AIRTH SMART HOME AQI MONITOR VULNERABILITY

CVE-2025-67399

Prepared by: Rupesh B. Surve

Contents

1. Introduction

1.1 Product Overview

The AIRTH Smart Home AQI Monitor is a Wi-Fi–enabled indoor air quality device designed for 24×7 monitoring of the air you breathe, primarily measuring PM2.5/PM10 particulate pollution along with temperature and humidity, and displaying the data on a clear digital LED screen as well as on a smartphone app via Wi-Fi. It is intended for home or office use to give real-time awareness of indoor pollution levels, helping users decide when to ventilate rooms or use air purifiers, and is best suited for tracking air quality trends and day-to-day changes rather than professional-grade environmental analysis.

1.2 Research Team

This research was carried out by **Rupesh B. Surve**, an IoT Security researcher with over 5 years of professional experience in hardware-level Pen-testing and 10 years of experience in Embedded Product Development.

1.3 Methodology

Testing involves Identification of chip using datasheet. Identification of UART port and Baud Rate by scanning port using suitable tools. Which reveals that the UART port of Bluetooth chip is open to access.

Further, Suitable tool like USB to TTL convertor is connected to this UART port and connected to PC. Using Chip's dedicated programming software whole memory of the chip is extracted.

2. Summary

Below table lists the total vulnerabilities identified during the assessment.

Vulnerability Category	Count
High Severity Vulnerabilities	0
Medium Severity Vulnerabilities	1
Low Severity Vulnerabilities	0
Informational Vulnerabilities	0
Total	**1**

Table – 1: Total Vulnerability Identification

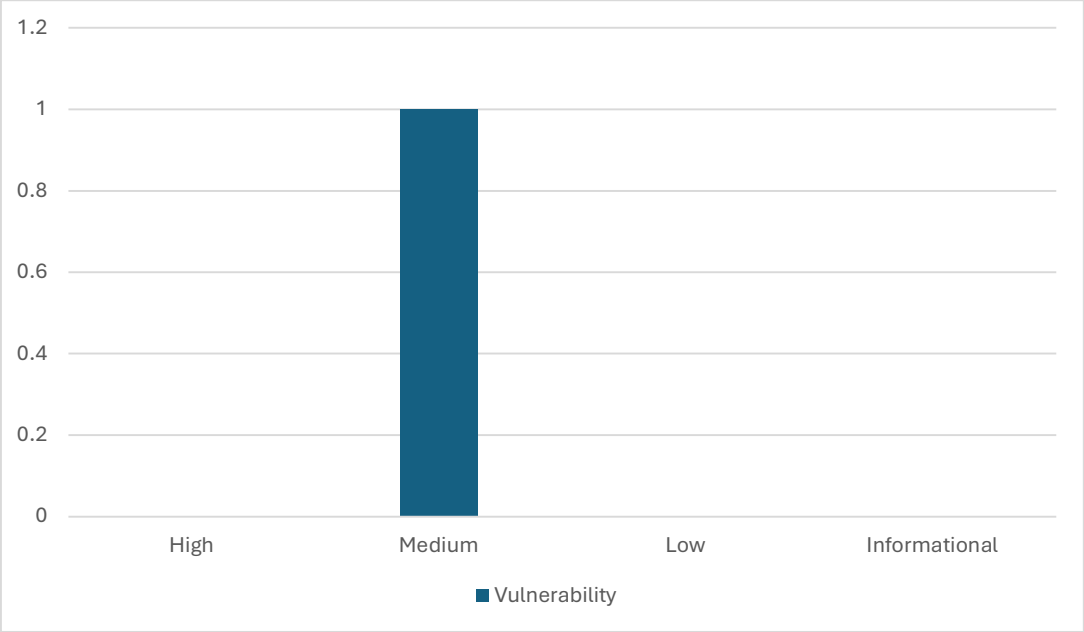


Table – 2: Vulnerability Distribution Bar Graph

Vulnerability ID	Vulnerability	Severity
VUL-001	Open UART port leading to unauthorized access to the internal flash code	Medium

3. Detailed Description of the Vulnerability

3.1 Description:

The AIRTH Smart Home AQI Monitor contains a Bluetooth-enabled system-on-chip (SoC) identified as CB3S, which internally uses the BK7231N chipset. Through physical inspection of the device, the internal SoC was exposed and its part number identified.

Using the publicly available BK7231N datasheet, the UART (TX/RX) debug/programming pins on the chip were identified. Physical access to these pins was achieved by directly connecting them to a USB-to-TTL serial converter, which was then interfaced with a PC.

The vendor-provided software used for communication with the BK7231N chipset was installed and executed. Through this interface, unrestricted read access to the chip's memory was obtained. This allowed the complete firmware and memory contents of the device to be dumped without any form of authentication, encryption, or debug interface protection (such as read-out protection, secure boot enforcement, or disabled debug interfaces).

The vulnerability arises from the lack of hardware-level security controls to prevent unauthorized access to the UART/debug interface and unrestricted firmware extraction.

3.2 Impact:

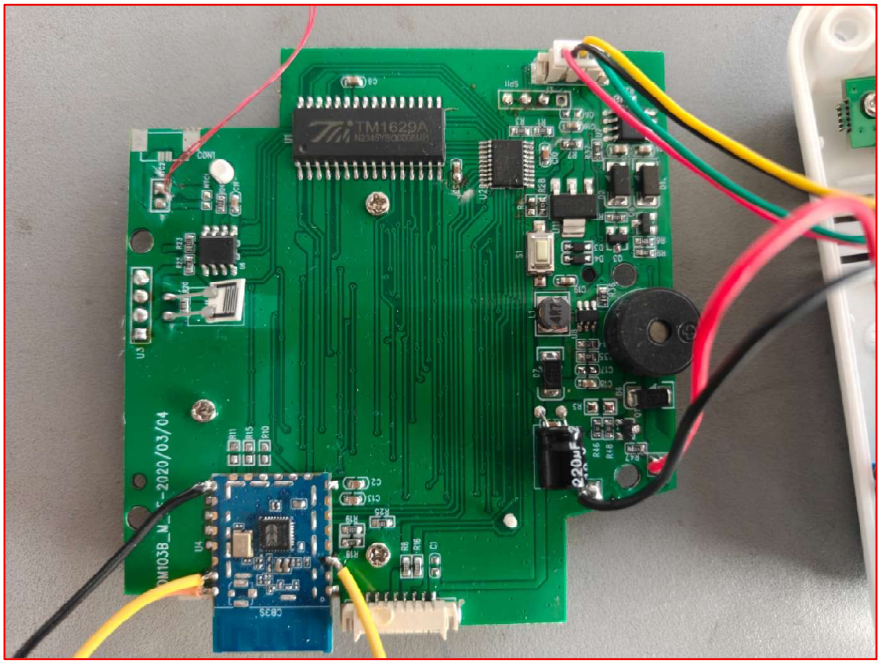
This vulnerability allows an attacker with physical access to the device to fully extract the firmware and internal memory contents. As a result:

- **Firmware Intellectual Property Exposure**: Proprietary firmware, algorithms, and implementation details can be copied, reverse engineered or reused.
- **Credential and Key Disclosure**: Sensitive data potentially stored in firmware or memory (such as Wi-Fi credentials, encryption keys, or API tokens) may be exposed.
- **Device Cloning and Counterfeiting**: Extracted firmware can be flashed onto other hardware, enabling unauthorized device replication.
- **Firmware Modification and Malicious Reprogramming**: Attackers could modify the firmware to introduce malicious functionality, persistent backdoors, or altered device behaviour.
- **Loss of User Privacy**: Modified firmware could silently collect or transmit sensor data or network information without user consent.

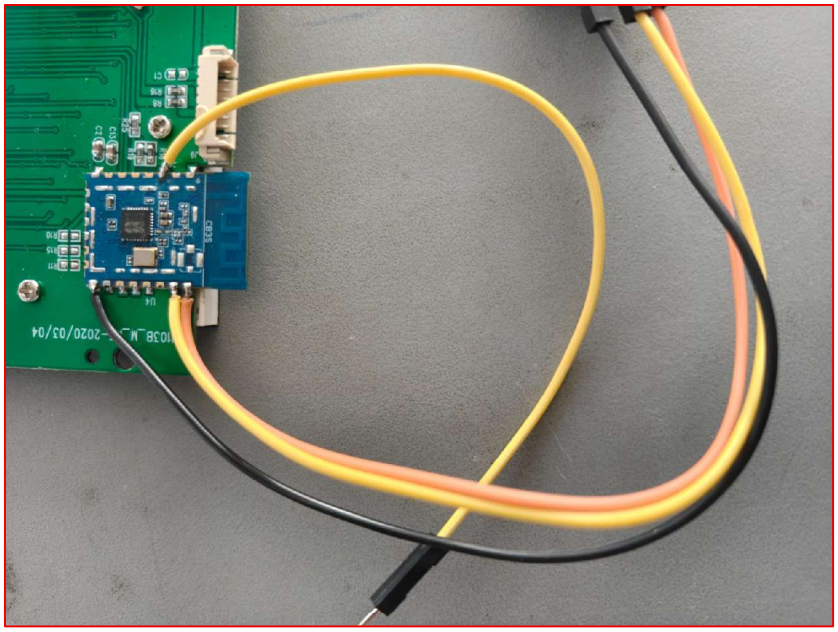
While exploitation requires physical access, the absence of basic hardware security protections significantly lowers the barrier for firmware compromise and poses a serious risk to device security and intellectual property.

3.3 Steps to reproduce:

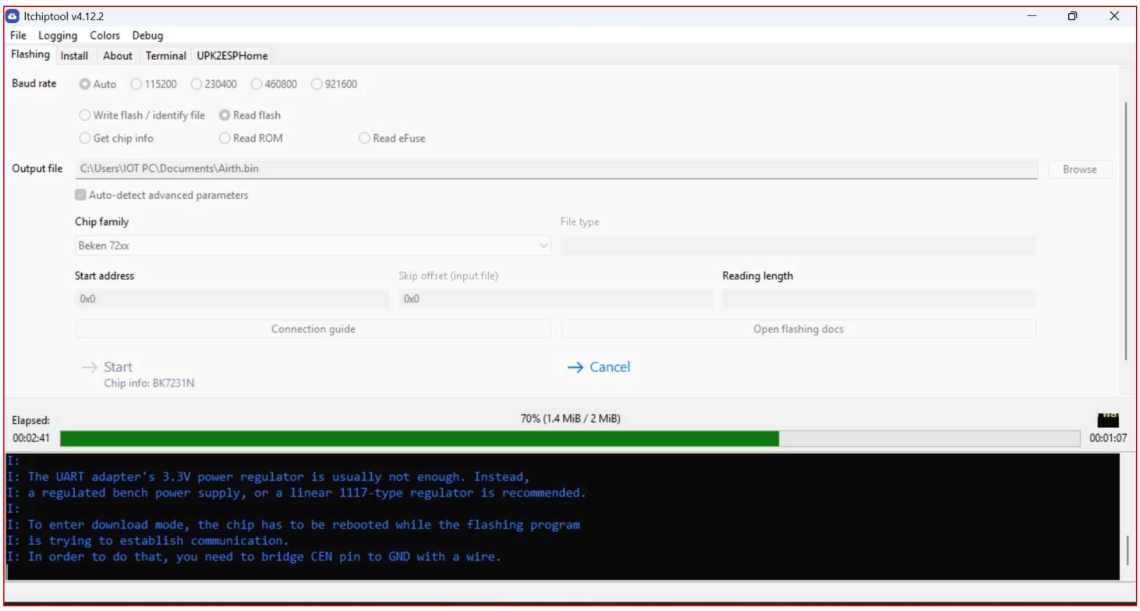
1. Open the device and do basic reconnaissance. Find out the part numbers of the IC's and their respective datasheets.



2. Try to look for the Test Points or pads, which might be the suspected port pins. (in this case, no test points were observed on PCB).
3. Now desolder the outer covering of Bluetooth module U4 and get access of internal circuit.
4. Check for the datasheet of its chip BK7231N on internet, its easily available.
5. Find out its UART or programming pins and connect jumper cable to it.



6. Download BK7231N's programming software, which is again available on internet and install it in laptop.
7. Now connect Rx. Tx and GND of BK7231N chip to USB to TTL chip and connect this tool to Laptop.
8. Run the software, select target chip.
9. Check on "Read Flash" and press START.
10. To put the BK7231N in to programming mode you need to connect its EN pin to GND for 2 seconds. At the same time your software is trying to connect to this chip.
11. As soon as chip EN pin is connected to GND, software will automatically connect to target chip and it will start reading the memory.



3.4 CVSS Scoring:

Overall CVSS Score: 6.8

CVSS 3.1 Vector: AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H