NETSPI

Embedded Systems Test

Executive Summary

Project: MVC 860

Yealink

January 8, 2024

Contents

Chapter 1 | Project Summary

NetSPI performed an analysis of Yealink (Xiamen) Network Technology CO., Ltd's (Yealink) MVC 860 device 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 MVC 860 device, including potential business impacts and specific remediation instructions.

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 MVC 860 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

Testing and verification was performed between September 5, 2023 and September 22, 2023. The scope of this project was limited to the following devices, associated firmware, and embedded applications.

COMPONENT	VERSION
Mini PC	MCore Pro
UVC86	151.431.0.15
MTouch Plus	282.410.0.25
Yealink RoomConnect Application	2.31.67.0

NetSPI conducted the tests using a production version of MVC 860. All Production MVC Series devices use identical software and firmware. All other applications and servers were out of scope. All testing and verification was conducted from outside of Yealink's offices.

1.3 Summary of Findings

NetSPI's assessment of the MVC 860 device revealed the following vulnerabilities:

- 1 high severity vulnerability
- 2 medium severity vulnerabilities
- 2 informational severity vulnerability

VULNERABILITY NAME	SEVERITY	REMEDIATION STATUS
Private key disclosed	High	Remediated
Common Private Key	Medium	Remediated
Unsupported Version - Microsoft VC Runtime	Medium	Remediated

VULNERABILITY NAME	SEVERITY	REMEDIATION STATUS
Weak or Default Password - Local Administrator Password	Informational	Not Remediated
Weak Assembly Control - Expired Signing Certificate	Informational	Remediated

TABLE 1: FINDINGS SUMMARY

The Default Local Administrator Password is specified by Microsoft as required for all Teams Room devices. See https://learn.microsoft.com/en-us/microsoftteams/rooms/security?tabs=Windows#account-security for more information.

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.