29/**03/2024**

Agasta

Product Security Assessment Report

Sanketlife 2.0 Pocket 12-Lead ECG Monitor

Fw Version : 3.0

Company Details

Company Name	Agasta
Email	care@agasta.com

Document History

Version	Date	Author	Remark
1.0	29/03/2024	Yashodhan Mandke	First Draft

Security Assessment Details

1.1 Executive Summary

Security Assessment of Sanketlife 2.0 Pocket 12-Lead ECG Monitor has been performed, considering below common security issues:

- ✔ If any Wireless security issues identified

Overall security postures of the device are good, though some of the security controls/measures have not been properly thought of/implemented during the design and coding of the application.
The security assessment revealed **1 critical severity** security issue a in this product in the scope of security assessment.

The consolidated summary of the assessment has been presented in the Executive Summary section. Additional information is contained within the Detailed Vulnerability Information section of this report.

1.2 Scope and Objectives

The scope of this assessment was limited to Bluetooth Low energy (BLE) Communication of Sanketlife 2.0 Pocket 12-Lead ECG Monitor.

1.3 Technology Impact Summary

The security assessments on the BLE communication has been performed. These assessments aim is to uncover any security issues in the assessed Sanketlife 2.0 Pocket 12-Lead ECG Monitor, explain the impact and risks associated with the found issues, and provide guidance in the prioritization and remediation steps.
Following are technical impact.

- ► An attacker can create denial of service, bypass device authentication, device authorization and also able to read the information from the BLE by performing BLE Device Impersonation and Unauthorized Access attack

1.4 Business Impact Summary

Following is the business impact

- Due to BLE attack the customer suffers from unavailability of service that may reduce reputation of product in market
- Impersonation of device
- Loss of competitive advantage
- Patient safety risk
- Operational Disruption

1.5 Testing Environment and Tools

To carry out wireless assessment on BLE hardware tools such as android phone and software tool such as nrf connect application has been used. Also Ubuntu machine with GATTTOOL has been used.

1.6 Table of Findings

Vulnerability ID	Scope	Finding	CVSS Score	CVSS String	Severity	Stauts
SL-P12LEM-01	Wireless - BLE	BLE Device Impersonation and Unauthorized Access	9.6	CVSS:3.1/ AV:A/ AC:L/ PR:N/UI:N/ S:C/C:L/ I:H/A:H	CRITICAL	Not Fixed

1.7 Device Strengths

N.A. (The scope of assessment was only BLE, so other device security strengths are not assessed during the release of the report)

1.8 Device Weakness

The below mentioned vulnerabilities were identified during the process of Wireless communication.

- The BLE stack and BLE authentication is vulnerable to attack

Technical Findings

2.1 SL-P12LEM-01: BLE Device Impersonation and Unauthorized Access

Potential Impact : CRITICAL

Description :
A BLE Device Impersonation and Unauthorized Access attack is a type of cyber attack that targets wireless BLE networks, causing a loss of connectivity and potentially interrupting service for connected devices, also it connects the BLE device to unauthorized user without authentication. The confidentiality, integrity and availability of device is compromised with this attack.
During the assessment it was identified that whenever this attack is launched the device can not be accessed by its original application resulting in denial of service of heart rate measurement.

Affected Hosts : BLE Stack, Agasta Sanketlife Android Application, Device Connectivity & Control.

Technical Risk : The unavailability of device control via application, unauthorized access, unauthenticated device

Business Risk : Customer is unable to connect the device to application resulting in customer complaints, loss of reputation etc.

Mitigation :Device Authentication

Steps to Reproduce:

1. Turn on the Sanketlife 2.0 Pocket 12-Lead ECG Monitor
2. Scan the device using NRF connect prior to connecting to its official application. (Attacker can be in scanning mode ans can immediately connect to device). The BLE address of the device under security assessment is DC:FB:99:94:82:CF
3. Connect the device toi NRF connect and read all parameters from BLE service of device

Generic Access
UUID: 0x1800
PRIMARY SERVICE

Device Name
UUID: 0x2A00
Properties: READ, WRITE
Value: Sanket 2AD

Appearance
UUID: 0x2A01
Properties: READ
Value: [0] Unknown

Peripheral Preferred Connection Parameters
UUID: 0x2A04
Properties: READ
Value: Connection Interval: 15.00ms - 15.00ms,
Slave Latency: 0,
Supervision Timeout Multiplier: 100

Generic Attribute
UUID: 0x1801
PRIMARY SERVICE

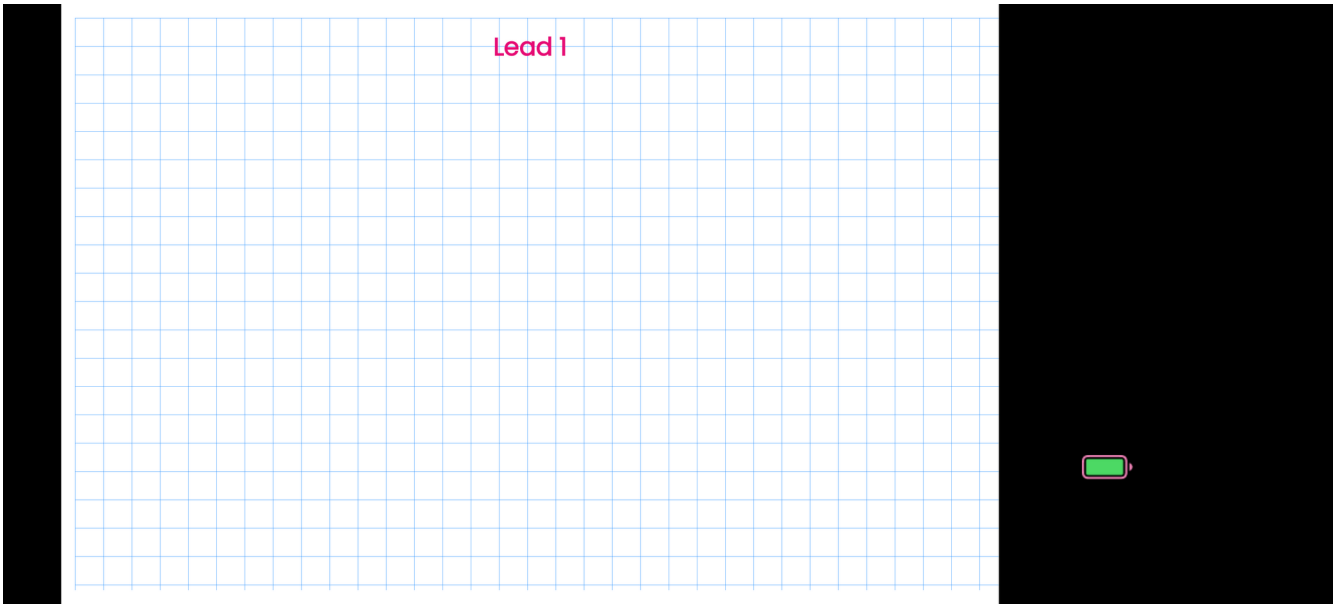
Unknown Service
UUID: 0xFFB1
PRIMARY SERVICE

Unknown Characteristic
UUID: 0xFFB2
Properties: NOTIFY, READ, WRITE
Value: (0x) 94-05-7F-05-7C-05-85-05-88-05-88-05-76-05-6D-05-58-05-49-05
Descriptors:
Client Characteristic Configuration
UUID: 0x2902
Value: Notifications and indications disabled

Battery Service
UUID: 0x180F
PRIMARY SERVICE

Battery Level
UUID: 0x2A19
Properties: NOTIFY, READ
Value: 96%
Descriptors:
Client Characteristic Configuration
UUID: 0x2902
Value: Notifications and indications disabled

4. Start and log in to Sanketlife mobile application, try connecting device which fails as device already connected to unauthorized device as shown in below figure



################ End of Document ####################