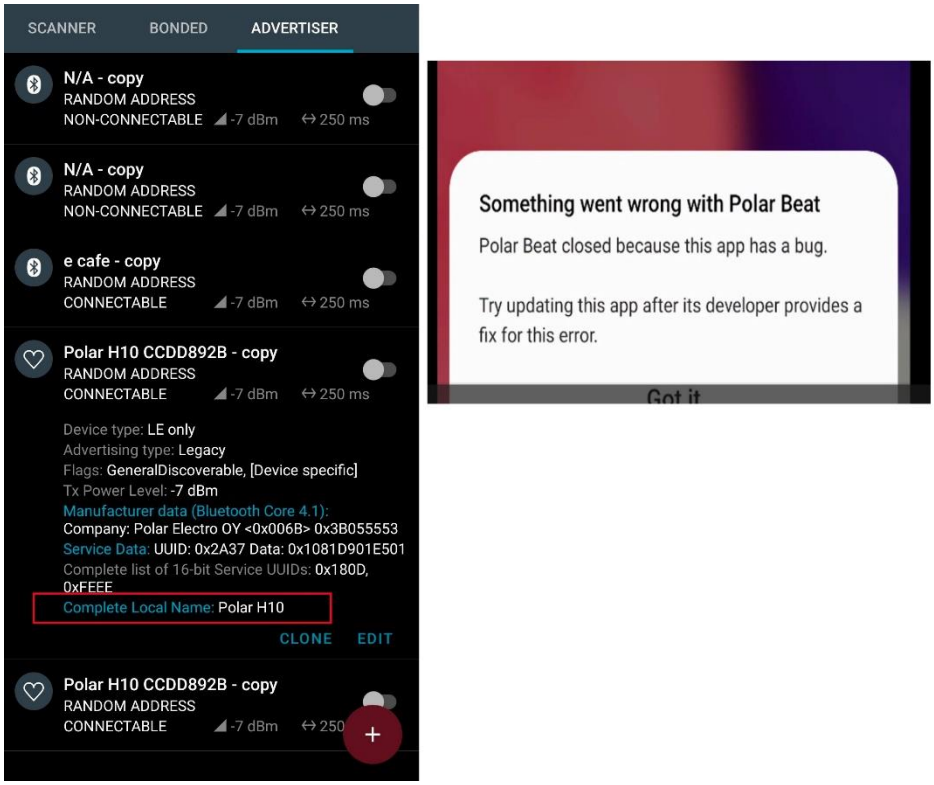


Figure 12: Polar beat App crashed

Remediation:

Add mechanism where manufacture data and service UUID can be hide and encryption of data, add authentication mechanism between app and device so device do not connect with other apps.

CVSS Score:

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

CVSS Base Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L Base Score: 3.3

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