24/08/2024

Firebolt

Product Security Assessment Report

Fireboltt Artillery Smart watch

Fw Version : NJ-R6E-10.3

Company Details

Company Name	Firebolt
Email	infocare@boltt.com

Document History

Version	Date	Author	Remark
1.0	24/08/2024	Harish Manam	First Draft

Security Assessment Details

1.1 Executive Summary

Security Assessment of Fireboltt Artillery Smart Watch 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 HIGH 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 Fireboltt Artillery Smart Watch.

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 Fireboltt Artillery Smart Watch., 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
- 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.

1.6 Table of Findings

Vulnerability ID	Scope	Finding	CVSS Score	CVSS String	Severity	Status
FB-ART-SW-01	Wireless - BLE	BLE Device Unauthorized Access	8.2	CVSS:3.1/ AV:A/ AC:L/ PR:N/UI:N/ S:C/C:L/ I:N/A:H	HIGH	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 FB-ART-SW-01: BLE Device Unauthorized Access

Potential Impact : HIGH

Description :
A BLE Device 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.
Affected Hosts : BLE Stack, FB-Active Android Application, Device Connectivity & Control.

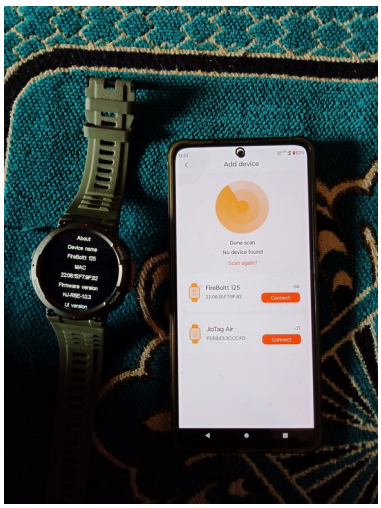
Technical Risk : The unavailability of device control via application, unauthorized access, unauthenticated device

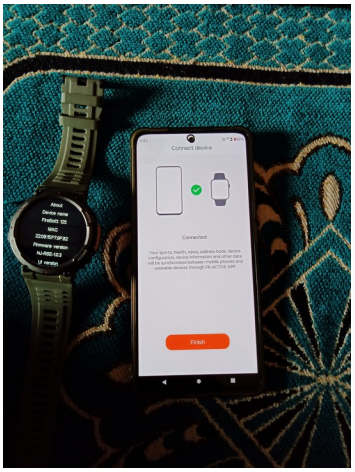
Business Risk : Customer is unable to connect the device to application resulting in customer complaints, loss of reputation etc.

Mitigation :Device Authentication and authorization

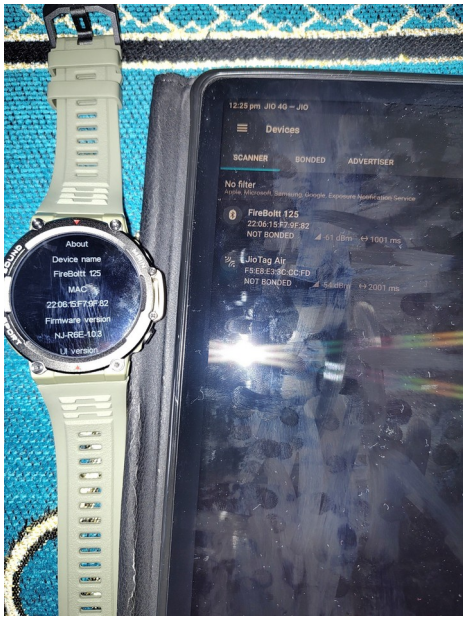
Steps to Reproduce:

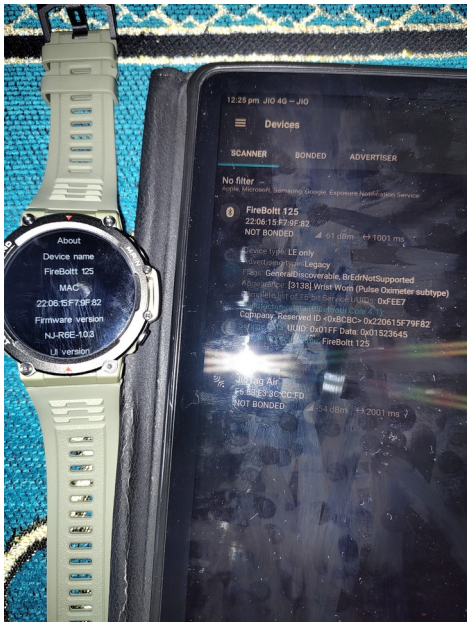
1. Turn on the Fireboltt Artillery Smart Watch.
2. Scan and pair the device with FB-Active mobile application. The device BLE address is 22:06:15:F7:9F:82

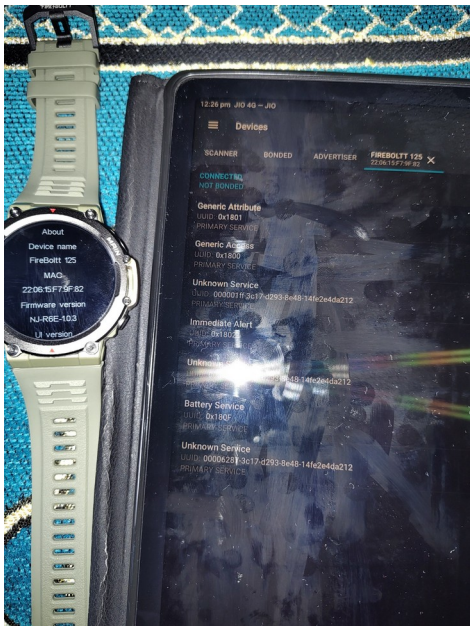




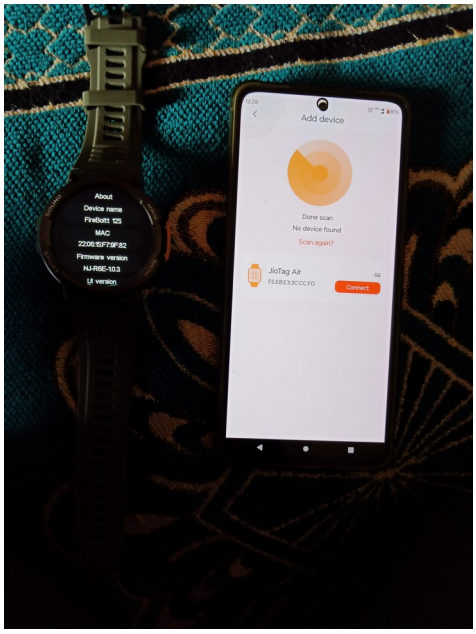
3. Now disconnet the BLE and unpair the device to create attack scenario
4. Scan the device using NRF connect prior to connecting to its official application. (Attacker can be in scanning mode ans can immediately connect to device). The device is now connected to NRF application







5. Now scan the device with FB-Active application, where it can not connects since its already paired with another device running NRF application causing denial of service as shown below.



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