MeetingBar
Security White Paper

CONTENTS

1. Overview

As a global leader in communication and collaboration solutions, Yealink is committed to safeguarding user information and adheres to the principle of "Security First, User First." We strive to provide a secure product environment for customers worldwide.

This white paper focuses on the protection of user privacy and data. By integrating enterprise security management, the OWASP application security standards, and Android security best practices into our software development process, Yealink has built a comprehensive security framework. This framework is designed to continuously deliver robust security protections for Yealink device users.

Leveraging over 20 years of security expertise and incorporating industry best practices, Yealink provides secure and reliable products and services to customers across the globe. Yealink has achieved ISO/IEC 27001:2022 and SOC 2 Type 2 certifications and complies with the GDPR and other applicable regulations. For more information, please visit the Yealink Trust Center: https://www.yealink.com/en/trust-center.

ISO/IEC 27001 is the internationally recognized standard for information security best practices. Certification to this standard reflects the establishment of structured security implementation processes and demonstrates Yealink's ongoing investment in security management and product security design. The SOC (System and Organization Controls) framework, developed by the American Institute of Certified Public Accountants (AICPA), is one of the most widely adopted internal control auditing standards worldwide. The SOC 2 Type 2 audit report confirms Yealink's rigorous service controls in the areas of security, availability, confidentiality, and privacy, and affirms our ability to deliver secure and stable products and services.

This document provides an overview of Yealink's product security architecture and solutions to help users and security professionals better understand the security technologies and features embedded in Yealink products. The content is organized into the following chapters: Hardware Interface Security, System Security, Network Security, Transmission Security, Meeting Security, Data Security, Encryption, User Privacy, and Product Release Process.

Applicable Models: MeetingBar A10, MeetingBar A25, MeetingBar A40, MeetingBar A50, CTP25

2. Hardware Interface Security

2.1 Debug Interface

- Disable Debug Interfaces

Debug interfaces such as UART, ADB, and Telnet are disabled before the product leaves the factory to prevent unauthorized access and minimize the risk of data breaches.

2.2 Secure Boot

The device supports secure boot. During the boot process, the system verifies the integrity of the device using a signature public key. At every stage of startup—including the bootloader, kernel, and partition integrity—integrity verification is required. Only systems that pass the integrity check can boot normally; otherwise, the device will fail to start. The purpose is to prevent the loading and execution of unauthorized programs and to block attempts to gain device control by modifying boot parameters to access the shell environment.

Secure boot specifically includes:

- Unauthorized firmware not officially released by Yealink cannot be flashed.
- Unauthorized firmware not officially released by Yealink cannot be executed.
- Any data tampering at any stage will cause the device to fail to boot.

2.3 Trusted Storage Service

Yealink achieves physical tamper-resistant storage of cryptographic keys through a Hardware Security Module (HSM), combined with the device's Trusted Execution Environment (TEE) hardware-isolated space. Following the principle of role-based access control with hierarchical permission management, Yealink implements full lifecycle management of cryptographic keys.

At the hardware level, chip-level TrustZone technology is used to divide the processor's operating states into a Secure World (Trusted Execution Environment, TEE, also known as the trusted execution environment) and a Non-secure World (Rich Execution Environment, REE, also known as the normal execution environment).

The TEE is isolated from the operating system and other conventional software components, providing a hardware-protected secure area for sensitive code and data, thereby ensuring their confidentiality, integrity, and availability.

- **Secure Isolation**: A dedicated execution environment is established at the hardware level, separating sensitive data and code from the standard operating system and applications. This isolation ensures that content within the TEE is invisible to the external environment and subject to strict access control.
- **Encryption Protection**: Data entering or exiting the TEE is automatically encrypted and decrypted. Encryption keys and algorithms are safeguarded by hardware within the TEE. Even if data is intercepted during transmission or storage, it cannot be decrypted without access to the secure keys, thereby ensuring confidentiality.
- **Secure Storage**: Sensitive data and encryption keys are stored within the TEE. This storage area uses hardware-based encryption to prevent unauthorized access to data at rest.

The PKI management system adopts a two-tier CA architecture supplemented by Hardware Security Modules (HSMs) to protect cryptographic keys:

- **Network Isolation**: Key generation and key injection are strictly performed within the production environment. At the same time, stringent network isolation is enforced in the production environment to restrict access at the network level.

- **Authentication Measures**: The production environment follows the principle of least privilege, combined with Ukey-based two-factor authentication, ensuring that only authorized personnel can access servers to perform cryptographic operations, thereby reducing security risks.

- **Key Management**: Shamir's Secret Sharing technology, together with supervised operational procedures, is employed to ensure the security of root keys while providing high availability assurance.

Applicable Models: MeetingBar A25, MeetingBar A40, MeetingBar A50, CTP25

2.4 External Storage Security

When mounting USB partitions, security parameters are applied to prevent executable permissions from being granted to programs or scripts stored on external media (such as SD cards, USB drives, or network storage). This mechanism blocks unauthorized execution of potentially unsafe scripts or programs from external partitions.

3. System Security

3.1 MDEP Security Standardized Platform

The devices are based on solutions developed on the Microsoft Device Ecosystem Platform (MDEP). By design, they deeply integrate Microsoft ecosystem security capabilities (such as Intune and Azure Attestation) with the underlying architecture of the Android Open Source Project (AOSP). Through core features including remote key management, multi-factor authentication, device compliance management, and real-time monitoring, a full-chain security protection system is established for meeting devices—from boot to runtime, and from on-premises to the cloud—meeting enterprise customers' stringent requirements for device trustworthiness, data integrity, and operational compliance.

MDEP achieves data protection through the following mechanisms:

- **Remote Key Management**: Based on Microsoft Public Key Infrastructure (PKI) and the chip-level Trusted Execution Environment (TEE), authentication key pairs and Certificate Signing Requests (CSRs) are generated within a secure environment, and certificate chains are securely stored, ensuring that keys are not exposed.
- **Multi-Factor Authentication**: Multiple layers of defense, including device identity authentication (with secure boot) and user identity authentication, leverage hardware-bound unique identifiers, dynamic credential validation, and system image integrity verification to ensure trusted device identity during runtime.
- **Device Compliance Management**: Through deep integration with Microsoft Intune, security policies are centrally enforced, device status is monitored in real time, and network access compliance checks are performed to ensure that connected devices meet enterprise-defined minimum security standards (such as patch levels, application whitelists, and data encryption policies).

Applicable Models: MeetingBar A25, MeetingBar A40, MeetingBar A50, CTP25

3.2 Android System Hardening

A highly customized Android system is adopted, with multiple hardening strategies applied to reduce security risks. Yealink has removed unnecessary native system services and applications from the Android OS to minimize the attack surface and enhance system security.

In terms of compilation options, secure build configurations are consistently applied to prevent buffer overflow and reverse engineering attacks. These include ASLR (Level 2), stack protection, and binary stripping during compilation.

3.3 Flash Encryption

User data stored on the device is encrypted using a secure key, which itself is encrypted. Once encryption is enabled, all user-generated data is encrypted after being written to the device's flash storage.

Flash encryption uses the AES 256-bit Advanced Encryption Standard. The encryption of the master key is also performed using a 256-bit AES algorithm, implemented via the OpenSSL library. The storage of the master key is protected in accordance with security standards to prevent unauthorized access or direct retrieval of key-related information.

3.4 Firmware Integrity Check and Digital Signature

Before performing a firmware upgrade, the device verifies the integrity of the firmware package. A hash (SHA-256) is first generated to obtain a digest of the firmware, and then public-private key cryptography is used to sign and verify the digest. The upgrade proceeds only after confirming the integrity and authenticity of the package, preventing any tampering or replacement of the firmware.

Additionally, the upgrade ROM package is encrypted using a high-strength encryption algorithm (AES-256). The encrypted partition is written directly to the operating system partition, which helps prevent reverse engineering during the data writing process.

3.5 Kernel Anti-Root Check

At the kernel level, Yealink has implemented a series of security measures to prevent unauthorized rooting. These include signing the entire system at the time of release, removing SU (superuser) functionality from the system, and blocking applications from obtaining elevated privileges.

3.6 SELinux

All Android devices adopt SELinux (Security-Enhanced Linux) as a security framework. Yealink's Android system uses predefined mandatory access control (MAC) policies to regulate process permissions. These policies restrict process access to system directories, files, other processes, and resources, thereby minimizing unnecessary access and enhancing overall system security.

Yealink has independently developed a set of mechanisms to prevent the bypassing of SELinux security controls, ensuring the secure operation of both the Android kernel and upper-layer applications.

3.7 SDK Security

Only Yealink-certified applications (e.g., Teams, Zoom) are allowed to access device-related APIs. Third-party applications that are not certified by Yealink are strictly restricted from accessing these interfaces.

3.8 Android Security Patches

Yealink collects and analyzes Android security bulletins on a monthly basis. Based on these official releases, security patches are applied on a quarterly cycle. In cases where critical vulnerabilities are identified, Yealink prioritizes patching to prevent potential exploitation.

4. Network Security

4.1 802.1X Functionality

The device supports 802.1X functionality, requiring user devices connected to switch ports to undergo authentication, thereby preventing unauthorized access to the network.

The supported 802.1X authentication modes include:

- EAP-MD5
- EAP-TLS
- EAP-PEAP/MSCHAPv2
- EAP-TTLS/EAP-MSCHAPv2

4.2 Wireless 802.1X

The device also supports 802.1X authentication over WLAN. Devices connecting to an access point (AP) are required to undergo authentication to prevent unauthorized access to the network.

The supported 802.1X authentication modes include:

- EAP-TTLS
- EAP-PEAP
- EAP-TLS
- EAP-PWD

4.3 Open VPN

The device supports OpenVPN functionality, allowing it to establish secure point-to-point data communication over public networks through an OpenVPN tunnel.

While transmitting data securely through the VPN tunnel, the device also supports application-layer encryption protocols such as SRTP, SIP TLS, and HTTPS, enabling multi-layer encryption for comprehensive data protection.

For detailed instructions on using OpenVPN, please refer to the Yealink Administrator Guide.

4.4 Network Proxy

The device supports Network Proxy functionality, allowing it to connect through deployed proxy servers to achieve privacy protection and access control. The device supports application-layer proxies (such as HTTP proxy) to intercept and process requests and responses at the application layer, as well as transport-layer proxies (such as SOCKS proxy) to intercept and handle network traffic at the transport layer.

4.5 Network Isolation

The meeting product network is divided into two network domains. The internal domain is a secure domain used exclusively for communication between accessories and the host. Devices within this network normally have no permissions to communicate with external networks.

For devices requiring external network access, a special address is assigned via NAT (Network Address Translation) to enable external communication. External firewall controls on host ports are implemented to protect the LAN network.

4.6 Wi-Fi Security

In addition to supporting wireless 802.1X, the device implements various security measures within the wireless network to protect user data and network communication from unauthorized access and attacks.

- **WPA3 Personal Support:** WPA3 employs a more secure communication protocol. It replaces WPA2's PSK authentication with SAE (Simultaneous Authentication of Equals). SAE effectively resists offline dictionary attacks and increases the difficulty of brute-force cracking. Additionally, SAE provides forward secrecy, ensuring that even if an attacker obtains the network password, they cannot decrypt previously captured traffic.
- **AP Isolation:** By isolating network domains, the device separates accessories connected in the secure domain from ordinary network devices in the guest domain, thereby protecting accessory data transmission security.
- **AP Password:** Each AP password is randomly generated, ensuring that every device's AP password is unique and preventing password leakage.

5. Transmission Security

5.1 Media Encryption (SRTP)

The media streams between endpoints and servers can optionally use SRTP for secure transmission. For detailed information, please refer to RFC 3711. Encrypted SRTP media streams provide integrity, authenticity, and confidentiality for media data.

5.2 Transmission Encryption (TLS)

All data transmitted over the Internet can use secure transmission channels to ensure data integrity and confidentiality, preventing information from being intercepted or tampered with during communication between the device and the server. The endpoint device supports TLS 1.3 functionality and enables it by default. TLS 1.3 improves performance and security compared to TLS 1.2 by removing vulnerable and less commonly used algorithms.

When providing web services, the device prioritizes TLS 1.3 and TLS 1.2 protocols and prohibits the use of TLS 1.0 and TLS 1.1 for communication. TLS signaling connections can only negotiate strong cipher suites, and users can specify cipher suites through configuration profiles. For detailed usage instructions, please refer to the Yealink Administrator Guide to enhance device security.

The default strong cipher suites used by the web service are as follows:

TLS 1.2 ciphers:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS 1.3 ciphers:

- TLS_AKE_WITH_AES_256_GCM_SHA384
- TLS_AKE_WITH_CHACHA20_POLY1305_SHA256
- TLS_AKE_WITH_AES_128_GCM_SHA256

6. Conference Security

6.1 IP Touch Console

Yealink's conferencing system supports the CTP series collaborative touch panels. When a CTP device connects to the host, it must first complete a trusted TLS authentication. Afterward, a secondary authentication is required via a PIN code to ensure the security of the device's connection to the host.

6.2 Wireless Auxiliary Stream Security

Yealink's conferencing system supports the WPP series wireless auxiliary stream devices. The host network is segmented into public and private IP address domains, with auxiliary streams accessing the host through the private network domain to ensure network data isolation.

Signaling during network transmission can be encrypted using TLS, while media data is transmitted using SRTP encryption, ensuring the confidentiality and integrity of transmitted data. For detailed usage, please refer to the Yealink Administrator Guide.

7. Data Security

7.1 Data Storage

- **Data Protection**

Comprehensive protection is provided for static data, dynamic data, and configuration data across three dimensions: storage isolation, encryption policies, and access control.

➢ **Storage isolation and access control**: A mandatory sandbox mechanism is adopted, allocating an independent private storage directory to each application. System-level policies strictly prohibit cross-application access, logically ensuring the isolation of static data.

➢ **Encryption of static data and dynamic data**: All static data stored on the device is encrypted using the AES-256 algorithm, ensuring the security of data on physical storage media. Dynamic data during processing resides only in system memory and is not written to persistent storage, effectively preventing data extraction through static file analysis.

➢ **Configuration data governance**: Device configuration data is stored in accordance with the principle of least privilege and is protected by strict access control policies, ensuring that only authorized users or administrators are permitted to access or modify it.

- **Password Security**

Password-related data transmitted over the network is encrypted using RSA prior to transmission. Password input fields apply obfuscation to ensure that passwords are not displayed in plaintext on the front end. If an incorrect password is entered three consecutive times during login, the account is locked to prevent brute-force attacks. During configuration backup, the device automatically removes all password-related configurations to avoid data leakage.

- **Key Security**

All cryptographic keys are generated using Hardware Security Modules (HSMs) that comply with the FIPS 140-2 Level 3 standard, with root keys permanently stored within the HSM's internal secure area. Physical certificate operations for devices are strictly confined to the internal production environment, and certificates are written to the device's TEE trusted execution partition via secure channels. The production environment enforces stringent Ukey authentication and network isolation measures, ensuring that the entire lifecycle of key generation, storage, distribution, and usage remains secure and controllable.

7.2 Data Deletion

- **Static Data Deletion**

Static data stored on the device (including user files and application data) is securely erased through the factory reset function. This operation restores the system storage to its initial state, ensuring that previously stored static data is no longer accessible.

- **Dynamic Data Deletion**

Real-time data (also referred to as data in use or dynamic data) exists only in system memory during processing and its lifecycle is bound to the device's operational state. Once the device is powered off (through restart or shutdown), all real-time data is immediately and completely cleared.

7.3 Access Control Security

The device is configured with differentiated access control permissions by default, dividing users into User and Administrator roles, each with separate passwords. Accessing advanced device settings requires administrator password authentication. User accounts have standard operation permissions, and the device supports administrators customizing different permissions for regular users. For detailed usage, please refer to the Yealink Administrator Guide.

8. Encryption

8.1 Secure Unique Device Identifier (SUDI)

During the manufacturing process, Yealink programs a Secure Unique Device Identifier (SUDI) into each device. This identifier is a globally unique X.509 certificate for every Yealink device and is used for device authentication. The SUDI is an extension of the device identifier defined by the IEEE 802.1 working group, representing an encrypted device identity. The SUDI is permanently embedded in the trusted anchor module and recorded by Yealink's manufacturing department for device authentication purposes.

By utilizing the SUDI, each Yealink device possesses a unique and secure identifier that facilitates authentication throughout the device's entire lifecycle, from manufacturing to decommissioning. This effectively defends against counterfeit devices and unauthorized access, thereby enhancing overall device security.

In summary, through the use of Yealink's trusted anchor and SUDI, Yealink devices achieve elevated security and authentication capabilities, protecting the system from counterfeit devices and unauthorized access.

8.2 Encryption Algorithms

During the TLS negotiation process, the device uses high-security-level cipher suites by default, disabling anonymous and other insecure cipher suites to ensure the security of data transmitted over the network. For users with stringent security requirements, administrators can configure the cipher suite list to further enhance security. For detailed usage, please refer to the Yealink Administrator Guide.

Cipher Suite List:

- TLS_AES_256_GCM_SHA384 (0x1302)
- TLS_CHACHA20_POLY1305_SHA256 (0x1303)
- TLS_AES_128_GCM_SHA256 (0x1301)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 (0x00a3)
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x009f)
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM_8 (0xc0af)
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM (0xc0ad)

- TLS_DHE_RSA_WITH_AES_256_CCM_8 (0xc0a3)
- TLS_DHE_RSA_WITH_AES_256_CCM (0xc09f)
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 (0x00a2)
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x009e)
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM_8 (0xc0ae)
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM (0xc0ac)
- TLS_DHE_RSA_WITH_AES_128_CCM_8 (0xc0a2)
- TLS_DHE_RSA_WITH_AES_128_CCM (0xc09e)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x006b)
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 (0x006a)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x0067)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 (0x0040)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x0039)
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA (0x0038)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA (0x0033)
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA (0x0032)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
- TLS_RSA_WITH_AES_256_CCM_8 (0xc0a1)
- TLS_RSA_WITH_AES_256_CCM (0xc09d)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
- TLS_RSA_WITH_AES_128_CCM_8 (0xc0a0)
- TLS_RSA_WITH_AES_128_CCM (0xc09c)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003d)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003c)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV (0x00ff)

9. Privacy Security

9.1 Audio and Video Privacy Protection

The device is equipped with a physical motorized privacy shutter. The camera automatically turns off when not in a meeting scenario.

9.2 Log Security

The device provides local and remote logging services to support troubleshooting and security event management. Log output strictly complies with the RFC 5424 standard, and the recording of sensitive data (such as passwords and cryptographic keys) in logs, debug information, or alerts is strictly prohibited. Log transmission supports TLS encryption to ensure confidentiality and integrity. When technical support is required, user authorization is mandatory before any diagnostic information can be accessed, and unauthorized users are not permitted to operate logging functions. Yealink accesses device logs only after obtaining user authorization, and strictly limits their use to device issue diagnosis purposes.

9.3 Configuration Backup

When exporting device configuration backups, password-related settings are removed by default to avoid the risk of password leakage. The configuration files are encrypted using the AES-256 encryption algorithm. This encryption is a strong symmetric encryption method that provides a high level of data protection.

Exported configuration files can be saved in encrypted binary formats such as config.bin, rather than plaintext text files. This security measure effectively protects users' privacy and configuration information during backup, preventing unauthorized access and disclosure.

9.4 Device Management

The device supports management platforms from various vendors, such as Teams Admin Center (TAC), Zoom Device Management (ZDM), and third-party platforms like Utelogy for device management.

Users can also choose Yealink's device management platforms for bulk device management. Yealink offers two deployment options:

1. **YDMP (Yealink Device Management Platform):** Customers install Yealink DM software on their own data centers.
2. **YMCS (Yealink Management Cloud Service):** Built on Microsoft Azure, widely recognized and trusted by enterprise users. YMCS has passed SOC2 Type 2 and GDPR certifications and operates independent data centers in the United States, Europe, and Australia, ensuring comprehensive user data security.

Core functions of Yealink device management services include:

- Monitoring device security and operational status
- Unified deployment and upgrades
- Remote device diagnostics

9.5 Preconfigured Domain Information

When the device restarts or executes operations, it needs to access predefined server addresses. The specific list is as follows:

Domain	Business Functions	Request Method
www.msftncsi.com/ncsi.txt, www.google.com/generate_204	Network connectivity checks are triggered upon reboot or network changes. If not required, the related services can be disabled.	Device
time.windows.com pool.ntp.org	NTP server address is queried at power-on and periodically thereafter. Users may modify the address as needed.	Device
update.yealink.com	Server address for device firmware upgrade check	User
redirect.ymcs.yealink.com	YMCS server address	User
www.google.com	Proxy test access site	User
www.yealink.com	Web hyperlink address providing quick access to Yealink's official website.	User
support.yealink.com	Web hyperlink address that provides quick access to the Support website.	User

Note:
Some addresses may change during the software release process. Please refer to the device's preset or deployed configurations for the most accurate information. If you have any questions, please contact Yealink Technical Support.

10. Security Management

10.1 Product Release Process

Yealink follows a secure Software Development Life Cycle (SDLC). During the product requirements and design phases, the security team collaborates closely with the product team to ensure secure design. In the coding phase, the security team conducts risk assessments of third-party libraries and tools used in the product to prevent vulnerabilities introduced through the supply chain, and performs security reviews.

Before software release, the product undergoes Alpha, Beta, and UAT testing phases, with the security team involved throughout, performing penetration testing, attack surface analysis, and security scanning on both software and hardware to ensure the released product meets the security standards for software release.

Penetration testing includes but is not limited to the following:

- **System Security:** Secure boot, file encryption, compile-time checks, etc.
- **Web Testing:** XSS (Cross-Site Scripting), file upload vulnerabilities, CSRF (Cross-Site Request Forgery), etc.
- **Vulnerability Scanning:** Using multiple leading industry scanning tools to test firmware and deployed devices, ensuring software security.

10.2 Secure Coding Standards

Key Management:
Core key management follows a dedicated personnel and role-based access control strategy, adhering to the principle of least privilege. Ordinary engineers do not have access to or control over cryptographic keys.

Code Management:
Yealink enforces strict secure coding standards internally. Every code update undergoes thorough code review and reliability verification. Device-related code repositories are governed by strict access control policies and company red lines. Uploading code to public or semi-public repositories such as GitHub or Gitee without authorization is strictly prohibited to prevent source code leakage.

Secure Environment:
Yealink's security team and IT department regularly conduct static and dynamic

vulnerability scans and penetration testing on the production environment and internal corporate network. This ensures that software development, firmware packaging, and device manufacturing processes operate within a secure network environment.

10.3 Security Incident Response

Security has always been a top priority for Yealink. With the continuous evolution of industry security technologies, Yealink annually invests significant resources to enhance its security posture. Additionally, Yealink engages multiple well-known and authoritative third-party organizations each year to conduct security validations, ensuring that its security level aligns with current industry standards.

If you encounter any potential security issues while using Yealink products, you can contact us through Yealink's Security Center or submit issues via the Ticket system. We will respond promptly and address related concerns.

The security incident response process is divided into four main phases: vulnerability collection, vulnerability assessment, vulnerability remediation, and follow-up resolution.

- **Vulnerability Collection:** Collect relevant logs and information based on reported security incidents, and assign dedicated personnel to track and handle them.
- **Vulnerability Assessment:** Prioritize vulnerability risks based on issue evaluation, and provide temporary mitigation measures during the handling phase to prevent further impact.
- **Vulnerability Remediation:** Analyze root causes based on incident occurrence, trace design flaws, and address vulnerabilities from the root.
- **Follow-up Resolution:** Investigate whether similar issues exist across all product lines and address them accordingly; all issues are collected into Yealink's vulnerability database for regular review.

For technical support, please visit Yealink Support (https://support.yealink.com) for firmware downloads, product documentation, FAQs, and more. To better serve you, we recommend submitting technical issues via the Yealink Ticket system (https://ticket.yealink.com).

11. Disclaimer

11.1 Statement

This white paper is for informational purposes only and does not grant any legal rights to any intellectual property of Yealink in any of its products.You are permitted to copy and use the content of this document solely for your internal reference purposes.

Yealink makes no express, implied, or statutory warranties regarding the information contained in this white paper.

For more information about the MeetingBar A25, MeetingBar A40, and MeetingBar A50, please visit the official Yealink website.

For additional security-related information, please visit the Yealink Security Center.

Last Updated: December 18, 2025