Yealink Teams Phone Security White Paper

This document applies to the following models: MP58-Teams, MP56-Teams, MP54-Teams, MP52-Teams, VP59-Teams, CP965-Teams.

Overview

With the rapid development of the mobile internet, enterprise communication terminal devices are widely used in different scenarios. In providing convenience to enterprises, security threats from multiple dimensions, such as hardware, system, application, and network, are becoming increasingly severe. The demands of end-users for data security and privacy protection are becoming more and more prominent.

This white paper takes the protection of user privacy data as its core. Taking enterprise security management, OWASP application security standards, and Android best security practices as software development guidelines, product security forms a systematic security protection system, continuously providing security guarantees for Yealink's end users.

Yealink complies with the world's strictest privacy and security law, the General Data Protection Regulation (GDPR). Yealink devices comply with current EU data protection regulations and have completed an independent GDPR compliance assessment, reflecting industry-leading data protection and privacy levels.

Yealink passed the GB/T 22080-2016/ISO/IEC 27001:2013 security system certification in July 2022. ISO/IEC 27001 is an international standard widely accepted as the best practice for security. The certification establishes a secure implementation process for products and means that the company continues investing in and optimizing security management and product security design.

This article introduces the security technology and features of Yealink products to help users and security practitioners understand the security architectures and solutions of Yealink products clearly. The article is mainly divided into the following sections: hardware interface security, system security, network security, transmission security, data security, encryption, user privacy, and product launch process.

Hardware Interface Security

Debugging Interface

The device debugging interface is closed by default.

By default, the UART serial port, ADB, Telnet and other debugging interfaces are turned off when the device leaves the factory. It is prohibited to enable related functions in any way externally to prevent unnecessary debugging interfaces from being exposed externally and causing data risks.

Secure Boot

The device supports secure boot, and the system verifies the device's integrity using a signed public key during the boot process. All boot programs (bootloader, kernel, partition integrity) are verified for integrity at any stage of the boot process. Only when the security check is passed can the system start-up usually. Otherwise, it cannot start up. The purpose is to prevent unauthorized programs from being loaded and run and to prevent access to device control by entering the Shell interface by modifying the boot parameters.

Secure Boot enhances security with the following:

- Unable to flash non-Yealink official firmware.
- Unable to run non-Yealink official firmware.
- Any data tampering at any stage will cause the device to fail to start.

External Storage Security

When mounting the USB partition, security parameters are added to protect execution permissions from being obtained by programs or scripts in external storage (SD card, USB flash drive, network storage, etc.) and to prevent unsafe scripts and programs from being executed through external partitions.

System Security

Disk Encryption

Yealink uses a secure encrypted key to encrypt all user data and store them. After encryption, all data (user-created data) is stored in encrypted form in the device storage space after being stored on the disk.

Disk encryption uses the AES 256-bit advanced encryption standard algorithm. The 256-bit AES algorithm is used to encrypt the primary key (implemented through calls to the OpenSSL library). The storage of the primary key will be

protected according to security standards to keep related key information from external access.

Firmware Integrity Checksum and Digital Signature

Before upgrading the device firmware, an integrity check will be performed on the firmware package to protect it from being tampered with or replaced. First, obtain the firmware package digest through hashing (SHA256), use public-private key encryption to sign, and then verify the digest's legality. The data of the ROM package being upgraded is also encrypted using a high-strength encryption algorithm (AES256). The encrypted partition is directly written to the operating system partition, which can prevent reverse analysis during the partition data writing process.

Kernel Anti-Root Check

Yealink provides users with a secure 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 has designed a series of restrictions to prevent Root based on the characteristics of illegal Root behavior, including signing the entire system when it is released; removing the SU function in the system to avoid application privilege escalation.

SELinux

Android devices all use the security solution of SELinux (Security-Enhanced Linux). The system controls process permissions through predefined mandatory access control policies, minimizing the operational permissions of system directories, files, processes, and other resources. It has internally designed a set of solutions to prevent bypassing the SELinux security mechanism, ensuring the secure operation of the Android kernel and upper-layer applications.

SDK Security

Only Yealink-certified apps can access device-related APIs, while uncertified third-party apps will be strictly restricted.

Network Security

802.1X Function

The device provides the function of 802.1X. User devices connected to the switch ports need to be authenticated, and unauthorized users are prohibited from accessing the network. The device supports the following 802.1X modes.

- EAP-MD5

- EAP-TLS
- EAP-PEAP/MSCHAPv2
- EAP-TTLS/EAP-MSCHAPv2
- EAP-PEAP/GTC
- EAP-TTLS/EAP-GTC
- EAP-FAST

Wireless 802.1 X

The device also supports WLAN's 802.1X function. The device needs to be authenticated when accessing the AP, and unauthorized users are prohibited from accessing the network. The devices support the following 802.1X modes:

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

Open VPN

The device supports the Open VPN function. In a public network environment, the device can establish point-to-point secure data communication through the network tunnel created by Open VPN. While users achieve secure data transmission through the VPN tunnel, it also supports data encryption on the application layer, such as SRTP, SIP TLS, HTTPS, etc., to protect data with multi-layer encryption. For specific instructions on using Open VPN, please refer to the configuration guide in the Yealink Teams Phone Admin Guide.

Transmission Security

Media Encryption (SRTP)

When a device establishes a real-time communication session with another encrypted device, media data are encrypted and authenticated using Secure Real-time Transport Protocol (SRTP), which supports AES-256 and AES-128 as encryption algorithms to generate keys. The key is dynamically generated when the call is created and is unique.

Transport Layer Security (TLS)

All data transmitted over the Internet uses a secure transmission channel to ensure data security between the device and the server. During the download process, data integrity verification is performed to ensure that information is not stolen or tampered with during the network transmission process between the device and the server. The terminal device supports TLS1.3, which is enabled by default. Compared with TLS1.2, TLS1.3 improves performance and security (removing vulnerable and less-used algorithms). When the device acts as a server, communication using TLS1.0 and TLS1.1 is not allowed. However, TLS1.1 will be used to be compatible with a wide range of servers when the device acts as a client. Users can disable the TLS1.1 protocol to improve device security performance by configuration. For specific usage methods, please refer to the configuration guide in the Yealink Teams Phone Admin Guide.

Data Security

Data Storage

- Business Data Storage

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

- Configuration File Encryption

  The device supports CFG configuration encryption. You can encrypt the original configuration file first, decrypt it automatically after deploying it to the device, and then update the configuration. Yealink provides encryption tools for Windows, Linux and other platforms to encrypt configuration files. The key is set by the user. Refer to Yealink Teams Phone Admin Guide for more details.

- Password security

  The device encrypts private data using RSA and transmits it over the network. The private data is anonymized in the input box and will not be displayed in plain text on the front end. If the number of incorrect attempts reaches three times, the account will be locked to prevent attackers from brute force cracking the device. During the configuration backup, the device will automatically clear password-related configurations to avoid losing the user's private data.

Data Deletion

When the device is restored to factory settings, all business data on the application will be deleted to ensure user data security.

Access Control-Security

By default, the device's access control permissions are divided into User and Administrator. Each user has a different password. When accessing advanced settings of the device, administrator password authentication is required. Users only have ordinary operation permissions. The device supports administrators to customize different permissions for ordinary users. Please refer to Yealink Teams Phone Admin Guide for more details.

Encryption

Device Unique Certificate

Devices are pre-installed with a device certificate with a unique identifier issued by Yealink Root CA. The certificate uses the SHA256 signature algorithm with a key length of 2048. The security standard follows the protocol standard of RFC 2818.

Encryption Algorithm

During the TLS negotiation process, the device uses a high-security level encryption algorithm suite by default and disables anonymous and other insecure algorithm suites, ensuring the security of data transmitted over the network. Administrators can set the algorithm list for security-conscious users to increase the security level. Please refer to the Yealink Teams Phone Admin Guide for more details.

Algorithm List:

- TLS_AES_256_GCM_SHA384 (0x1302)
- TLS_CHACHA20_POLY1305_SHA256 (0x1303)
- TLS_AES_128_GCM_SHA256 (0x1301)
- LS_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 is equipped with a physical camera privacy cover. The camera will automatically turn off when not in use to prevent users from unknowingly recording with the camera.

When malicious applications attempt to obtain microphone/camera permissions through deception, the device's UI interface will display relevant icons indicating that the device is in use.

Log Collection

The device is not configured with a remote log collection service when it leaves the factory. If you need to configure a remote log service, please refer to Yealink Teams Phone Admin Guide for more details. The device removes privacy data related to user authentication in the logs. If the user's device malfunctions and needs to be diagnosed, the user must cooperate and authorize the diagnosis file exported locally from the device for fault analysis. Unauthorized users cannot actively obtain the current device's diagnostic information.

Configuration Backup

The password-related configuration will be removed by default when exporting user configuration backup. The configuration file will be encrypted using the AES-256 encryption algorithm inside the device and then exported as a config.bin file through the web page. This file needs to be decrypted by a dedicated security decryption tool before it can be decompressed, which can effectively protect user privacy.

Device Management

As an enterprise user, you need to configure and manage devices through the Yealink Device Management Cloud Service (YMCS) (this service is not enabled by default). The device needs 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 includes mainly personal information and confidential usage data, which includes configuration files (usernames, passwords, associated accounts), resource files, log files, screenshots, etc.
- Device software update.
- Call quality statistics obtained through RTCP_XR, which complies with the protocol standard of RFC 3611.

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

Declaration:

The primary purpose of Yealink Management Cloud Service for processing information is limited to the following:

- Provide device management cloud services.
- Diagnose technical issues.
- Problem analysis to improve the technical performance of service.
- Respond to customer technical support requests.

Predefined Domain Information

When the device is restarted or when executing business, it is necessary to access the predefined server addresses as listed below::

Domain name	Business function	Request method
http://www.msftncsi.com/ncsi.txt,	Network connectivity check.	Active

Domain name	Business function	Request method
http://www.google.com/generate_204	Devices will access this address upon restart or network changes.	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 directed to Yealink technical support website.	Passive request

NOTE：

Some addresses will be optimized during the software release process. If there are any changes, you can check the version release notes.

Security Management

Product Launch Process

Yealink follows a secure software development life-cycle (SSDLC). During the product requirement and design phases, the security team works with the product team to design the product. During the coding phase, the security team assesses the risks of third-party libraries and tools used in the product to ensure no vulnerabilities are introduced through the supply chain and conducts security reviews. Before the software version is released, it undergoes Alpha version, Beta version, and UAT testing, with the security team participating in penetration testing, attack surface analysis, and security scanning at each stage to ensure that the released product software meets the security standards for the software release.

Penetration testing includes but is not limited to the following:

- System security: secure boot, file encryption, compilation condition detection, etc.
- Web Testing: XSS Cross-Site Scripting Attack, File Upload Vulnerabilities, CSRF Cross-Site Request Forgery Attack, etc.
- Vulnerability scanning: Use multiple mainstream scanning tools in the industry to test firmware and deployed devices to ensure the security of the software.

Code Security Standards

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

Code management: Yealink has strict coding security requirements internally. Each code update is reviewed and undergoes reliability verification. The device-related code library has strict permission management mechanisms and company red-line requirements. It is strictly prohibited to upload to public or semi-public services such as GitHub and Gitee without permission to prevent source code leakage.

Security Environment: Yealink's security team and IT department will regularly perform static and dynamic vulnerability scans and penetration testing on the production and internal network environments to ensure that the software

development, firmware packaging, and device production processes are in a secure network environment.

Security Emergency Response

Security has always been a focus of Yealink. As industry security technology iterates continuously, Yealink invests heavily in resources yearly to improve Yealink's security level. At the same time, Yealink invites multiple well-known, authoritative third-party organizations annually to conduct security verification to ensure that the security level matches the current security technology. If you find a possible security issue while using Yealink products, contact us at Yealink's security center or submit a ticket through the ticket system. We will respond promptly and deal with relevant issues.

Security emergency response is divided into four stages: problem collection, vulnerability analysis, vulnerability fix, and tracking resolution.

- **Problem collection**: Collect relevant logs and information based on reported security incidents, and assign dedicated personnel to track and handle them.
- **Vulnerability analysis**: Priority is given to determining vulnerability risks based on the problem. During the processing stage, temporary solutions will be provided first to avoid the issue from expanding.
- **Vulnerability fix**: Analyze the root cause of the problem based on its occurrence, trace the reasons for the defects in the design, and promptly solve the vulnerability problem from the root cause.
- **Track and resolve**: Investigate whether all product lines have the same problem and follow up to resolve it while regularly collecting the problem into Yealink's vulnerability database for periodic review.

Technical support can access Yealink Support (https://support.yealink.com) to learn about firmware downloads, product documentation, and frequently asked questions. We recommend using the Yealink Ticket system (https://ticket.yealink.com) to submit technical issues for better service.

Disclaimer

This white paper is for reference only and does not authorize any legal rights to any intellectual property in any Yealink product. You may copy and use the content of this document for internal reference purposes only.

Yealink makes no express, implied, or statutory warranties regarding the information in this white paper. For more information about Yealink Teams Phone series devices, please visit Yealink's official website. To learn more about security-related details, please visit Yealink Security Center.