22/01/2024

Fireboltt

Security Assessment Report

Fireboltt Dream Wristphone
Fw Version : BSW202_FB_AAC_v2.0_20240110-20240110-1956

Company Details

Company Name	Fireboltt
Email	infocare@boltt.com

Document History

Version	Date	Author	Remark
1.0	21/01/2024	Yashodhan V.	First Draft

Security Assessment Details

1.1 Executive Summary

Security Assessment of Fireboltt Dream Wristphone model 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 Wi-Fi Communication of Fireboltt Dream Wristphone

1.3 Technology Impact Summary

The security assessments on the Wi-Fi communication has been performed. These assessments aim is to uncover any security issues in the assessed Fireboltt Dream Wristphone, 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 by performing Wi-Fi Deauth attack on the device

1.4 Business Impact Summary

Following is the business impact

- Due to Wi-Fi deauth attack the customer suffers from unavailability of service that may reduce reputation of product in market
- Also if critical application is user working on gets

1.5 Testing Environment and Tools

To carry out wireless assessment on Wi-Fi hardware tools such as ESP8266 deauther and software tool has been used

1.6 Table of Findings

Vulnerability ID	Scope	Finding	CVSS Score	CVSS String	Severity	Stauts
FB-DRMWP-01	Wireless	Wi-Fi Deauth Attack (DoS Attack)	7.5	CVSS:3.0/ AV:N/ AC:L/ PR:N/UI:N/ S:U/C:N/ I:N/A:H	High	Not Fixed

1.7 Device Strengths

N.A. (The scope of assessment was only Wi-Fi, 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 Wi-Fi stack is vulnerable to Deauth attack

Technical Findings

2.1 FB-DRMWP-01: Wi-Fi Deauth Attack

Potential Impact : High

Description :
A WiFi deauthentication attack is a type of cyber attack that targets wireless networks, causing a loss of connectivity and potentially interrupting service for connected devices.
During the assessment it was identified that whenever the Wi-Fi Deauth attack has been launched the Fireboltt Dream Wristphone is unable to access internet resources even though it is connect to Wi-Fi and accessing the internet contents.

Affected Hosts : Wi-Fi Stack, Device Connectivity & Control

Technical Risk : The unavailability of device control via application

Business Risk : Customer device connected to the smart plug are affected which in turn affects control of peripherals and reputation loss for product.

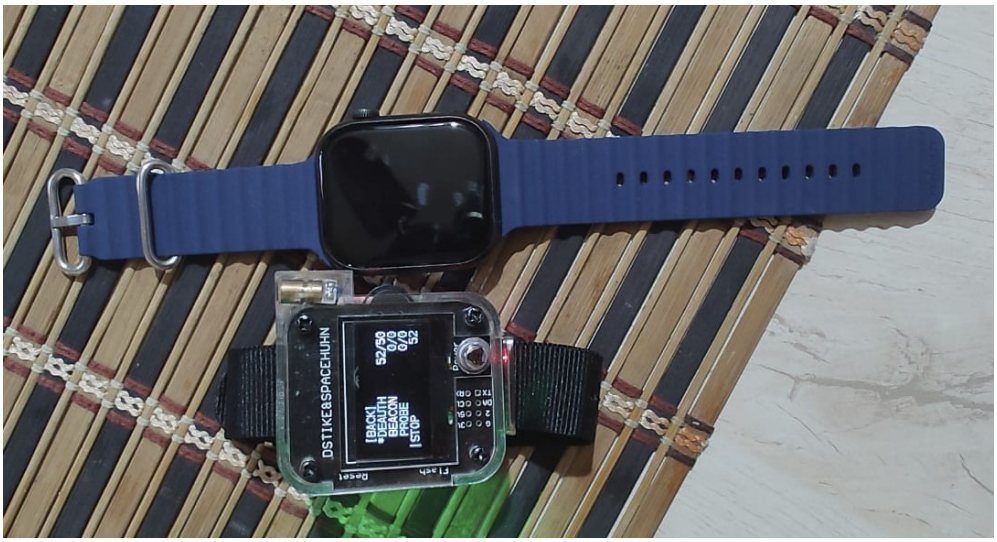
Mitigation : Use of 802.1X authentication can help protect device from WiFi deauthentication attacks by requiring a user to authenticate before connecting to the network.

Steps to Reproduce:

1. Turn on the Fireboltt Dream Wristphone and connect to the Wi-Fi Access point.
2. Set up ESP8266 Deauther watch and scan the MAC address of all stations.
3. The Wi-Fi MAC address of the Fireboltt Dream Wristphone under security assessment is b0:f2:7c:58:4d:38
4. Initially the device is connected to wifi access point, also youtube is accessible over the wristphone as shown below

5. The image below shows the last digits of mac address scanned by wifi deauther watch

6. Select the Deauth mode in deauther watch and launch of the deauth attack



7. Once the attack has been launched, the Wi-Fi access of the Wristphone is disabled

8. After the attack the device can not access the internet

9. After this attack Wi-Fi control of device is lost

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