NetSPI™

Embedded Penetration Test

Remediation Report

Project: Meeting Bar A40

Yealink

September 3, 2024

NetSPI™

Contents

Chapter 1 | Project Summary

On August 30, 2024, NetSPI performed remediation testing against Yealink's Meeting Board A40 to verify that the issues identified in the penetration test conducted between June 4, 2024, and June 10, 2024, had been fixed. The original test, as well as this remediation test, were performed by NetSPI to identify vulnerabilities, determine the level of risk they present to Yealink, and provide actionable recommendations to reduce this risk. NetSPI compiled this report to provide Yealink with detailed information on each vulnerability discovered within the Meeting Board A40, including potential business impacts and specific remediation instructions. Unless otherwise noted, all tested vulnerabilities that were found to be not remediated use the original verification steps to exploit the finding.

1.1 Project Objectives

NetSPI's primary goal within this project was to provide Yealink with an understanding of the current level of security in the device and its infrastructure components.

NetSPI completed the following objectives to accomplish this goal:

- Identifying application-based threats to and vulnerabilities in the device and application
- Identifying network-based threats to and vulnerabilities in the device
- Identifying hardware-based threats to and vulnerabilities in the device
- Comparing Yealink's current security measures with industry best practices
- Providing recommendations that Yealink can implement to mitigate threats and vulnerabilities and meet industry best practices

1.2 Scope & Timeframe

Initial testing and verification were performed between June 4, 2024 and June 10, 2024. The scope of this project was limited to the following devices, associated firmware, and embedded applications.

PRODUCT SERIES	TEST MODEL	FIRMWARE VERSION
Meeting Bar	A40	289.320.0.20

NetSPI conducted the tests using a production version of the devices. All other applications and servers were out of scope. All testing and verification were conducted from outside of Yealink's offices.

1.3 Summary of Findings

NetSPI's assessment of the Meeting Bar A40 device revealed the following vulnerabilities:

- 1 low severity vulnerability
- 1 informational severity vulnerability

VULNERABILITY NAME	SEVERITY	REMEDIATION STATUS
Weak Physical Controls - Missing or Inadequate Tamper Mechanisms	Low	Remediated
Weak Session Management - Concurrent Sessions Allowed	Informational	Partially Remediated

TABLE 1: FINDINGS SUMMARY

1.4 Network Geolocation Audit

At the request of Yealink, NetSPI audited the network traffic of the device during the firmware upgrade process as well as normal operation looking for traffic to hostnames or IP addresses which geolocate within the People's Republic of China. No such traffic was discovered.

Chapter 2 | Technical Detail

2.1 Overview

The detailed findings section contains the analysis and documentation of the vulnerabilities identified within the Yealink device. This analysis included:

- Identifying potential vulnerabilities associated with the device
- Assigning appropriate severity rankings to valid vulnerabilities and risks
- Formulating useful action-based recommendations that can improve the security posture of the IT environment

Vulnerabilities are grouped according to severity. Information for each of the vulnerabilities includes the following:

Name: The name of the vulnerability.

Severity: Each of the vulnerabilities has been assigned a severity based on its impact to the application and its associated resources. The following table summarizes the three severity levels:

SEVERITY	DESCRIPTION
High	Vulnerabilities that result in unauthorized access to application data or functionality, unauthorized access to the server file system, OS command execution, and exposure of sensitive data (e.g., personally identifiable information).
Medium	Vulnerabilities that result in the exposure of session data or security configuration information. Unencrypted transmission of sensitive data or use of weak encryption methods.
Low	Vulnerabilities that result in the exposure version information or non-critical configuration information. Implementation of weak password policies and procedures. Informational findings that may not require any remediation.

TABLE 2: SEVERITY REFERENCES

The severity ratings in this document are based upon industry standard and do not necessarily take into consideration the environment in which the vulnerabilities exist, other controls that maybe implemented within that environment, or an organization's classification of the information or functionality. As a result, the severity ratings in this document will not clearly represent the overall risk to an organization for each vulnerability instance.

Affected Assets and Services: Specific assets and associated services on which the vulnerability was found.

Vulnerability Details: Comprehensive explanation of the vulnerability that was found, including a high-level summary of how the vulnerability works.

Business Impact: This describes the potential business impact of the vulnerability, should it be exploited.

Recommendation: NetSPI's solution for repairing the vulnerability or mitigating the problem if no fix is yet available.

Affected URLs and Parameters: URLs and parameters associated with the finding, if applicable.

Affected Code: A list of affected code, including module name and line number, if applicable.

Verification: Screenshot or sample data from one instance of the finding showing how NetSPI has verified the finding manually, when possible.

References: These are other resources that have more information on the vulnerability.

2.2 Low Severity Findings

2.2.1 Weak Physical Controls - Missing or Inadequate Tamper Mechanisms [Remediated]

Severity: Low

Affected Assets and Services

ASSET
MeetingBar A40

Vulnerability Details

The affected devices did not have adequate physical controls to prevent users from dismantling or modifying the hardware. Equipment can be reconstructed and fully functional without evidence of potential manipulation. Tamper protection needs to alert the user or technician as to a change, even if the case was altered while the device was powered off.

Impact

A threat agent could access the device or embed malicious equipment in the device casing to target end users.

Recommendation

Include anti-tamper sensors into the design. Simple sensors can include resistive foils that tear if tampered with, or jumpers that will be removed if the case is disassembled. These passive tests will allow tamper warnings even if the device was altered in a powered off state. However, the warnings will likely only occur once the device is powered back on.

Implement tamper evident materials to notify users that a device may have been compromised. Such materials include housing adhesives, seals, or labels, but be warned that labels are easily purchased and replaced with common printing techniques.

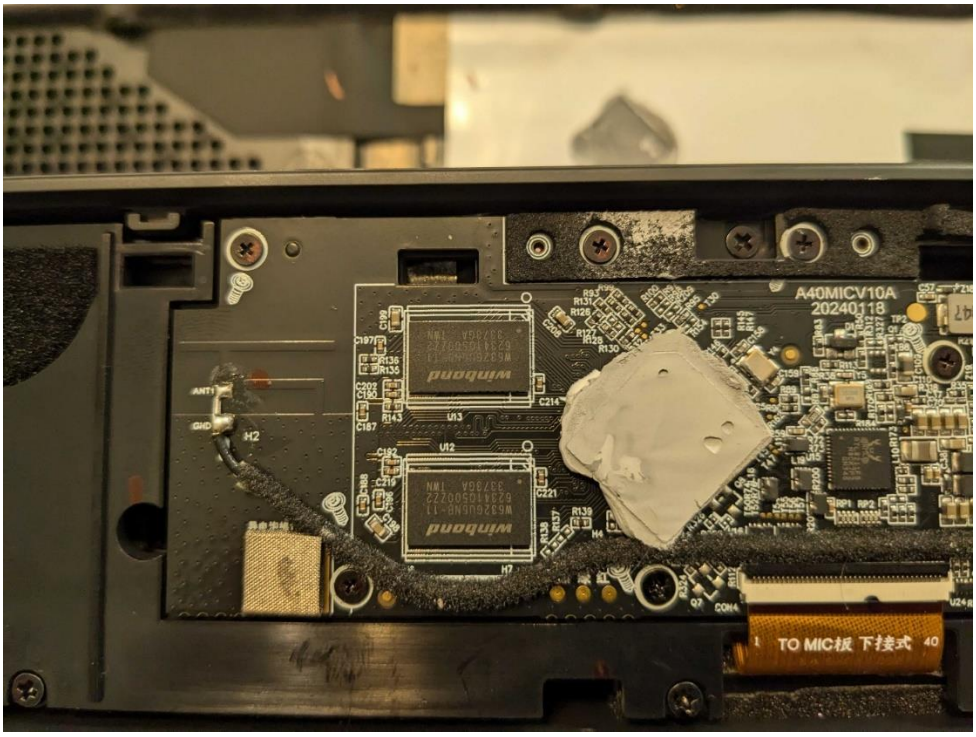
Additionally, consider utilizing security screws and bits during the manufacturing process to prevent rudimentary hardware-based attacks.

Verification

Scenario 1

Remediation Testing Observation – 08/30/2024: Yealink provided NetSPI with details on anti-tamper stickers that will be placed on the device during production. As such, NetSPI reviewed the instance and found it was remediated.

1. The device enclosure is fastened with cross head screws. Upon opening the enclosure there was no found method to alert the device or user that the device had been opened and tampered with. Nor was there any indication that the device behaved in a different manner after the device was opened.



2. The following image was provided to NetSPI as an example of the anti-tamper stickers that will be placed on the device in production.

2.3 Informational Severity Findings

2.3.1 Weak Session Management - Concurrent Sessions Allowed [Partially Remediated]

Severity: Informational

Affected Assets and Services

ASSET
MeetingBar A40

Vulnerability Details

The affected application allows concurrent account logins. Concurrent logins allow two or more sessions to be active for one user at a time. As a result, unauthorized users may be able to use the application without the owner's knowledge.

Impact

Concurrent logins may allow an attacker to access the application and use that application without being noticed.

Recommendation

Do not allow concurrent login sessions.

Solutions include, but are not limited to the list below:

- Generating a new session identifier for each page and destroying each session identifier after it is used.
- Tracking user sessions with a database and logging out users who have more than one session active.

If users are automatically logged out via either of these methods, display a message that states the session was reset due to multiple active user sessions.

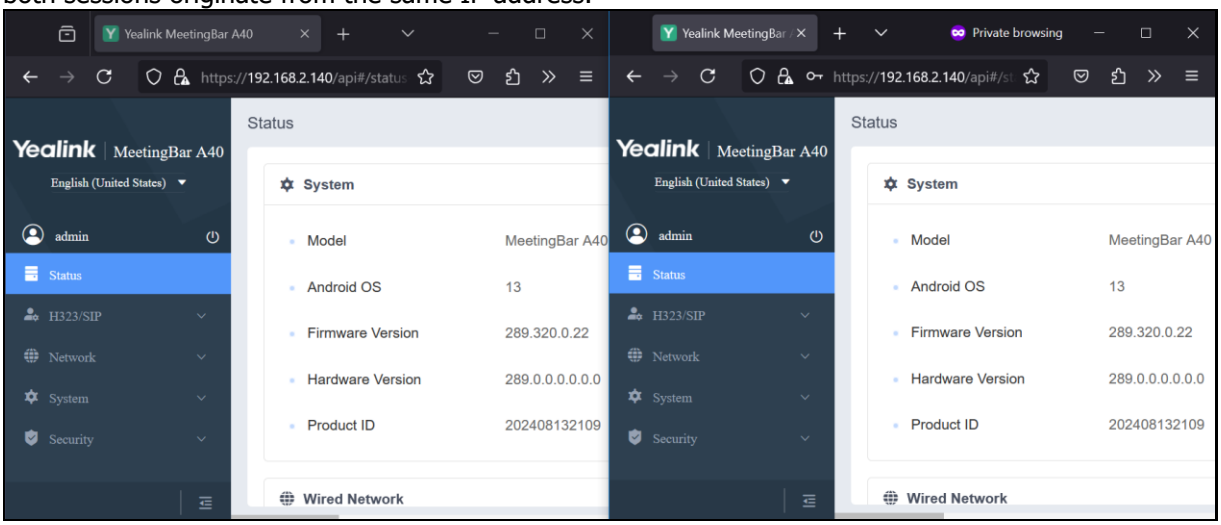
Verification

Scenario 1

Remediation Testing Observation - 08/30/2024: NetSPI reviewed the instance and found it was partially remediated. Initially, the device's web server allowed for concurrent sessions regardless of IP. During the remediation test, it was found that concurrent sessions were still allowed as long as both sessions originated from the same IP address. New verification steps have been provided to show the current method of exploitation. NOTE: The original verification steps can be found in the initial penetration test report.

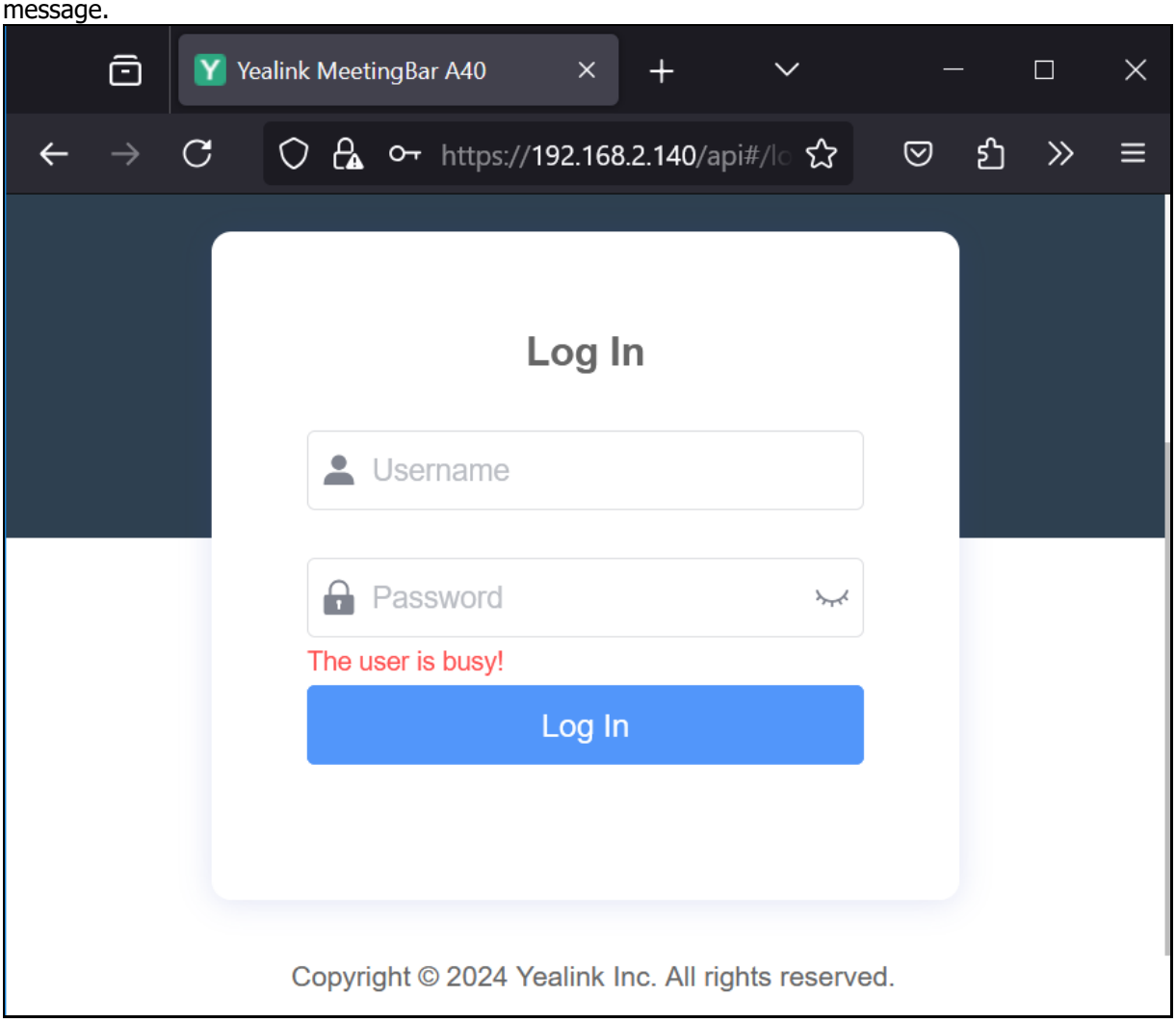
1. Log into the administrative web application in two separate browsers (or Private/Incognito Mode) from the same machine.

Observe that the application allows both sessions to remain active without informing the user. Note that both sessions originate from the same IP address.



2. Log into the administrative web application from two different machines with different IP addresses.

Observe that when attempting to login to the second session, the user receives a "The user is busy!" message.



Appendix A | NetSPI Contact Information

Please contact NetSPI with any questions regarding the findings, analysis, or recommendations contained in this report.

Consultant
Chas Becht
Chas.Becht@netspi.com
+14049540583

Project Manager
Vahid Shaikh
vahid.shaikh@netspi.com
+918879888808

Account Manager
Ryan Black
Ryan.Black@netspi.com
+447762892855

Appendix B | IoT Penetration Test Methodology

The following sections provide an overview of the Embedded Penetration Test.

Information Gathering

During each Embedded Penetration Test, NetSPI first works with Yealink to define project requirements and goals, identify areas of risk and concern, and gather the information necessary to assess the device. A walkthrough is performed with Yealink to help NetSPI better understand the device's architecture and business logic requirements, as well as to align expectations in terms of the testing approach. This information is used by the primary consultant and supporting team members to develop a test plan. This test plan is used as a basis for assessing the device and serves as a quality assurance measure.

Testing and Evaluation

NetSPI assesses Yealink's device(s), associated applications, and associated infrastructure for known security vulnerabilities from the perspectives of anonymous and authenticated users. If multiple user types exist, testing is performed for each type. During the assessment, manual and automated processes are followed that leverage commercial, open source, and proprietary software. All automated test results are manually verified to reduce false positives. NetSPI also conducts manual testing to identify data flow, business logic, and access control issues. The assessment includes testing for OWASP IOT Top 10 2018 vulnerabilities.

CATEGORY	DESCRIPTION
I1-Weak, Guessable, or Hardcoded Passwords	This covers use of easily bruteforced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorized access to deployed systems.
I2-Insecure Network Services	This covers unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorized remote control.
I3-Insecure Ecosystem Interfaces	This category covers insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.
I4-Lack of Secure Update Mechanism	This covers a lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.
I5-Use of Insecure or Outdated Components	This category covers the use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.
I6-Insufficient Privacy Protection	This covers occurrences where personal user information is stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.
I7-Insecure Data Transfer and Storage	This category covers a lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.
I8-Lack of Device Management	This category covers a lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.
I9-Insecure Default Settings	This covers devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.

CATEGORY	DESCRIPTION
I10-Lack of Physical Hardening	This category covers a lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

Data Analysis

All of the data collected is consolidated and analyzed using the NetSPI Resolve™ platform. Additional research is conducted to identify known vulnerabilities for individual application components. Additionally, vulnerabilities are prioritized based on the Payment Card Industry (PCI) severity system. After identifying, analyzing, and prioritizing vulnerabilities, NetSPI formulates recommendations for mitigating each of these security issues. During this phase, supporting team members walk through the test plan with the primary consultant to ensure the integrity of the results. A report containing findings and recommendations is then generated by the primary consultant and placed through both technical and stylistic review of supporting team members, as well as through a final review by the engagement manager.

Basis for Opinions

The industry standards on which NetSPI bases many of its recommendations are the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) standard 27002:2005, the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) guidelines. ISO/IEC 27002:2005 has become one of the strongest industry standards within the security industry and it contains guidelines for successful security policy, architecture, and configuration. The NIST and NSA guidelines are more detailed configuration guidelines with regard to devices and systems within the IT environment.

NetSPI also used secure coding guidelines such as those provided by the Open Web Application Security Project (www.owasp.org). NetSPI uses guidelines from the "OWASP Top 10 Internet of Things 2018" to review custom hardware and firmware and identify vulnerabilities.

Additionally, NetSPI bases findings and recommendations on industry regulations including the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), the Payment Card Industry (PCI) Data Security Standard, Sarbanes Oxley Act (SOX), and individual state privacy legislation.

Collaboration

In this phase, NetSPI presents an overview of the findings and delivers the preliminary report to the Yealink project team. NetSPI reviews the device's strengths and weaknesses with Yealink and discusses the recommendations for addressing security deficiencies. Yealink will have an opportunity to provide feedback and guidance for report revisions and the final presentation.

Presentation

After an agreed-upon timeframe, NetSPI finalizes the report, incorporating any feedback from Yealink. This document in the final version is delivered in all required formats and to all required parties.

Appendix C | Risk Management Approach Overview

This section provides an overview of the risk management approach used by NetSPI during the project.

1. NetSPI worked with the client to identify the individuals from both sides that needed to be involved or made aware of the project. In the event of an issue, good communication helps ensure that emergency reactions to testing activities are not made; ad-hoc system changes during the test may invalidate test results and result in a service disruption.

2. NetSPI worked with the client to identify potential areas of risk that relate to the networks, systems, and applications that were tested directly or could be affected by tested.

3. NetSPI and the client created and executed on action items to address the identified areas of risk. Responsibilities were assigned to both teams.

4. NetSPI and the client created an escalation procedure that included a calling tree to address and reduce the impact of potential incidents. Calling trees typically include up to three contacts from the NetSPI and the client to ensure that the appropriate action can be taken as soon as possible.

Revision History

VERSION	DATE	AUTHOR	COMMENTS
0.1	July 3, 2024	Chas Becht	Document Created
0.2	July 3, 2024	Larry Trowell	Report QA
1.0	July 4, 2024	Vahid Shaikh	Report Delivery
1.1	August 30, 2024	Carolyn Matous	Remediation Document
2.0	September 3, 2024	Vahid Shaikh	Remediation Report Delivery