Meeting Series Security White Paper

This document applies to models: MeetingBar A10, MeetingBar A20, MeetingBar A30, MeetingBoard 65, MeetingBoard 86, MeetingEye500

Overview

With the rapid development of the Internet, enterprise communication devices are widely used in different scenarios. In providing convenience to enterprises, security threats from hardware, system, application, network and other multi-level and multi-dimensional are also becoming increasingly serious, and the user's demand for data security and privacy protection is becoming more and more prominent.

This article takes the protection of user privacy data as the core, and through enterprise security management, OWASP application security standards and Android best security practices as software development guidelines. The product security forms a systematic security protection system to provide security for Yealink's users continuously.

Yealink complies with the General Data Protection Regulation (GDPR), which has been described as the most stringent privacy and security law in the world. Yealink devices comply with current EU data protection regulations and have completed an independent GDPR compliance assessment, demonstrating an industry-leading level of data protection and privacy protection.

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 Continuous investment and optimizing.

This article helps users and security practitioners clearly understand the security architecture and solutions of Yealink products by introducing product security technologies and features. This article is divided into the following sections: Hardware Interface Security, System Security, Network Security, Transmission Security, Conference Security, Data Security, Encryption, User Privacy, and Product Release Process.

Hardware Interface Security

Debugging Interface

The device debug interface is disabled by default:

The UART serial port, ADB, Telnet and other debugging interfaces are closed by default. It is forbidden to open related functions in any way externally. To prevent data risks caused by unnecessary debugging interface exposure to the outside world.

Secure Boot

The device supports secure boot, where the system uses a signed public key to verify the device's integrity during the boot process. At any boot stage, integrity verification is performed on all startup programs (boot program, kernel, and partition integrity), and the system can only be started normally if it passes the safety verification. Otherwise, it cannot be started. The purpose is to prevent loading, run unauthorized programs, and obtain

control of the device by modifying boot parameters and other ways to access the shell interface.

Safe Start Enhanced Security includes the following:

- Unable to program non-Yealink official firmware
- Unable to run non-Yealink official firmware
- Data tampering at any stage can cause the device to fail to boot

External Storage Security

A security parameter is added to the USB partition mount to prohibit programs or scripts in external storage (SD card, USB stick, network storage, etc.) from obtaining access to execute, preventing the execution of unsafe scripts and programs through external partition boot.

System Security

Disk Encryption

The process of storing all user data on a device encrypted using a security key (the key itself is also encrypted). After the device is encrypted, all data (user-created data) is stored encrypted in the device storage after it is deposited to disk.

Disk encryption is performed using the AES 256-bit Advanced Encryption Standard algorithm, and the primary key is encrypted using the 256-bit AES algorithm (implemented through calls to the OpenSSL library). The storage of the primary key is protected according to the standard security specification to prevent external access to the key information.

Firmware integrity checks and digital signatures

Before the device firmware is upgraded, the integrity of the firmware package is verified first. First, the summary of the firmware package is obtained by hash (SHA256), and then the legality of the summary is signed and verified using the public and private keys. The integrity and legality of the upgrade package are ensured before the upgrade is performed to prevent the firmware package from being tampered with or replaced. The data of the upgrade ROM package is also encrypted with a high-strength encryption algorithm (AES256), and the encrypted partition is directly programmed to the OS partition, which can prevent reverse analysis during the partition data writing process.

Kernel anti-rooting check

Yealink provides users with a safe and reliable operating system and does not provide an application store to the public to avoid installing unreliable applications. At the kernel level, the device will design a series of restrictions to prevent Root based on the characteristic behavior of illegal Root. These include whole system signature when the system is released; removing the function of SU in the system to prevent the application from lifting power.

SELinux

Android devices use SELinux (Security Enhanced Linux) security scheme. The system through a predefined mandatory access control policy to achieve process permission control, restrict the process operation of the system directory, files, processes and other resources to minimize the operation rights. A set of internal independent designs to prevent bypassing

the SELinux security mechanism scheme to ensure the safe operation of Android kernel and upper layer applications.

SDK Security

Only Yealink certified APP can access the device-related API, and uncertified third-party APP will have strictly restricted access.

Android Patch Update

Yealink collects and analyzes the patches announced by the official Android announcement every month, and fixes them every quarter based on the official patch release. When a severe problem is judged, patch fixing will be prioritized to avoid vulnerabilities from being exploited.

Network Security

802.1X Features

The device provides 802.1X functionality, where user devices connected to the switch port must be authenticated to prevent unauthorized users from accessing the network. The device supports 802.1X mode:

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

Wireless 802.1 X

The device also supports 802.1X for WLAN, which requires authentication of the device when accessing the AP and prohibits unauthorized users from

accessing the network. The devices support 802.1X mode with the following:

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

Open VPN

The device supports the function of Open VPN, which allows the device to communicate securely peer-to-peer through the network tunnel established by Open VPN in the public network environment. The device also supports SRTP, SIP TLS, HTTPS and other application layer data encryption. Users can achieve secure data transmission through the VPN tunnel to achieve multi-layer encryption for data protection. The specific usage of Open VPN can be found in the configuration guide of the Yealink Admin Guide.

Network Isolation

The network of the conference product is divided into two network domains, the internal network domain for the security domain: which is only used for communication between the accessories and the host, and the network devices under normal circumstances without any external network communication rights. For those who need to access the external network, use the NAT network address translation technology to assign a special address to the Internet access device in the internal network and perform NAT conversion on the special address to communicate with the external network domain of the host. Through the external firewall on the host port control to achieve the purpose of protecting the LAN network.

Transmission Security

Media Encryption (SRTP)

When the device establishes a session with another encrypted device, the media data is optionally transmitted using AES-128 Secure Real-Time Transport Protocol (SRTP) with a key length that supports the configuration of AES256 bits; the key is dynamically generated at the time of call creation and is unique.

Transport Encryption (TLS)

All data transmitted in the Internet network, the connection between the device side and the server, can be secured using a secure transmission channel. The download process performs integrity checks on the data to ensure that information is not stolen or tampered with during the network transmission between the device and server sides. TLS1.3 is supported and enabled by default on the end device. TLS1.3 improves performance and security over TLS1.2 (e.g., removes vulnerable and less used algorithms). On the server side, TLS1.0 and TLS1.1 are not allowed for communication. In contrast, TLS1.1 can be negotiated client-side for compatibility with a wide range of servers, and users can configure the protocol to disable TLS1.1 to improve the security performance of the device.

Secure Peer-To-Peer Conference Communications (H.235)

Yealink's conferencing system supports the H235 security protocol in the peer-to-peer conferencing function, which encrypts the media stream during the conference to ensure the security of the conference data. To be

more compatible with the scenario, users need to use the H235 function to open through the webpage or configuration. Refer to the configuration guide of the Yealink Admin Guide for specific use.

Conference Security

Slave Security Access

Yeaklink's conference system supports the CTP18 collaborative touch conference tablet. The CTP18 requires trusted TLS authentication when accessing the host and requires secondary authentication via Pin code after authentication is completed to ensure the security of the slave access.

Content Sharing Safety

Yeaklink's conferencing system supports WPP20 and WPP30 wireless devices, which delineate public and private network addresses on the host network, and the additional stream passes through the private network domain of the accessing host to ensure network data isolation. In network transmission control, signaling can be transmitted by TLS encryption, and media data is transmitted by SRTP encryption to ensure the confidentiality and integrity of network transmission data. Refer to the configuration guide of the Yealink Admin Guide.

Data Security

Data Storage

- Business Data Storage

The business data involved in the device is stored directly on the device, and only users and administrators have relevant read and access rights.

- Configuring File Encryption

The device supports CFG configuration encryption, which can be encrypted on the original configuration file first, and then decrypted by automatic deployment to the device internally before updating the configuration. Yealink provides encryption tools for Windows, Linux and other platforms to encrypt the configuration file, where the user sets the key. For details, please refer to the configuration guide of the Yealink Admin Guide.

- Password Security

The device transmits the private data in the network through RSA encryption in the network data transmission. Privacy data is anonymized in the input box and will not be displayed in plain text on the front end. The account will be locked if the number of errors reaches 3 times during brute force cracking to prevent attackers from brute force cracking the device. During the configuration backup process, the device will automatically clear the password-related configuration to avoid the loss of the user's private data.

Data Deletion

All business data on the application will be deleted when the device is restored to the factory to protect user data security.

Access Control Security

By default, the device has differentiated access control privileges: users and administrators, and each user has a different password. User only have normal operation privileges, and the device supports administrators to

customize additional privileges for normal users. Refer to the configuration guide of the Yealink Admin Guide for details.

Encryption

Equipment Unique Certificate

The device is shipped with its own uniquely identified device certificate issued by the root certificate of Yealink Root CA. The certificate uses the SHA256 signature algorithm, the certificate key length reaches 2048 bits, and the security specification follows the protocol standard.

Encryption Algorithms

During TLS negotiation, the device uses a high-security encryption algorithm suite by default. It disables anonymous and other insecure algorithm suites to ensure the security of data transmitted over the network. For security-critical users, you can set the algorithm list through the administrator to improve the security level. Refer to the configuration guide of the Yealink Admin Guide for details.

Algorithm 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)

Privacy and Security

Audio and Video Privacy Protection

The device has a physical camera privacy cover, automatically turning off when not working. Avoid the user unknowingly camera called for recording.

Log Collection

The device is not factory configured for remote log collection. If you need to configure remote log service, refer to the configuration guide of the Yealink Admin Guide. The device removes the privacy data related to user authentication from the logs. If the user's device fails and problem diagnosis is required, the user needs to cooperate and authorize the local export of the device's diagnostic file for failure analysis. Non-authorized users cannot actively access the diagnostic information of the current device.

Configuration Backup

When exporting user configuration backups, the password-related configuration is removed by default. The configuration file is encrypted using the AES256 encryption algorithm inside the device. Then the config.bin file is exported through the web page, which needs to be

decrypted by a special security decryption tool before it can be decompressed, which can effectively protect user privacy.

Equipment Management

When you are an enterprise user and need to configure and manage your device through Yealink Management Cloud Service (YMCS) (the service is not enabled by default), the device requires to report the following information to the server (the specific information reported by the device to YMCS can be found in the Yealink Management Cloud Service Security White Paper):

- Device information (MAC, product type, SN, IP)
- Device Diagnostic Log
- The data reported by the device contains mainly personal information and confidential usage data: including configuration files (user name, password, associated account), resource files, log files, screenshots, etc.
- Device Software Updates
- Get call quality statistics via RTCP_XR, following the protocol standard of RFC 3611

If users have questions about the reported content, they can contact the enterprise administrator and Yealink's technical support staff.

Statement:

Yealink Device Management Cloud Service processes information for the following primary purposes:

- Provide device management cloud services
- Diagnosing technical problems
- Problem analysis to improve the technical performance of the service
- Respond to customer technical support requests

Preset Domain Information

The preset server addresses need to be accessed when the device is rebooted or when executing a service, as listed below:

Domain name	Business function	Request method
http://www.msftncsi.com/ncsi.txt, http://www.google.com/generate_204	Network connectivity check. Devices will access this address upon restart or network changes.	Active request
https://rpscloud.yealink.com	Yealink redirection service address for automatic deployment. Devices will access this address after the factory reset, which will be closed after the successful deployment.	Active request
time.windows.com pool.ntp.org	NTP server address. Devices will access this address periodically or when the device is powered on. Power-on and periodic query.	Active request
https://dm.yealink.com	The address of the ROM package for checking and upgrading. It is turned off by default and needs to be enabled by the user.	Active detection
http://www.yealink.com	Web static address. When clicking it, users will be directed to Yealink's official website.	Passive request
http://support.yealink.com/	static Web address. When clicking it, users will be	Passive request

Domain name	Business function	Request method
	directed to Yealink technical support website.	

Notes:

Some addresses are subject to change during the software release, and the devices pre-configured or deployed configuration is required, so you can consult Yealink technical support if you have any questions.

Security Management

Product Launch Process

Yealink follows the Secure Software Development Life Cycle (SSDLC), in which the security team will work with the product team to design the product during the requirement and design stages. The security team will conduct a risk assessment of the third-party libraries and tools used in the product during the coding stage to ensure that no vulnerabilities are introduced by the supply chain and conduct security reviews. The security team is involved in penetration testing, attack surface analysis, and security scanning of hardware and software at each stage to ensure that the released product meets the security standards for a software release.

Penetration testing includes, but is not limited to, the following:

- **System security**: secure boot, file encryption, compile condition detection, etc.
- **WEB testing**: XSS cross-site scripting attacks, file upload vulnerabilities, CSRF cross-site forgery request attacks, etc.
- **Vulnerability scanning**: Use several industry-leading scanning tools to test the firmware and deployed devices and ensure the security of the software.

Code Security Specifications

Key Management: The core key management adopts a dedicated strategy. Based on the principle of least privilege, ordinary engineers cannot access and obtain the key.

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 tough permission management mechanisms and requirements. It is strictly forbidden to upload to public or semi-public services such as Github, Gitee and other general code bases without permission to prevent source code leakage.

Security 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.

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 while using Yealink products, you can contact us in Yealink's Security Center or submit your case through the Ticket system. We will respond and handle the issue promptly.

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 promptly.
- **Tracking and resolution**: Check whether all product lines have the same problem, and collect the issues to 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 using the Yealink Ticket system to submit technical questions.

Disclaimers

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 concerning the information in this white paper. For more information about the Yealink Meeting series of devices, you can visit Yealink's official website, and for

more security-related information, you can visit Yealink SECURITY & COMPLIANCE.