securitylabs

spirent.com

Penetration Test

Yealink Inc.

March 11, 2022

Low Risk

Security Consultants from Spirent SecurityLabs executed a penetration test of the systems under review. Consultants utilized a combination of open-source, proprietary, and custom tools to enumerate vulnerabilities within the system and its components and tested those vulnerabilities for exploitability. Spirent's penetration tests conform to the recommendations set forth in NIST 800-115 section 5. The process consists of multiple phases – planning, reconnaissance, scanning, exploitation, post-exploitation, and reporting. During the planning and reconnaissance phases, Spirent collaborated with representatives from Yealink Inc. to determine the Rules of Engagement and confirm systems which are in scope for testing. Consultants then proceed through a loop of scanning, exploitation, and post-exploitation as the consultants attempt to gain a foothold in the environment and expand their access. Spirent SecurityLabs rates the overall risk posed by the assets in this penetration test as Low. Since no vulnerabilities were discovered there are no actions needed, but be aware there is no such thing as a totally secure application or device, so continued vigilance should be observed along with periodic security testing.

Summary

Target Details	**Test Name:** T54W **Test Target:** T54W Firmware 96.86.0.60	**Target Environment:** Production **Status:** Completed
Date/Time	**Started On:** 03/02/2022	**Finished On:** 03/11/2022
All Findings	Critical: 0 High: 0 Medium: 0 Low: 0	

Test Results

Classification	Severity	Count

Reconnaissance

Hardware Name	Firmware Version
T54W	96.86.0.60

Testing Methodology

Open Source Intelligence Gathering [OSINT] for the device
Open Source Intelligence gathering about the vulnerabilities and unlock functionality discovered by phone enthusiasts and hackers in the device. OSINT will be gathered on public and semi-private forums as well as on invite only forums on clearnet and darknet, as well as from established contacts.

Device Security Tests
Device Penetration Testing will cover both industry best practices as well as goal based testing. Goal based testing will attempt to meet the capture of certain flags. The flags will include demonstrating the ability to root the device at will.

- Password Management
- Authentication
- Access Controls
- Patch Management
- Software Updates
- Audit Log
- Communication Encryption
- Multi-factor Authentication
- Remote Deactivation
- Secure Booting
- Device Identity
- Encrypted Data Storage
- Digital Signatures
- Tamper Evidence
- Design-In Features
- Malicious firmware updates
- USB Host attacks
- Routing

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

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.

Tethered Testing
Testing the device over USB connection in tethered mode, as well as exploring possible USB-OTG capability, mass file storage and device pairing. Testing will be conducted to attempt to gain access to the device file system, sensitive files, credentials, firmware as well as configuration files via the USB port. Engineering utilities collected during the OSINT portion of the assessment will be utilized during this phase as well.

Unintended Functionality

Go to Test Results »

Identifying unlock codes, secret codes, menus, engineering interfaces including 4G LTE provisioning menus which may have been left behind in the code for troubleshooting and diagnostics. Any issues identified during this time are likely to be discovered quickly by the general public and on phone enthusiast forums. The identification will ensure that any interfaces not intended for most users are not easily identified or easily accessible. This phase of testing will cover the front LCD interface as well as USB and web interface.

Hardware Reverse Engineering
This phase 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 as well as other data from the device. This will include data at rest as well as data in motion.
Vulnerable services
Identification of services running on the device (if applicable). Identification of vulnerable services, as well as services configured insecurely.

Encryption
Supplier will review the ciphers, other crypto and crypto-related algorithms like asymmetric key signing/verification, key agreement protocols, key derivation, message authentication, random number generation and cryptographic suites chosen for various functions of the Infrared Heating device.
Supplier will review to ensure the implementation of cryptographic functions and algorithms is consistent with industry best practices, NIST standards, NSA best practices.

Cryptanalysis
Supplier will perform analysis of recovered data, communication, data at rest, data in motion, cryptographic key storage. Data will be analyzed using known plain text attacks
Supplier will utilize its expertise, industry standard software as well as custom developed software and our private cracking servers to aid in these efforts.

Update/Upgrade
Supplier will review the update mechanism for encryption methods, secure transmission, and exposure of sensitive data.

WiFi Testing
Testing will be done on the Wifi interface of the device, both 2.4Ghz and 5.8Ghz band. Supplier will analyze pairing, key management, authentication, susceptibility to common WiFi attacks such as evil twin, DoS, deauthentication, WEP Cracking, jamming, WPA Cracking, WPA Pairing vulnerabilities, Zero Touch configuration vulnerabilities, encryption downgrade attack, session brute forcing, etc.

Web Application Analysis:
Analysis of web applications includes scanning and modifying requests using commercial tools to find any vulnerability such as SQL, XSS, Authentication, etc. that can be exploitable. Potential vulnerabilities from scanning are tested to determine if it is a false positive.

Go to Test Results »

Narrative

- **Recon**
  - Obtained firmware images from Yealink.
  - Reviewed documentation for phone operations and default access.
- **Hardware Interfacing**
  - Performed a device teardown and identified serial interfacing points.
  - The device components were also identified and categorized.
  - The SoC and flash storage was identified and accessed.
- **Firmware Analysis**
  - After studying the downloaded firmware, it was determined that the images were encrypted using an unknown cipher and key.
  - A binary(version), LZMA compressed blob(rfs), and an encrypted blob(bootloader) was extracted from the firmware image.
  - The extracted version binary appears to be used to process firmware images.
  - The rfs LZMA blob was decompressed and an encrypted UBIFS filesystem was found.
  - The bootloader encrypted blob appears to be encrypted with "cypher 3".
- **Scanning**
  - Network scanning of the phones were performed to identify any open ports.
- **Web App Analysis**
  - Web application was scanned and analyzed for any vulnerability based on the OWASP top ten web app security risk.
  - Any potential risks were tested.

Go to Test Results »

Go to Test Results »