مجلس الأمن السيبراني

CYBER SECURITY COUNCIL

United Arab Emirates

Critical Bluetooth Headphone Vulnerabilities in Airoha-Based Devices

Tracking #:432318193

Date:30-12-2025

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed Security researchers has disclosed three critical vulnerabilities affecting Bluetooth audio devices built on Airoha Bluetooth System-on-Chip (SoC) platforms.

TECHNICAL DETAILS:

Security researchers has disclosed three critical vulnerabilities affecting Bluetooth audio devices built on Airoha Bluetooth System-on-Chip (SoC) platforms. These vulnerabilities allow unauthenticated attackers within Bluetooth range to connect to affected headphones and earbuds without user interaction, abuse a powerful factory-debug protocol, extract cryptographic keys, and ultimately impersonate trusted headphones to compromise the user's smartphone.

Vulnerability Details:

1. **CVE-2025-20702**
   - Severity: Critical
   - Description:
     - Unauthenticated access to the RACE diagnostic protocol allows full device compromise, including memory access and credential extraction.
   - Affected Chipsets:
     - AB156x series
     - AB157x series
     - AB158x series
     - AB159x series
     - AB1627
   - Affected Software Versions:
     - Airoha IoT SDK for BT Audio v5.5.0 and earlier
     - Airoha AB1561x / AB1562x / AB1563x SDK v3.3.1 and earlier

2. **CVE-2025-20700**
   - Severity: High
   - Description:
     - Missing authentication on BLE GATT services exposes critical RACE protocol data, allowing unauthorized remote access without user interaction.
   - Affected Chipsets:
     - AB156x series
     - AB157x series
     - AB158x series
     - AB159x series
     - AB1627
   - Affected Software Versions:
     - Airoha IoT SDK for BT Audio v5.5.0 and earlier
     - Airoha AB1561x / AB1562x / AB1563x SDK v3.3.1 and earlier

3. **CVE-2025-20701**
   - Severity: High
   - Description:

  - Bluetooth Classic allows unauthorized pairing in non-pairing mode, enabling remote privilege escalation without user consent.
- Affected Chipsets:
  - AB156x series
  - AB157x series
  - AB158x series
  - AB159x series
- Affected Software Versions:
  - Airoha IoT SDK for BT Audio v5.5.0 and earlier
  - Airoha AB1561x / AB1562x / AB1563x SDK v3.3.1 and earlier

Chained Attack: "Headphone Jacking"
When all three vulnerabilities are combined, attackers can pivot from headphones to the paired smartphone.
Attack Chain

1. **Silent Connection**
   Attacker connects via BLE or Bluetooth Classic (CVE-2025-20700 / 20701)
2. **Flash Memory Extraction**
   RACE protocol used to dump flash contents (CVE-2025-20702)
3. **Credential Theft**
   Bluetooth **Link Key** for paired smartphone is extracted
4. **Impersonation**
   Attacker spoofs the headphones and connects directly to the phone

Affected Devices (Confirmed Examples)
The following devices were **verified as vulnerable** during research (non-exhaustive list):

- **Sony:**
  WH-1000XM4 / XM5 / XM6, WF-1000XM3 / XM4 / XM5, LinkBuds S
- **JBL:**
  Live Buds 3, Endurance Race 2
- **Marshall:**
  Major V, Acton III, Stanmore III, Motif II
- **Beyerdynamic:**
  Amiron 300
- **Others:**
  Teufel, JLab, MoerLabs, Bose (partial), EarisMax

Due to supply-chain reuse of Airoha SDKs, **many additional models are likely affected**

RECOMMENDATIONS:

- Immediately update headphone firmware via official mobile apps.
- Remove unused Bluetooth pairings from smartphones.
- Disable Bluetooth when not in use.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://www.airoha.com/product-security-bulletin/2025
- https://insinuator.net/2025/12/bluetooth-headphone-jacking-full-disclosure-of-airoha-race-vulnerabilities/