Yealink

Yealink Device Management Platform Security White Paper

Version 38.10.0.0 | November 2022

Contents

Introduction

Security is always the most critical consideration for all Yealink products and services.

To improve the security posture of our products, we invite third-party security organizations to do a thorough security vulnerability scanning and penetration testing on all devices on a regular basis. Our security team also focuses on security concerns and offers a hot patch or release a new version to address them.

This white paper describes security-related practices regarding Yealink Device Management Platform (“YDMP”) and includes information about how these practices are applied to the design, development, testing and improvement.

This white paper will be updated from time to time, and the latest version of this paper will be available on https://www.yealink.com/en/onepage/trust-center-security-compliance.

Product Design Security

Yealink follows Security by Design principles throughout our product creation and delivery lifecycle which includes considerations for confidentiality, integrity (data and systems) and availability. These extend to all systems that Yealink uses – both on-premises and in the cloud as well as to the development, delivery and support of Yealink products, cloud services and managed services.

The foundational principles which serve as the basis of Yealink's security practices include:

1. Security is required, necessary and foremost
2. Product full lifecycle design security
3. Data security, especially personal data security
4. Security testing and validation
5. Adherence to operational security and compliance audits

Product Basic Security

Physical Security

YDMP software is provided by Yealink, installed and deployed on clients' servers. Therefore, the data access and storage are fully controlled by the clients. Yealink has no access or permission to the data.

The software of YDMP is designed and developed based on and compliant with the industrial security standards and encryption rules.

Application Security

Identity authentication

YDMP supports a strong password policy, in which the password should include 8 to 32 characters with a combination of numbers, letters, and special characters (excluding space), to ensure account security. In addition, YDMP provides multi-factor authentication, which requires two-step authentication to ensure login security.

Protection against malicious injections

YDMP has limits on the data format for all the input boxes, for example, the length and the characters, to avoid constructing SQL statements directly through the input boxes. Furthermore, executable commands are prohibited.

File and resource security

YDMP restricts the size and the format of the uploaded files, to avoid maliciously uploading large files and illegal executable files. Additionally, YDMP restricts the directory of the uploaded files to avoid modifying the storage directory of the server from the front end. What's more, only the templates provided by YDMP are supported.

Protection against protocol attacks

A private protocol and TLS are used between the device and YDMP to encrypt transmission. Therefore, attackers are unable to obtain and forge protocol information to establish communication with the server.

Web Access Security

YDMP allows you to set the expiration time for the web session to prevent illegal operations by non-authenticated users. If the session timed out, the user needs to log in again.

Device Connection Security

The connection between phone and YDMP uses TLS 1.2 and a custom TCP. Only through TLS 1.2 mutual authentication can the phone be connected to YDMP.

When the phone and YDMP perform mutual authentication, YDMP verifies the legitimacy of the phone based on the phone's certificate (only a Yealink self-signed certificate can pass the verification) and MAC (the MAC of each phone is unique). At the same time, the phone verifies the certificate sent by YDMP to determine whether it is YDMP.

After the phone is connected to YDMP, the requests between them are authenticated by HTTPS and the data are transmitted by TLS 1.2.

API Security

Third-party applications need to apply for the AccessKey and the SecretKey if they want to access YDMP.

YDMP supports the anti-replay mechanism to avoid data packet spoofing, and it also uses the HTTPS to secure the access.

Data Security

Data Processing

Since YDMP is deployed on the clients' sides, the data is also stored in the clients' servers. Therefore, the data processing is fully controlled by clients and independent of Yealink. Yealink has no access or permission to clients’ data.

Storage Security

Since YDMP is deployed on the clients' sides, the data is also stored in clients' servers. Therefore, the storage security entirely depends on the clients' server abilities and strategies.

Data Access Security

Clients control data access of YDMP. Yealink has no access or permission to the data. Therefore, the data access security is more related to the strategies of the hosted server clients choose.

Data isolation between the enterprise administrator accounts

The enterprise accounts are divided into the administrator and the sub-administrator accounts.

The administrator creates the sub-administrator accounts. He can divide the sub-administrator accounts according to the site and assign the function and data permissions to the sub-administrator accounts. Besides, the administrator can delete the sub-administrator accounts and modify the assigned function and data permissions.

The sub-administrator account can only add, delete, and modify the device under the site he can manage. The sub-administrator can only use the assigned function and data permissions.

Transmission Security

The access to YDMP uses HTTPS and is encrypted by ECDHE-RSA-AES256-GCM-SHA512.

All communication in YDMP web portal is over a standard secure SSL connection, which encrypts all requests and responses. Besides, all connections to YDMP are encrypted with TLS 1.2 to secure the data transmission.

Yealink ensures that the data between the device and YDMP is encrypted through long connection protocols based on SSL and TLS, which can prevent malicious attacks and data tampering to ensure data security. The keys of the certificates used in Long Connection Protocol is also stored with encryption, which can effectively prevent the key from being used illegally if it is stolen. Moreover, sensitive data is transferred with TLS_RSA_WITH_AES_128_CBC_SHA encryption.

Data Deletion and Retention

All information collected by YDMP is controlled by Yealink clients independently. Yealink has no access or permission to delete and keep the data.

Privacy Data Processing Authorization

All the data processing is controlled by Yealink clients independently. Yealink has no access or permission to process the data.

Cluster Deployment and Disaster Recovery

YDMP supports cluster deployment and disaster recovery mechanism. When one server node goes down unexpectedly due to outages, the system will automatically and seamlessly switch to back-up server without interrupting the business operation. Therefore, it greatly enhances business continuity and system security.

Operation Security

Operation Norms

Yealink regularly organizes project review, code inspection, vulnerability detection, and virus cleaning to ensure that the release of YDMP meets the industry standards.

Also, Yealink provides after-sales service for issues related to YDMP.

Access and Audit

YDMP is hosted in Yealink clients' own servers. The access to the production server of YDMP is controlled by Yealink clients independently.

Besides, the system records operation and maintenance logs for later audits if required. Clients can export the server logs for server maintenance.

Security Incident Response

Yealink classifies YDMP-software-related security incidents and adopts different solutions.

From the stage of occurrence, processing, analysis, and review, Yealink conducts closed-loop management and continuous improvements for enhancing the ability to respond to the security incidents and keeping the system stable.

When a security event occurs, the related log and information are collected, and an expert group is established.

In the stage of processing, the expert group makes temporary solutions and assists the later improvements.

In the stage of analysis, Yealink reviews the process of how the security incident occurs, analyzes the problem from all aspects, and improves it in the later version.

In the stage of review, we will summary the root cause and improve the mechanism of controlling beforehand and detecting in the process.

Security Test

Both static and dynamic vulnerability scanning as well as penetration testing are regularly performed for production releases and against our internal corporate network by both internal and external test teams. Yealink maintains a partnership with NetSPI Group, a leading international security penetration testing organization, to regularly perform security penetration tests on a wide range of our products.

Security Certification

ISO/IEC 27001:2013

Overview

The International Organization for Standardization 27001 Standard (ISO 27001) is **the world's best-known standard** for implementing an Information Security Management System (ISMS) and specifies best practices to manage, monitor, review, and continuously improve an organization's ISMS. Certification is performed by an independent third party auditor and provides assurance that certain security controls are in place and operating effectively.

Yealink's ISO 27001 Certification

Yealink's latest ISO 27001:2013 certification, which was issued on July 28, 2022, covers the following Yealink products: DECT phone, Video phone, SIP phone, conference phone, conference TV terminal system, headset and accessories. This accreditation certifies that Yealink has implemented best-practice information security processes.

ISO/IEC 27001:2013

SOC 2

Overview

The American Institute of Certified Public Accountants (AICPA) Service Organization Controls (SOC) 2 reports are an independent examination of the

suitability of design and operating effectiveness of a service organization's controls relevant to security, availability, processing integrity, confidentiality, or privacy.

Yealink's SOC 2 Type I Report

Yealink's SOC 2 Type 1 report, which is as of August 18, 2022, provides independent attestation on the suitability of design effectiveness of the controls relevant to the security, availability, and privacy of Yealink Management Cloud Service (YMCS) and Yealink Device Management Platform (YDMP).

Yealink's SOC2 Type II & SOC3 Report

Pending in April 2023.

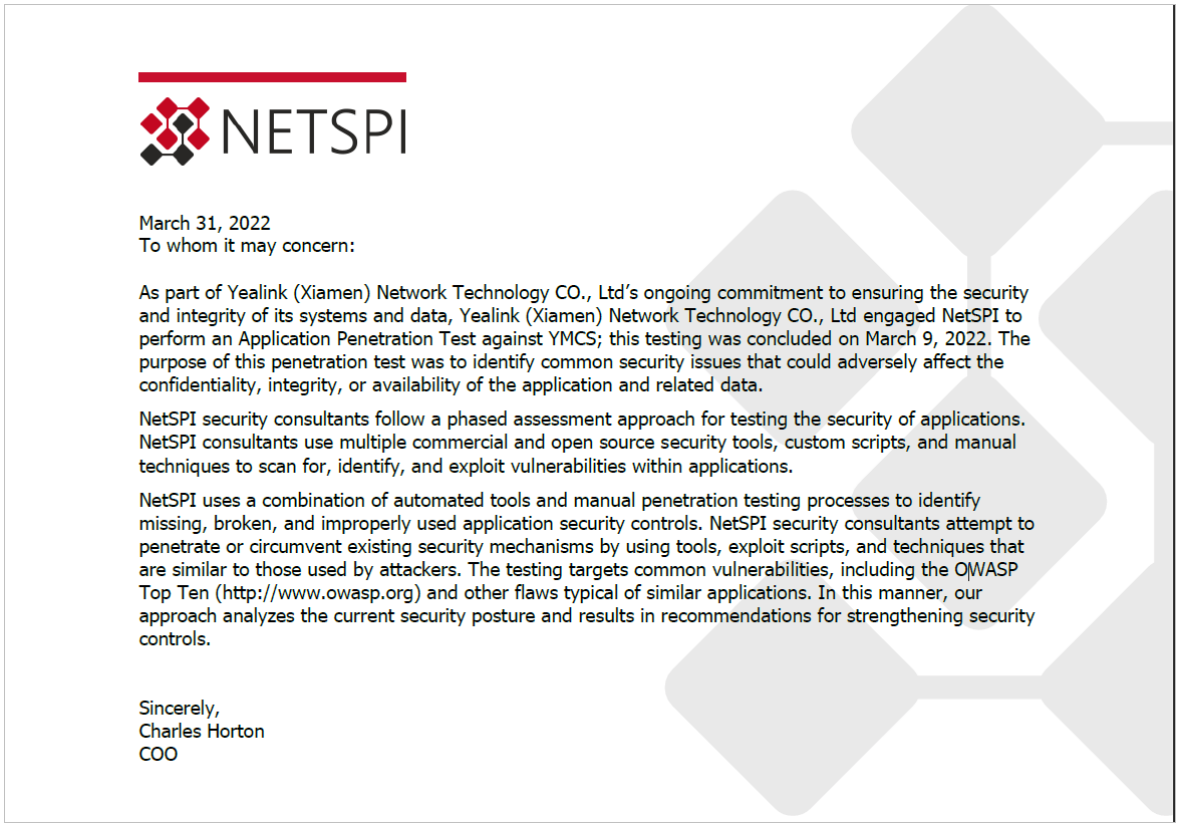
GDPR Compliance

The General Data Protection Regulation (GDPR) has been known **as the world's toughest privacy and security law**. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU

Yealink complies with current EU data protection regulations and has completed an independent GDPR compliance assessment, demonstrating our industry-leading level of data protection and privacy safeguarding.

Penetration Test Independent Security Testing by Leading Labs

Penetration security testing is regularly executed by leading independent labs to meet the toughest security standards. Before any of our products are released, security testing is the most crucial step.



NETSPI

March 31, 2022
To whom it may concern:

As part of Yealink (Xiamen) Network Technology CO., Ltd's ongoing commitment to ensuring the security and integrity of its systems and data, Yealink (Xiamen) Network Technology CO., Ltd engaged NetSPI to perform an Application Penetration Test against YMCS; this testing was concluded on March 9, 2022. The purpose of this penetration test was to identify common security issues that could adversely affect the confidentiality, integrity, or availability of the application and related data.

NetSPI security consultants follow a phased assessment approach for testing the security of applications. NetSPI consultants use multiple commercial and open source security tools, custom scripts, and manual techniques to scan for, identify, and exploit vulnerabilities within applications.

NetSPI uses a combination of automated tools and manual penetration testing processes to identify missing, broken, and improperly used application security controls. NetSPI security consultants attempt to penetrate or circumvent existing security mechanisms by using tools, exploit scripts, and techniques that are similar to those used by attackers. The testing targets common vulnerabilities, including the OWASP Top Ten (http://www.owasp.org) and other flaws typical of similar applications. In this manner, our approach analyzes the current security posture and results in recommendations for strengthening security controls.

Sincerely,
Charles Horton
COO

Yealink

Technical Support

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