Security White Paper

> This article applies to models: BH71 Series, BH70, BH72, BH74, BH76 Plus, BH76 and BH78.

1. Overview

With the rapid development of IoT, Bluetooth technology is widely used in different fields, and enterprises are paying more and more attention to security requirements. When Yealink provides users with high-quality business Bluetooth headsets in the mixed office field, it not only pays attention to the high-quality audio experience but also pays attention to the risks brought by Bluetooth in terms of security. By practicing the best security practices of the Bluetooth industry, Yealink provides reliable headset products for end users and enterprises.

Yealink passed the GB/T 22080-2016/ISO/IEC 27001:2013 safety system certification in July 2022. ISO/IEC 27001 is an international standard for safety best practices accepted by a wide range of users, and the system certification establishes a safety implementation process for the product, and means that the company is continuously investment and optimizing.

This article explains the working principle of Bluetooth security and the security level of Bluetooth to help users and security practitioners clearly understand the security architecture and security solutions of Yealink Bluetooth headset products. This article is mainly divided into the following sections to explain: Bluetooth working principle, Bluetooth security transmission, and Bluetooth security management.

2. Bluetooth Working Principle

Bluetooth is a wireless communication technology standard that communicates

over short distances via the 2.4G wireless frequency band. By following Bluetooth security best practices, the risk of an attacker obtaining access to Bluetooth signals for eavesdropping and access control is minimal. Bluetooth requires the following security verification steps to be performed during the connection establishment process:

- Pairing: Create a shared key
- Binding: Store the key after pairing and use it during subsequent connections to form the behavior of trusted devices
- Authentication: Verify that both sides of the Bluetooth communication have the same key
- Encryption: The information transmitted wirelessly needs to be encrypted to prevent direct theft and analysis
- Message integrity verification: prevent messages from being forged and exploited by third parties
- Secure and simple pairing: prevent passive eavesdropping and man-in-the-middle attacks

3. BLT Security Transmission

Mandatory levels in the authentication and encryption security processes are defined in the BR/EDR/HS standard.

- Security Mode 1: The device is insecure, and security features are disabled forever.
- Security Mode 2: Service-level enforced security mode, in which authentication and encryption are performed in the controller.
- Security Mode 3: Link-level enforced security mode requires all connections to be authenticated and encrypted before they can be made, so the search service cannot be performed even before authorization and encryption.
- Security Mode 4: Service-level enforced security mode, where the security feature is activated after the physical and logical connections are established. This mode uses Secure Simple Pairing (SSP), where the ECDH key protocol is used for link key generation.
  Yealink's Bluetooth devices use Bluetooth version 5.0 or later and use Security Mode 4 with a service level 3.

3.1 Pairing

The pairing process requires the device to enable Open Discover, and the user must enter Bluetooth pairing mode to complete the pairing. The Open Discover will be disabled automatically after 300S, and the Workstation can be disabled by configuring the timeout. During the pairing process, the device uses P-192 Elliptic Curve to calculate the Link Key and then creates a shared key after the pairing is completed. Only the public key will be transmitted in the wireless signal during the encryption process, and the private key will not be transmitted in the wireless signal, so the attacker cannot steal the decrypted private key.

When paired with multiple Bluetooth devices, the Link Key calculated by P-192 Elliptic Curve is one-to-one and not shared with other devices.

3.2 Binding

After successful pairing, the key is stored in both devices. While ensuring successful pairing without repeating pairing each time, Yealink’ s device has the function of disk encryption to protect the security of the key in the device. It is difficult for an attacker to obtain the key of Yealink after pairing it to simulate another device to attack and crack the data transmitted wirelessly.

3.3 Encryption

After the devices are successfully paired, Bluetooth encrypts the voice and control streams with data in the device's controller using the key between trusted devices at the time of pairing, using E0 encryption. Only the paired devices know the information necessary to perform encryption and decryption, and the key is never sent over the air. This makes it difficult for eavesdroppers to obtain any information from the data, even if they can access it.

3.4 Risk Analysis and Assessment

- Wiretapping
  Attack method: Third-party access through Bluetooth to listen to calls or use interception of wireless signals to parse out the data stream.
  Risks: High security, pairing needs to be actively triggered, requires a physical connection to get the key Low feasibility.
- Third Access Control
  Attack Method: Crack Bluetooth's identity and encrypted information through low-security authentication.
  Risk: High security. Yealink uses Bluetooth version 5.0 or later and completely removes insecure authentication methods.
- Man-in-the-middle attack
  Attack method: Control the device by message interception, tampering, and forwarding to other devices.
  Risk: High security, the attacker needs to be close to the attack target in order to implement; beyond the wireless range cannot be implemented. Actually, this type of attack is a low likelihood of implementation.

4. Security Management

4.1 Code Security Standards

Key management: The core key management adopts a dedicated and special

strategy with minimal privileges, so ordinary engineers cannot access and obtain the keys.

Code management: Yealink has strict coding security requirements inside, and every code update will review the code and perform reliability verification. Device-related code libraries have strict permission management mechanisms and requirements. It is strictly forbidden to upload to public or semi-public services such as Github, Gitee and other public code bases without permission to prevent source code leakage.

Secure Environment: Yealink's security team and IT department regularly perform static and dynamic vulnerability scans and penetration tests for both production and internal network environments to ensure that software development, firmware packaging, and device production take place in a secure network environment.

4.2 Security Emergency Response

Security has always been a priority for Yealink. Industry security technology is constantly iterating, and Yealink invests high resources every year to upgrade Yealink security level to ensure that the security level matches the current security technology. If you find a possible security issue during the use of Yealink products, you can contact us in Yealink's Security Center or submit your issue through the Ticket system. We will respond and handle the issue in a timely manner.

Security emergency response is divided into four phases: issue collection, vulnerability analysis, vulnerability repair, and tracking and resolution.

- Issue collection: Based on the feedback of security incidents, collect relevant logs and information, and arrange for dedicated personnel to follow up and deal with them.
- Vulnerability analysis: Give priority to judging the risk of vulnerabilities based on the problem, and give priority to providing temporary solutions during the processing phase to avoid the expansion of the impact of the problem.
- Vulnerability repair: analyze the root cause of the problem, trace the cause of the defects in the design, and solve the vulnerability problem from the root cause in a timely manner.
- Tracking and resolution: Check whether all product lines have the same problem, and collect the problems

from Yealink's vulnerability database for regular checking.

Technical support can visit Yealink Support for firmware downloads, product documentation, FAQ, and more. For better service, we recommend that you use the Yealink Ticket system to submit technical questions.

5. Disclaimers

5.1 Declaration

This white paper is for informational purposes only and does not grant any legal rights to any intellectual property in any Yealink product. You may copy and use the contents of this document for your internal use for reference purposes. Yealink makes no express, implied, or statutory warranties with respect to the information in this white paper. For more information about Yealink's BH7X series of headsets, you can visit Yealink's official website, and for more security-related information you can visit Yealink SECURITY & COMPLIANCE.