Security on Yealink Android Devices

Introduction

This white paper addresses security and privacy related information for the Yealink RoomPanel products, and which may be updated from time to time. The most current version of this white paper will be available on Yealink's website.

RoomPanel products provide meeting room reservation function for the meeting room and can indicates room status. They are deployed on-premises withinthe customer's environment. As these systems are deployed in the customer's environment, it is the responsibility of the customer to protect data that resides on the systems.

Android Security Practices

On all Yealink Android based video endpoints, the Android operating system is locked down. Android features and functions that are not necessary for standard operation of a given device are disabled.

- Devices run a modified and restrictive implementation of Android which limits the capabilities of the device as compared with commonly available Android phones and tablets
- Yealink removes the ability to side-load APKs or access the Google Play store, and we formally test that these restrictions remain in place across product releases.
- We follow Android recommended guidelines for signature verification of installed applications, and all device software updates are restricted to Yealink signed update packages.
- All devices are tested against known rooting and jailbreaking methods and are hardened against architecture modification.
- Endpoints are designed and tested to ensure that a device administrator can configure the security posture according to local needs. Examples of configuration options available to a local administrator include configuration of password policy, encryption strength and responses to failed login attempts. Logging, both internally and remotely, is also configurable.

RoomPanel product is based on Android operating system. As many usersmay worry about the security of the Android system, Yealink devotes ourselves to providing users with a secure system environment based on Android. No matter the Android system or the related service on Android provided by Yealink, they are bothequipped with multiple security solutions.

The following security solutions provided by Yealink will be introduced in details in this guide:

- Streamline Android system and update security patches timely to reduce security vulnerabilities.
- Employ Security Enhancements for Android (SE Android) solution to prevent root privilege escalation
- Embed built-in Application Deployment and Management (ADM) mechanism to strictly control the privilege of third-party application.
- Provide powerful Virtual Private Network (VPN) feature to prevent data leakage.

Security Vulnerability Problem:

Since Android system consists of a large number of modules, if there are any vulnerabilities in some of the modules, the system may be easy to be attacked by themalicious users.

Solution:

Yealink has streamlined the Android system for Yealink Android Device and only the modules related to the product features is retained, greatly reducing the system security risks. Meanwhile, in order to enhance the system security, the security patches released by Google will be updated timely for Yealink Android Device to fix all the known security vulnerabilities.

Root Privilege Escalation Problem:

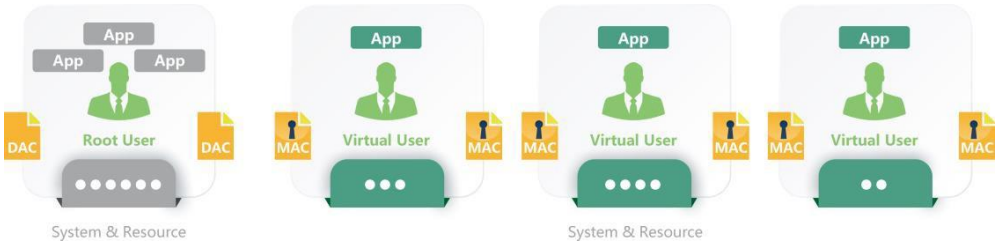
The Linux-based Android system supports Discretionary Access Control (DAC) which allows users to grant themselves access to read, write, and execute files. Under this mechanism, if a security vulnerability is exploited by malicious users, they could get the super Administrator privileges easily and potentially obtain unauthorized access to data files, applications and resources.

Solution:

Yealink Android Device protects the system through SE for Android, which is built on the SELinux technology.

SELinux employs Mandatory Access Control (MAC) mechanism, which the privileges of users and applications are control by the policy file other than being discretionary, even the super Administrator doesn't have the privilege to modify the policy file.

SE for Android secures the system by separating it into distinct security domains. Within each domain, applications are given the minimal permission needed to operate. This process will contain the damage in one area and leave other areas uncompromised.

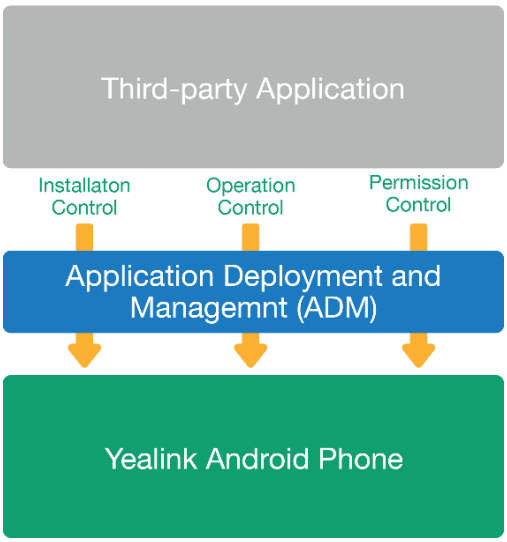


Malicious Application Problem:

There exist third-party applications on the market which are of varying quality. Some malicious codes are even found in part of these applications, which could compromise the security of the system and steal the user's data.

Solution:

A built-in Application Deployment and Management (ADM) mechanism has been implemented in Yealink Android Device, which limits the user to install third-party applications as a default, thereby fully controlling the installed third-party applications.



By means of Auto Provisioning, administrators can deploy and manage applications conveniently, including installing, updating, and uninstalling applications, configuring whether users can install and uninstall third-party applications via user interface, whether the application can run on startup, run in the background, or function during the call and whether a third-party application can use the privilege which is applied at the time of installation. For more information on this, please contact **support@yealink.com**.

Data Leak Problem:

If the unencrypted application's data are sent to the network, they might be monitored, intercepted, and tampered with.

Solution:

Since Yealink Android Device supports OpenVPN, the application data will be encrypted when transmitted through OpenVPN.

OpenVPN employs OpenSSL for data encryption, allowing the terminals to participate in the establishment of VPN to use default private key, third party certificate, or user name/password for authentication, while still supporting TUN and TAP mode. Compared with the Android native VPN, OpenVPN provides richer functionality. In addition to ensuring the data secure in the communication, OpenVPN allows secure access to corporate resources by establishing an encrypted tunnel across the Internet.

Cryptographic Security

RoomPanel product uses secure communication channels for all over data networks. RoomPanel product implements cryptographic libraries on the system and will encrypt all data being transmitted. Data transfers use HTTPS data stream over port 443, using TLS andunsymmetrical encryption algorithms RSA.

Administrator Authentication

The customer's administrator can access Yealink RoomPanel product for management and configuration by using the device's web interface. Access to the device's web interface requires administrator credentials to be entered via a web browser.

Data Processing

By default, the following information is processed and stored locally on the Yealink RoomPanel devices:

- MAC address
- Serial number
- IPv4/v6 addresses
- Admin ID and password
- System log files
- Directory entries
- IP peripheral details

This information is used by the device to provide basic functionality, device pairing operations.

If you elect to use the Yealink RoomPanel product with the optional Yealink Device Manager Platform, it will send information to that system for the purpose of provisioning and management. For details about this data processing, please refer tothe Privacy section of the Yealink Device Manager Platform

As these devices and systems are deployed in the customer's environment, it is the responsibility of the customer to protect the data processing.

Customer Feedback

We are striving to improve our documentation quality and we appreciate your feedback. Email your opinions and comments to DocsFeedback@yealink.com.

Technical Support

Visit Yealink WIKI (http://support.yealink.com/) for the latest firmware, guides, FAQ, Product documents, and more. For better service, we sincerely recommend you to use Yealink Ticketing system (https://ticket.yealink.com) to submit all your technical issues.