Yealink MVC Series Room Systems

for Microsoft Teams

Certified Secure Assessment

March 2021

DR21031E

Contents

1.0 Executive Summary

With working at home and remote company life becoming an increasing trend, virtual conferencing platforms have become a staple necessity for enterprises for basic communication. Enterprises rely on video unified communications conferencing solutions to exchange sensitive company information during remote meetings. The dramatically expanded use of video conferencing systems by business has become a much larger target of opportunity for attackers. Businesses need to ensure the video conferencing solutions they rely for these communications are inherently secure.

Yealink offers video conferencing, voice communications, and collaboration solutions while providing consumers with high-end security and data protection. By following the specifications provided by Microsoft, Yealink delivers secure video conferencing services in conjunction with high quality and performance. The Yealink solution is secure provided parameters of deployment of Microsoft Teams, Groups and or Skype are adhered, as well as effective Microsoft Endpoint management and security are provided.

Yealink engaged Miercom to conduct a security vulnerability assessment on two different Microsoft Teams Rooms system deployments. Vulnerability tests were conducted on each solution in a real-world environment to evaluate protective measures as well as identify strengths and opportunities for security hardening regarding Yealink hardware and software.

Key Findings

- Analysis of data in transit was proven encrypted
- Tamper resistant design verified on MCore and peripherals, including security locks to prevent theft and tampering
- No vulnerable APIs, Windows services or ports were found on the Yealink networked components in test

Based on our findings, the Yealink MVC Product family demonstrates competitively superior security and performance tested with real-world exploits and stressful conditions. We proudly award the Yealink MVC Rooms Systems for Microsoft Teams the ***Miercom Certified Secure*** certification.

2.0 Test Summary

Physical Hardware and Accessibility	**Pass**
Encryption	**Pass**
Data Integrity	**Pass**
Endpoint Vulnerability Scanning	**Pass**

3.0 Introduction

The scope of testing included physical security analysis of Yealink MVC400 and MVC840 MCore Mini-PC components as well as the included peripherals for each solution. The MVC Series uses a common mini-pc and touch console with a combination of different grade audio and video components to match a customer's specific needs. Vulnerability assessments were conducted on each component within a simulated business environment to ensure secure functionality after deployment. A security assessment of Yealink communications in this simulated environment was also conducted in order to analyze the confidentiality and integrity of data in transit.

3.1 Products to be Tested

Yealink MVC840
Microsoft Teams certified video conferencing system for large rooms. Includes the MCore Mini-PC, MTouch II Touch Panel, UVC84 USB PTZ Camera, VCM34 Array Microphone, and Yealink Soundbar. This video conferencing system will be utilizing a Windows 10 deployment.

Yealink MVC400
Microsoft Teams certified video conferencing system for small rooms. Includes the MCore Mini-PC, MTouch II Touch Panel, and UVC40 USB Video Bar. This video conferencing system will be utilizing a Windows 10 deployment.

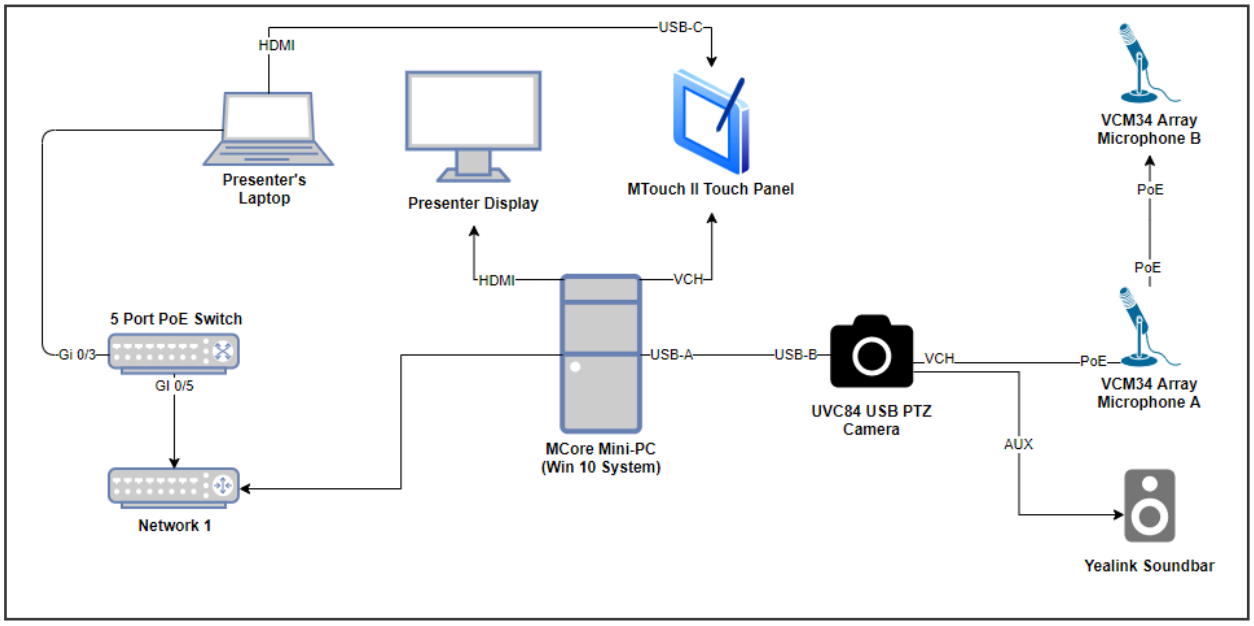
Testing focused on the following:

- Physical Security of Hardware Components
- Data Integrity and Confidentiality
- Network Component Security

4.0 How We Did It

Using a simulated enterprise network environment, we tested MVC840 and the MVC400 for basic functionality while conducting monitoring and penetration testing activities.

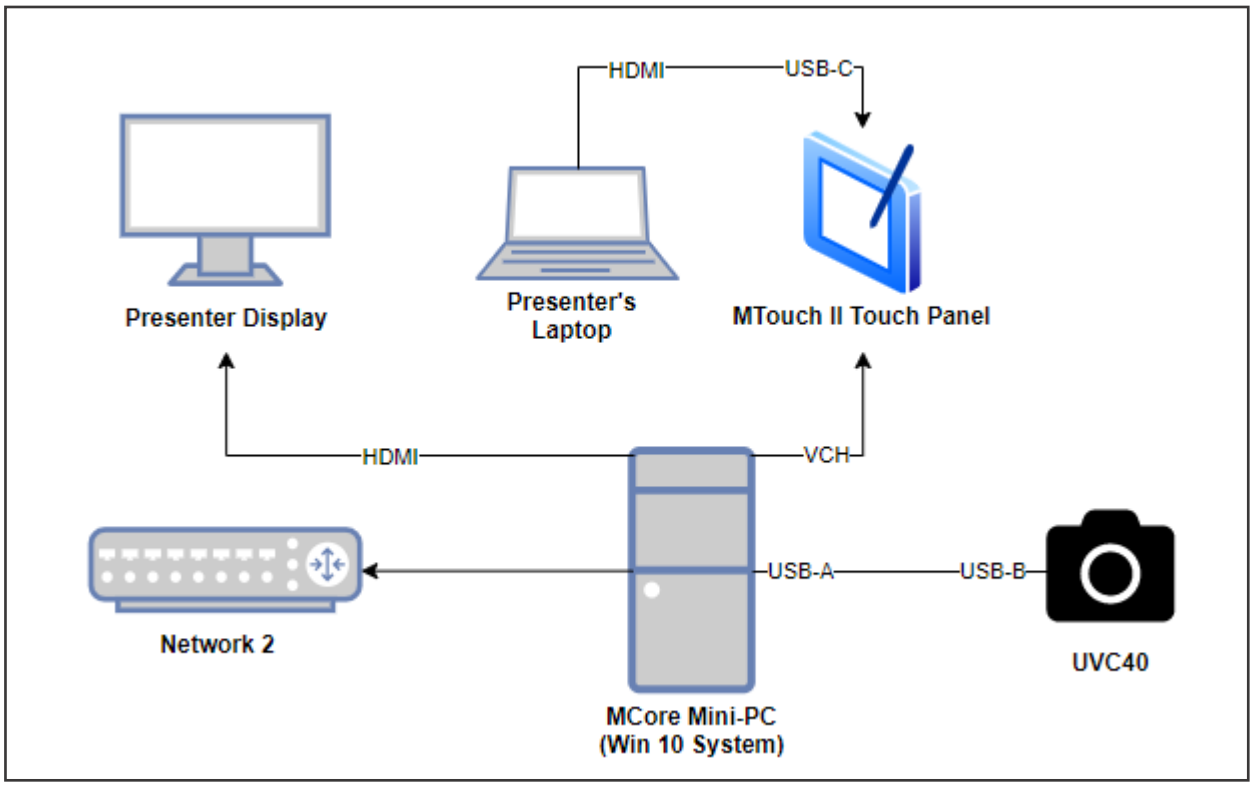
Test Bed Overview 1



The network topology above was used for the MVC840 deployment. With the MCore Mini-PC as the centerpiece, the PoE switch will be connected to the supporting network and will also include the Presenter's Laptop. This will act as the interface for the user. The USB-A to USB-B connects the UVC84 USB PTZ Camera to the two VCM34 Array Microphones and the Yealink Soundbar and will deliver and receive audio/visuals to supplement the meeting experience. Lastly, the Presenter's Display will display what the user decides based on their interactions with the MTouch II Touch Panel.

Device/Feature
UVC84 Camera
MTouch II Touch Panel
Microsoft Windows 10

Test Bed Overview 2



The test network topology above was used for the MVC400 deployment. With the MCore Mini-PC as the centerpiece, we connected it to the network and also connected to the Presenter's Laptop to the MTouch II Touch Panel.. This will act as the interface for the user. The Presenter's Display will show what the user decides based on their interactions with the MTouch II Touch Panel. The UVC40 will be the all-in-one camera, microphone, and speaker.

Device/Feature
UVC40 Video Camera
MTouch II Touch Panel
Microsoft Windows 10

Test Tools

The following tools are a representative list of software tools and exploits we implemented to conduct our security assessment.

CyPerf	Keysight CyPerf is the industry's first cloud-native software test solution that recreates every aspect of a realistic workload across a variety of physical and cloud environments to deliver unprecedented insights into end user experience, security posture, and performance bottlenecks of hybrid networks.
Wireshark 3.2.7	Open-source packet sniffer that can be used for network troubleshooting and analyzing.
Nessus Vulnerability Scanner 8.13.1	A proprietary security scanning tool developed by Tenable, Inc. It provides high speed and accurate scanning with minimal false positives.
Kali Linux 2021.1	Using Debian 10 with Kernels 4.1.x inside KVM Virtual Machines with physical Ethernet connections via PCIE bridging. We tested using 64-bit Linux.
Nmap 7.91 + Zenmap	Nmap ("Network Mapper") is an open-source tool for network exploration and security auditing. It was designed to rapidly scan networks using raw IP packets in novel ways to determine what available hosts, offered services (application name and version), running operating systems (OS versions), types of packet filters/firewalls, and dozens of other characteristics. Nmap is also useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Zenmap is an X11+GTK frontend for Nmap.
Hiren's BootCD 1.0.1	An all-in-one bootable disc aimed as a rescue utility. Contains only free and legal software and is legal in the terms of Microsoft's usage purposes.

5.0 Methodology

5.1 Physical Hardware and Accessibility

MCore Mini PC

The MCore Mini PC features a physical security lock slot for hardware theft prevention. Additionally, the Mini PC provides optional screws under the unit to limit physical port access and enable tidy cable management.

The MCore also contains a significant 128GB of storage. Notably, the reset button is visible on the unit's font face - this function resets the MCore Mini PC to factory settings. It is recommended that the reset button be relocated to the secured portion of the unit to prevent external tampering of the USB and other peripherals.

MTouch II Touch Panel

There is a USB port located on the right side of the touch panel however, this port is used for wireless connectivity of the display and does not interface with the Windows 10 system. Resembling the Mini PC, the touch panel includes optional screws to secure the display's input/output connections.

UVC84 Camera, Soundbar, and Mic Arrays

Miercom carefully examined Yealink peripherals including the UVC84 Camera, Soundbar, and Mic Arrays. These components do not pose a substantial vulnerability risk if properly configured and follow Yealink recommended setup. Yealink recommends that these components are not connected to the network, effectively reducing network based vulnerabilities.

5.2 Public Facing Information

5.2.1 Administrator Default Password

The default administrator password for the Windows 10 Mini PC is available through public Yealink documentation. This provides full access to device management along with Windows desktop access as a privileged user. A default password change is encouraged in security recommendations document from Yealink.

5.3 Encryption and Data Integrity

Yealink utilizes the TLSv1.2 cryptographic protocol and the SRTP protocol for real-time data transport. Miercom verified the encryption of traffic that we captured by Wireshark.

We initiated a Microsoft Teams call between the MVC840 and MVC400 deployment and transferred multiple file formats including .doc, .docx, .htm, .jpg, .mp3, .mp4, .pdf, .png, .pptx, and .txt. By adding a mirrored switch between Network 2 and the MVC840 deployment system, we observed encrypted traffic via Wireshark .pcap capture. We observed no confidential data and were able to transfer all data securely.

5.4 Endpoint Vulnerability Scanning and Assessment

5.4.1 Assessment

Bluetooth networking is enabled by default on the Yealink system as recommended by Microsoft. The security hardening guide from Yealink provides additional details on how to disable this feature if it is not needed.

The Yealink's video conferencing system components were not found to have any vulnerabilities in themselves. It is nonetheless still the enterprise's responsibility to employ their own security strategy when deploying a Yealink system.

Yealink Entrust Video Conferencing Security specifies the following "when the system is powered on, it is protected by a 'secure boot'".

5.4.2 Vulnerability Scanning

Vulnerability scans utilized Nessus Vulnerability Scanner and Nmap to comprehensively assess each component in their respective lab environments. After careful inspection, we observed no high-risk vulnerabilities however, minimal information was resolved from each scan. The MVC840 and MVC400 returned information relating to the MAC Address and Ethernet Card Manufacturer, firewall detection, and resolution of the FQDN.

5.4.3 DoS Attack and Recovery

A DoS (Denial of Service) attack was performed on the MCore Mini PC component. As the device is connected to a network, it is susceptible to a DoS attack. The meeting successfully recovered after directed DoS attack at the networked component.

About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report, but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.

All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.

By downloading, circulating or using this report this report in any way you agree to Miercom's Terms of Use. For full disclosure of Miercom's terms, visit: https://miercom.com/tou.