Yealink

# SIP Phone Security White Paper

# Contents

**Contents ......................................................................................................1**

**Introduction ...................................................................................................3**

**Hardware Interface Security...........................................................................3**

Debugging Interface ..........................................................................................3

Hardware Penetration Testing............................................................................3

**System Security..............................................................................................4**

Partition Encryption ...........................................................................................4

Secure Boot.......................................................................................................4

Address Space Layout Randomization (ASLR) ...................................................4

BootLoader........................................................................................................4

External Storage................................................................................................4

Firmware Security..............................................................................................4

**Coding Security ..............................................................................................5**

General Coding Security ....................................................................................5

Application Coding Security................................................................................5

Third-Party Components/Libraries......................................................................5

Channel and Port Security..................................................................................6

**Application Security ........................................................................................6**

Permission Security...........................................................................................6

Session Security................................................................................................7

Anti-Brute Force Cracking..................................................................................7

Leak Proof ........................................................................................................7

Data Management.............................................................................................7

Anti-Vulnerability Attack .....................................................................................7

**Communication Security..................................................................................7**

Protocol/Service Security ...................................................................................8

Wireless Transmission Security .........................................................................8

Communication Security Testing.........................................................................8

**Data Security ........................................................................................................9**

Identity Certificate Security...........................................................................9

Encryption Algorithm ....................................................................................9

Hash Algorithm ..............................................................................................9

Weak Algorithm Scanning ............................................................................9

Password Security .........................................................................................9

Configuration and Diagnosis Security.........................................................10

URL Security ...................................................................................................10

**Security Testing Product and Launch ...........................................................10**

Product Launch Process.................................................................................11

Firmware Security Testing .............................................................................11

Code Security Specification...........................................................................11

**Privacy Security ...............................................................................................12**

**Appendixes .......................................................................................................12**

Appendix 1: Spirent Security Test Reports on Yealink Phone Device...........................12

Appendix 2: Network Mapper (Nmap) Port Scanning Reports....................................13

Appendix 3: URLs...............................................................................................17

# Introduction

Device security is the top priority for Yealink.

To improve the security posture of our devices, 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 SIP IP phones 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 Yealink's website.

# Hardware Interface Security

## Debugging Interface

All hardware debugging interfaces are turned off by default at the factory to prevent unnecessary physical debugging interface exposure and information transmission.

## Hardware Penetration Testing

The results of Hardware Reverse Engineering and USB Testing are safe, as shown in appendix 1.

Hardware Reverse Engineering will focus on attempting to identify JTAG headers and debug pins, determining if they are active, and attempting to dump the firmware, sensitive device storage, key store, and other data from the device.

USB Testing uses industry-standard hardware and software for USB analysis and PenTesting (Facedancer) and custom modified and in-house developed fuzzers, protocol analysis, and blob extraction tools. Communication will be reviewed for sensitive communication and authentication, keys, etc. The USB port will be tested to identify additional services available through USB Root Hub, including networking stack etc.

# System Security

## Partition Encryption

Device sensitive information has been encrypted and stored on the memory chip (such as flash, nand, or emmc) through the operating system partition encryption.

## Secure Boot

Support secure boot. Execution of the boot sequence is always authenticated by a previously trusted step. The secure boot chain starts from the bootloader, and the installed firmware validates the digital signature. Authentication will be performed on the device firmware and the primary Flash partition when you start the device. After the authentication succeeds, the device starts.

## Address Space Layout Randomization (ASLR)

ASLR is enabled to prevent buffer overflows.

## BootLoader

The secure boot chain starts from the bootloader, which uses authentication methods to prevent modifying boot parameters to enter the SHELL interface to control the device.

## External Storage

Running programs or scripts from external storage (such as an SD card or USB flash drive) is forbidden to prevent the system from being implanted with malware or scripts.

## Firmware Security

The firmware is encrypted using a Yealink-customized encryption algorithm (SHA-256 or higher) which meets the requirements of a high-strength algorithm.

Authentication is required to install the firmware. Only authentic and correct Yealink firmware can run on

Yealink IP phones.

# Coding Security

## General Coding Security

- **String or Memory Manipulation Functions**

  The system and application use safe string or memory manipulation functions that will perform bounds checking to prevent attackers from carrying out buffer overflow attack.

- **Format Function Parameters**

  The system and application use format functions but not the external controllable variables as parameters to prevent serious harm caused by format string vulnerabilities.

## Application Coding Security

- **Stack Cookie Overflow Protection**

  The CANARY stack overflow protection option of the Linux program is enabled by default when compiling the Linux program code.

- **Stack Non-Executable Protection**

  The NX stack non-executable protection option of the Linux program is enabled by default when compiling the Linux program code.

- **Base Address Random Loading Protection**

  The application enables the base address random loading protection option of the PIE application.

- **Linux Program Code Compilation**

  When compiling Linux program code, use the Strip function to delete the debug symbol table to increase the difficulty of reverse analysis and reduce the program size.

- **System Call Function Parameters**

  When using system call functions in coding, externally controllable parameters should be filtered to prevent command injection.

## Third-Party Components/Libraries

For the third-party components/open-source software involved in the device, we only use the official versions that comply with the open-source license. We do not use any unsecured third-party components, such as low versions, unverified, or from unknown resources.

Also, we will regularly check the official vulnerability announcements and patches of third-party components and fix them in time.

## Channel and Port Security

- **Channel Management Security**

  Support access control on the admin interface, which means that users cannot visit the admin interface using its user login interface. Also, the information viewed and managed by different users varies.

- **Port Attack Defense**

  To defend against DDoS attacks, we only open ports that are necessary and required by users for external communication connections. The communication ports being used will be listed on the product communication matrix documentation, and the dynamic listening ports are limited to a reasonable range. You can also use a port scanning tool (see appendix 2 for the port scanning report by Network Mapper) to ensure that the ports not listed in the communication matrix are closed (and should be closed). In addition to limited open ports, applications using open ports can detect and filter malformed packets and packets that do not meet the rules.

- **Access Security**

  All physical interfaces, communication ports, and protocols that can manage devices have access authentication mechanisms. The login service provided by devices requires users to re-authenticate if users do not operate for some time.

# Application Security

## Permission Security

- **Authentication Bypass**

  To prevent unauthorized users from accessing resources requiring authentication, every request that requires authorized access must be verified whether the user's session ID is legal and the user is authorized.

- **Vertical Ultra Vires**

  Users with low-level permissions cannot access resources that are only available to users with high level permissions.

## Session Security

We adopt Yealink's internal session security management mechanism and various methods to ensure session security.

## Anti-Brute Force Cracking

The authentication module adopts the anti-brute force cracking mechanism. After several failed login attempts, the account or IP address is locked, and it needs to be unlocked to continue access.

## Leak Proof

We use security protocols for encryption when the device transmits the user name and password to the server. For example, the web login needs to use HTTPS. Besides, the configuration file, log, cookie, and debugging trace information show passwords in the ciphertext.

## Data Management

The data processing by the device is done on the device end; that is, the final input processing (authentication), validity (data legitimacy), etc., are all performed on the device.

## Anti-Vulnerability Attack

Yealink devices use the vulnerability scanning tools the industry uses to ensure that the devices are free of medium and high-risk vulnerabilities when they leave the factory.

# Communication Security

# Protocol/Service Security

- **Support TLS 1.3**

  TLS is used to authenticate and encrypt all SIP signaling messages sent between the phone and server. Currently, T3X, T4XU, and T5XW series support the TLS 1.3 to avoid the risk of information leakage or tampering due to the use of plaintext transmission protocols such as HTTP.

- **Support SRTP**

  The device adopts the Secure Real-Time Transport Protocol (SRTP) to provide encryption, message authentication, integrity assurance and protection for real-time voice and video streams transmitted over the network.

- **Support HTTPS**

  The device uses HTTPS security protocol to offer more secure transmission for features like web page login, auto-provisioning update, TR069, etc.

# Wireless Transmission Security

**Support 802.1X**

Support 802.1X. During device pairing, the certificate and TLS key will be burned in via the USB cable. It will not be delivered in the air and thereby has no possibility of being stolen.

**Support WPA3**

Support WPA3 protocol (the device should support Wi-Fi) to efficiently reduce the risk of extracting passwords from attackers by capturing packets or analyzing.

# Communication Security Testing

Yealink devices pass the communication security testing performed by Spirent, including LAN Testing, Communication Encryption Testing, and Wi-Fi Testing. See appendix 1 for details.

**LAN Testing**: Penetration testing of the LAN side of the device will include (where applicable) broadcast traffic inspection/manipulation, port and service enumeration, version fingerprinting/vulnerability identification, Man-in-the-Middle (MitM) testing, client isolation testing and routing/switching attacks.

**Wi-Fi Testing**: Testing will be done on the Wi-Fi interface of the device, both 2.4Ghz and 5.8Ghz bands.

The supplier will analyze pairing, key management, authentication, and susceptibility to common Wi-Fi attacks such as evil twin, DoS, de-authentication, WEP Cracking, jamming, WPA Cracking, WPA Pairing vulnerabilities, Zero Touch configuration vulnerabilities, encryption downgrade attack, session brute-forcing, etc.

**Communication Encryption Testing**: this testing includes malicious analysis and attack testing on secure transmission protocols, encryption algorithms and keys, communication data cracking, and others.

# Data Security

## Identity Certificate Security

Each device is pre-configured with its unique device certificate (encrypted using the SHA-256 algorithm) at the factory. The preset device certificate is used by default during mutual authentication with the server.

## Encryption Algorithm

The device uses secure encryption algorithms and the key length meets the minimum requirements of the corresponding algorithm, such as no less than 128 bits for AES and no less than 256 bits for SHA. Additionally, we do not use insecure encryption algorithms such as DES, TDES, and RC4.

## Hash Algorithm

Use secure hash functions above 256 bits, such as SHA-256, and do not use hash functions with existing security risks, such as MD5 or SHA-1.

## Weak Algorithm Scanning

Third-party security agencies will review the device encryption and algorithm to comply with industry best practices, NIST standards (National Institute of Standards and Technology), and NSA best practices (US National Security Agency). See appendix 1 for details.

## Password Security

### Password Usage

- Users can see obvious prompts when using the default password.
- Modifying passwords must meet security requirements to take effect.
- Support anti-brute force cracking.
- Password transmission adopts RSA encryption.
- The password of any input box cannot be displayed in cleartext, nor does it support copying.
- The account will be automatically logged out when it times out.
- Low-level users cannot modify the information of high-level users.
- The exported configuration files and logs do not contain passwords.

### Password Protection

- The password is not allowed to be stored in the phone in cleartext or using BASE64 encoding.
- When entering the password, it cannot be displayed in cleartext, nor does it support copying.
- In scenarios where password recovery is not required, an irreversible algorithm must be used for encryption.
- The password cannot be stored in cleartext inside the system.

## Configuration and Diagnosis Security

- When exporting the user configuration, the password cannot be exported.
- All passwords in logs are displayed in the ciphertext.
- Support using AES-256 to encrypt configuration files.
- The exported configuration file cannot be decompressed unless it is decrypted using a special security decryption tool.

## URL Security

Yealink device software does not contain any IP addresses, URLs, domain names, email addresses, etc., that are not described in the product documentation. External links are limited to the URLs indicated in appendix 3.

# Security Testing Product and Launch

# Product Launch Process

Yealink follows standard product launch process specifications and sticks to strict software and hardware development life cycle management to ensure the quality and safety of software and hardware products. Each stage (such as design, development, testing, and trial production) will undergo strict review by multiple departments in the hardware development and launch process. In the trial and small batch production stages, the testing and safety teams will ensure product quality standards and safety. The performance is higher than the industry certification requirements.

Before the software version is released, it will go through the Alpha, Beta, and user acceptance testing. Security teams will participate in penetration testing, security scanning, attack surface analysis, and others at each stage.

# Firmware Security Testing

To ensure a secure network environment for software development, firmware packaging and device production, the Yealink security team and IT department regularly perform static and dynamic vulnerability scanning and penetration testing on the production environment and its internal network environment.

Every time before the firmware's official release, the Yealink security team will use a variety of mainstream anti-virus software to scan the firmware to ensure that the firmware is not infected or embedded with viruses or Trojans.

The results of penetration testing for secure boot, malicious firmware analysis, and tampered firmware updates are all safe. See the security report in appendix 1 for details.

# Code Security Specification

Yealink has strict coding security specifications for the R&D teams internally. Code review and reliability verification are performed for each code update.

Device-related codebases have strict permission management mechanisms and Yealink redline requirements. To prevent source code leakage, we forbid uploading codes without permission to public code repositories such as GitHub and Gitee.

# Privacy Security

From the factory to the end of the phone's life cycle, all user data (including account information, contacts, call records, audio and video call information, etc.) are managed directly and locally by the customer in the customer device end. Yealink follows the local privacy protection policy and does not illegally acquire, store and collect of unauthorized customer data by any means.

The user data of the phone device will be stored in an encrypted form to reduce the risk of privacy leakage caused by improper user operations.

The network connection and network access generated by the phone device are determined by the company's internal network and user behavior operations. The phone device will not actively communicate with the IP address or server that the customer does not allow.

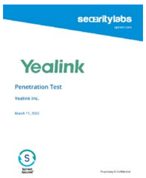
If the user's device fails and needs to be diagnosed and repaired. Yealink has no way to obtain the current information of the device and requires the cooperation and authorization of the customer to export the phone's diagnostic file locally for troubleshooting.

# Appendixes

## Appendix 1: Spirent Security Test Reports on Yealink Phone Device

Founded in 1936, a listed company on the London Stock Exchange, Spirent is the leading provider in communications testing and testing solution fields. Many of the world's leading communications equipment providers and communications network operators have used its testing solutions to evaluate the equipment's latest technologies and performance. The testing fields include safety, performance, function, etc.

Click to view the test report.



securitylabs

spirent.com

Yealink

Penetration Test

Yealink Inc.

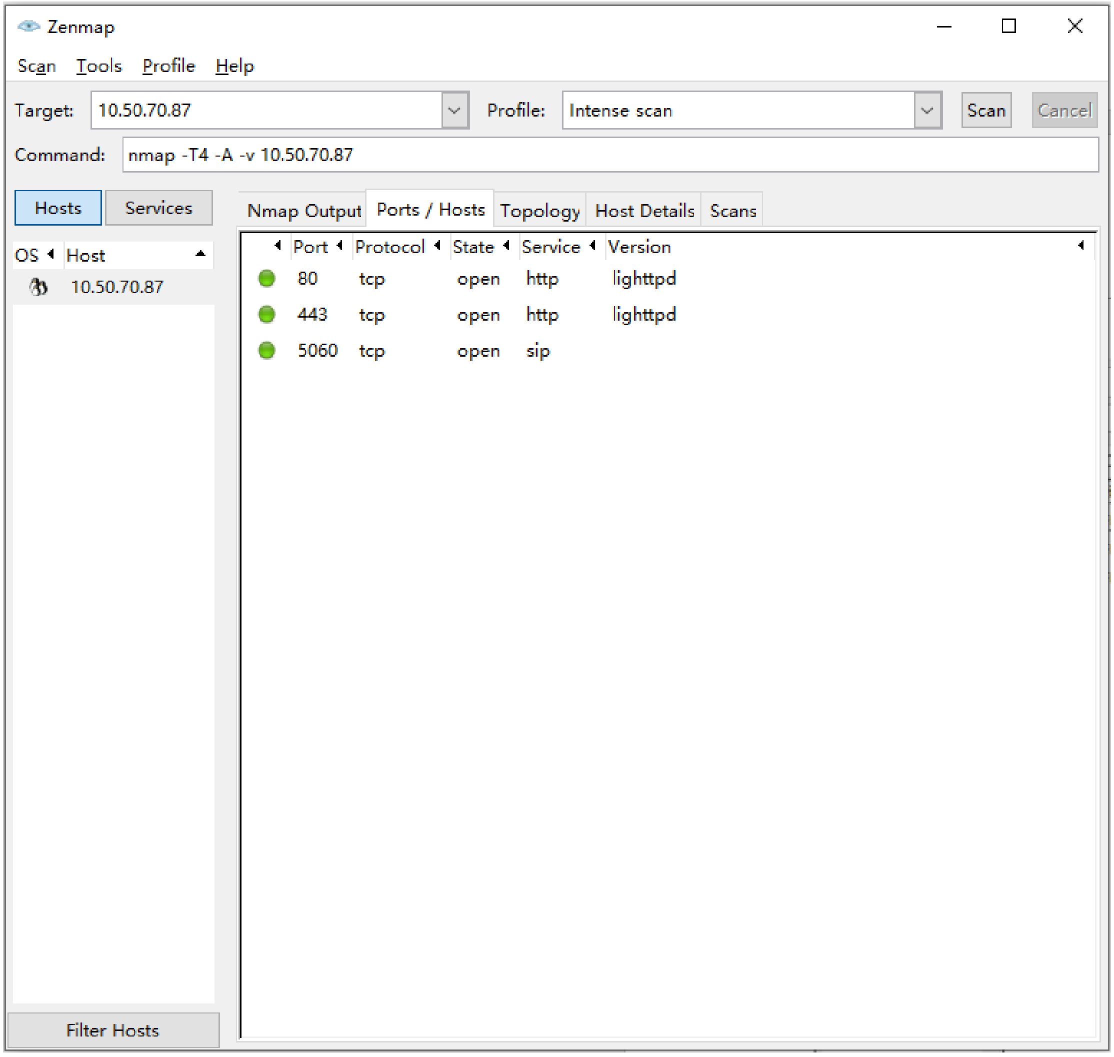
March 11, 2022

Spirent Assured

Proprietary & Confidential

# Appendix 2: Network Mapper (Nmap) Port Scanning Reports

The scanning results of the T3X series:



Target: 10.50.70.87

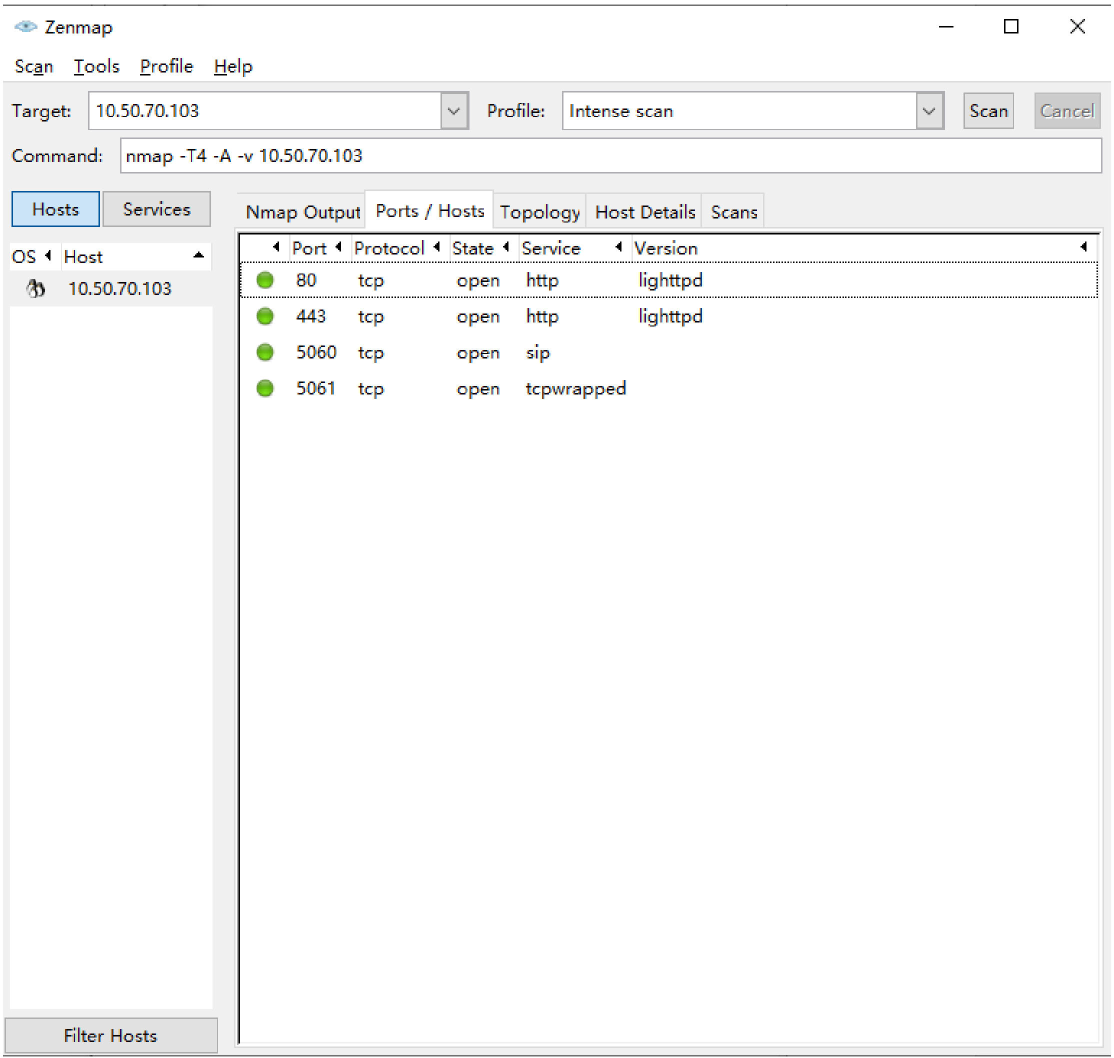
Profile: Intense scan

Command: nmap -T4 -A -v 10.50.70.87

| OS | Host |
|---|---|
| | 10.50.70.87 |

| | Port | Protocol | State | Service | Version |
|---|---|---|---|---|---|
| ● | 80 | tcp | open | http | lighttpd |
| ● | 443 | tcp | open | http | lighttpd |
| ● | 5060 | tcp | open | sip | |

The scanning results of the T4X series:



Target: 10.50.70.103

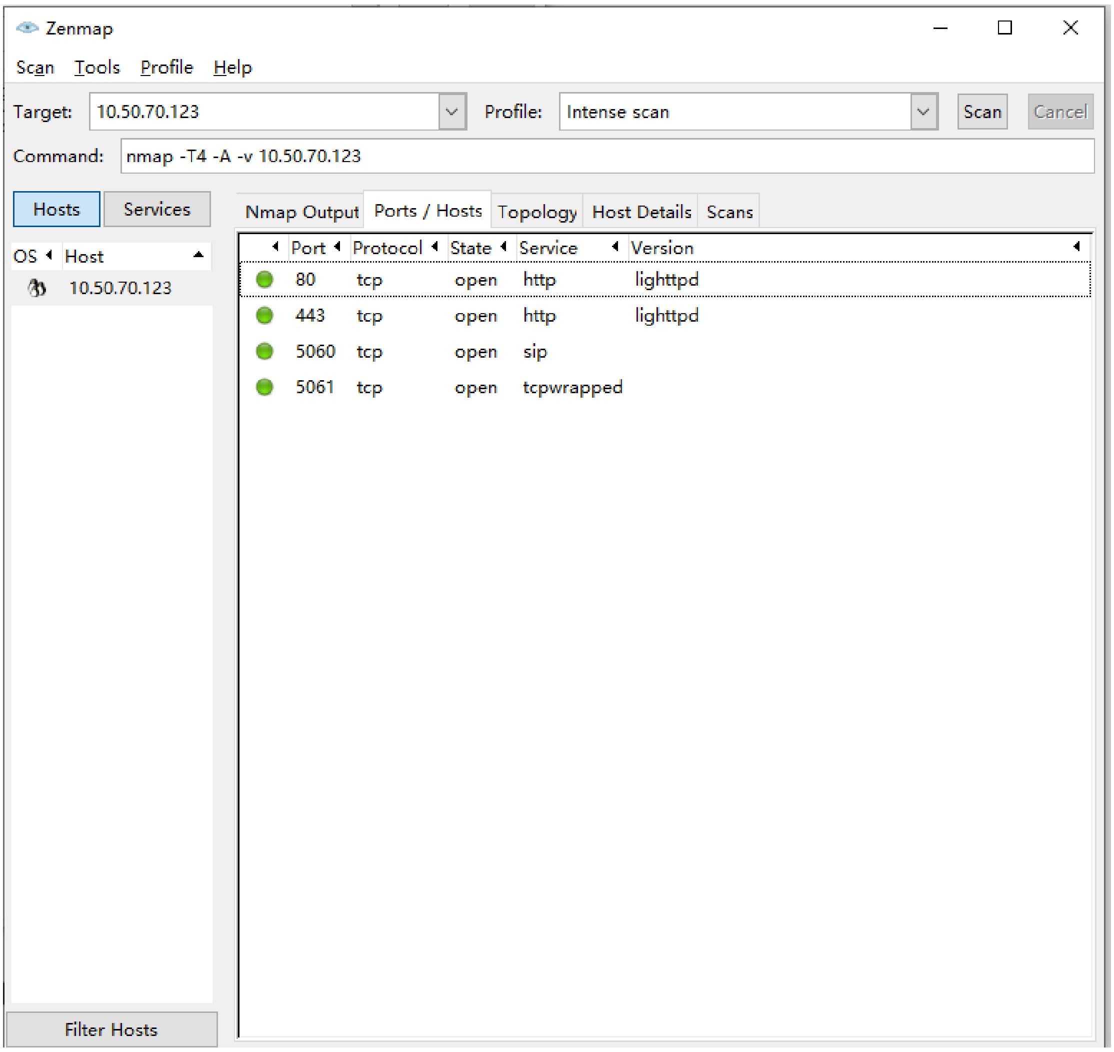
Profile: Intense scan

Command: nmap -T4 -A -v 10.50.70.103

10.50.70.103

| | Port | Protocol | State | Service | Version |
|---|---|---|---|---|---|
| ● | 80 | tcp | open | http | lighttpd |
| ● | 443 | tcp | open | http | lighttpd |
| ● | 5060 | tcp | open | sip | |
| ● | 5061 | tcp | open | tcpwrapped | |

The scanning results of the T5X series:



Target: 10.50.70.123

Profile: Intense scan

Command: nmap -T4 -A -v 10.50.70.123

| | Port | Protocol | State | Service | Version |
|---|---|---|---|---|---|
| ● | 80 | tcp | open | http | lighttpd |
| ● | 443 | tcp | open | http | lighttpd |
| ● | 5060 | tcp | open | sip | |
| ● | 5061 | tcp | open | tcpwrapped | |

The device port matrix is described as follows:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Nmap Version | 7.80 | | | | | | | |
| Nmap port scanning result | | | | | | | | |
| Features | Listening port | Transport layer protocol | Usage | Can I change the port? | Configuration line | Default value | Authentication method | Encryption method |
| SIP | 5060 | UDP | SIP UDP listening port | Yes | sip.listen_port | Enabled | The user name/password of the SIP account | None |
| SIP | 5061 | TCP | SIP TCP listening port | Yes | sip.tls_listen_port | Enabled | The user name/password of the SIP account | TLS |
| WEB server | 443 | TCP | WEB TLS access port | Yes | static.network.port.https | Enabled | The user name/password of the phone admin account | TLS |
| WEB | 80 | TCP | WEB | Yes | static.network.po | Enabl | The user | None |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| server | | | TCP access port | | rt.http | ed | name/password of the phone admin account | |

**Note**: Nmap (Network Mapper) is an open-source tool for network detection and security auditing. It can quickly scan the network in a novel way using raw IP packets. Therefore, it can determine which hosts are available, services provided (application name and version), running operating system (OS version), packet filters/the types of firewalls, and dozens of other features.

# Appendix 3: URLs

The product software is not allowed to include unpublished public network addresses that are not visible in the user interface or not described in the product documentation. The public network addresses contain IP addresses, public network URL addresses/domain names, and email addresses. The URLs we mentioned in the documentation are the support website and some server addresses, as described in the following table:

| Resource IP Address | Target IP address | Data Packet Type | Feature Description | Configuration Line |
|---|---|---|---|---|
| Phone IP address | cn.pool.ntp.org | TCP | NTP server | local_time.ntp_server1<br>local_time.ntp_server2 |
| Phone IP address | rpscloud.yealink.com | TCP | RPS server | static.redirect.enable |
| Phone IP address | 224.0.1.75 | SIP | PNP data packet | static.auto_provision.pnp_enable |

## Disclaimer

This white paper is provided for informational purposes only and does not convey any legal rights to any intellectual property in any Yealink product. You may copy and use this paper for your internal reference purposes only.

YEALINK MAKES NO WARRANTIES, EXPRESS OR IMPLIED OR STATUTORY AS TO THE INFORMATION IN THIS WHITE PAPER.

To learn more about Yealink IP Phone Series devices, visit our website.