Security Whitepaper

Overview

As one of Microsoft's core hardware solution partners, Yealink has devoted significant efforts to providing industry-leading hardware solutions to meet intra- and inter-enterprise communication needs. In 2019, Yealink and Microsoft jointly launched the first MVC Room System for Microsoft Teams Room. With the increasing market demand for MVC Teams Room System, Yealink has also launched new-generation MVC Room System one after another.

This white paper aims to illustrate and prove the security of Yealink MVC Room System in design and daily use.

Product Introduction

MVC Room System is a Windows-based video conferencing system, equipped with Windows 10 IoT Enterprise system and a native Microsoft Teams Room app. It can provide video conferencing, content sharing, and other features to meet users' videoconferencing collaboration demands.

- Microsoft provides Microsoft Teams Room (MTR) and the Teams services for communication.
- Yealink provides the hardware solution, which has been strictly tested and certified by Microsoft.

Security Strategies on MVC Room System

Hardware Security

In Teams Rooms environment, Yealink MCore (mini-pc) acts as a central compute module that runs Windows 10 IoT Enterprise edition. Yealink MCore has a secure mounting solution, a security lock slot (Kensington lock), and I/O port access security measures that IT admin can fasten the screws in mini-pc to prevent the connection of unauthorized devices. You can also disable specific ports via Unified Extensible Firmware Interface (UEFI) configuration.

Every MCore mini-pc (certified compute module) is shipping with Trusted Platform Module (TPM) 2.0 compliant technology enabled by default. TPM is used to encrypt the login information for the Teams Rooms resource account.

Secure boot is enabled by default. Secure boot is a security standard developed by members of the PC industry to help make sure that a device boots using only software that is trusted by the Original Equipment Manufacturer (OEM). When the PC starts, the firmware checks the signature of each piece of boot software, including UEFI firmware drivers (also known as Option ROMs), EFI applications, and the operating system. perating system. If the signatures are valid, the PC boots, and the firmware gives control to the operating system. For more information, see Security boot.

Access to UEFI settings is only possible by attaching a physical keyboard and mouse. This prevents being able to access UEFI via the Teams Rooms touch-enabled console as well as any other touch-enabled displays attached to Teams Rooms.

Kernel Direct Memory Access (DMA) Protection is a Windows 10 setting that is enabled on Teams Rooms. With this

feature, the OS and the system firmware protect the system against malicious and unintended DMA attacks for all DMA-capable devices:

- During the boot process.
- Against malicious DMA by devices connected to easily accessible internal/external DMA-capable ports, such as M.2 PCIe slots and Thunderbolt 3, during OS runtime.

Teams Rooms also enables Hypervisor-protected code integrity (HVCI). One of the features provided by HVCI is Credential Guard. Credential Guard provides the following benefits:

- **Hardware security** NTLM, Kerberos, and Credential Manager take advantage of platform security features, including Secure Boot and virtualization, to protect credentials.
- **Virtualization-based security** Windows NTLM and Kerberos derived credentials and other secrets run in a protected environment that is isolated from the running operating system.
- **Better protection against advanced persistent threats** When Credential Manager domain credentials, NTLM, and Kerberos derived credentials are protected using virtualization-based security, the credential theft attack techniques and tools used in many targeted attacks are blocked. Malware running in the operating system with administrative privileges can\'t extract secrets that are protected by virtualization- based security.

Software Security

Microsoft Teams Rooms App

After Microsoft Windows boots, Teams Rooms automatically signs into a local Windows user account named Skype. The Skype account has no password. To make the Skype account session secure, the following steps are taken.
The Microsoft Teams Rooms app runs using the Assigned Access feature found in Windows 10 1903 and later. Assigned Access is a feature in Windows 10 that limits the application entry points exposed to the user. This is what enables single-app kiosk mode. Using Shell Launcher, Teams Rooms is configured as a kiosk device that runs a Windows desktop application as the user interface. The Microsoft Teams Rooms app replaces the default shell (explorer.exe) that usually runs when a user logs on. In other words, the traditional Explorer shell does not get launched at all. This greatly reduces the Microsoft Teams Rooms vulnerability surface within Windows. For more information, see Configure kiosks and digital signs on Windows desktop editions .
Additionally, lock down policies are applied to limit non-administrative features from being used. A keyboard filter is enabled to intercept and block potentially insecure keyboard combinations that aren\'t covered by Assigned Access policies. Only users with local or domain administrative rights are permitted to sign into Windows to manage Teams Rooms. These and other policies applied to Windows on Microsoft Teams Rooms devices are continually assessed and tested during the product lifecycle.

Yealink RoomConnect App

As Yealink self-developed management app, Yealink RoomConnect is pre-installed in the MCore mini-pc. It can identify the accessories connected to Yealink MVC system and allow you to configure or upgrade firmware of the accessories.
By default, the following information of peripherals is only processed between peripherals and Yealink RoomConnect application and stored locally on the Yealink MCore mini-pc.

- MAC address

- Serial number
- Firmware version number
- Device system log files (When exported out from device for the purpose of troubleshooting)

This information is used by the device and Yealink RoomConnect application to provide basic functionality and update purpose.
For Yealink Auto Update feature, the Yealink RoomConnect application detects and downloads available firmware of peripherals regularly from Yealink cloud-based platform.
Data transmitted via Yealink RoomConnect application between firmware update server is encrypted over TLS1.2. This service uses following security protocol to ensure the data protection:
TLS_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

Data Processing and Protection

Information that is processed is used for enhancing the user experience, allowing configuration of settings required for proper delivery of services and easy access to frequently used data.
By default, some information is processed and stored locally on the Yealink Solution for Microsoft Teams on Windows server. These details can be found at https://learn.microsoft.com/en-us/microsoftteams/rooms/data-and-privacy-info.
For data store and protection, please refer to Microsoft Teams Rooms on Windows security .

Account Security

Teams Rooms devices include an administrative account named \"Admin\" with a default password. We strongly recommend that you change the default password as soon as possible after you complete setup.
The Admin account isn\'t required for proper operation of Teams Rooms devices and can be renamed or even deleted. However, before you delete the Admin account, make sure that you set up an alternate local administrator account configured before removing the one that ships with Teams Rooms devices. For more information on how to change a password for a local Windows account using built-in Windows tools or PowerShell, see the following:

- Change or reset your Windows password
- Set-LocalUser

You can also import domain accounts into the local Windows Administrator group. You can do this for Azure AD accounts by using Intune. For more information, see Policy CSP - RestrictedGroups.

Network Security

Generally, Teams Rooms has the same network requirements as any Microsoft Teams client. Access through firewalls and other security devices is the same for Teams Rooms as for any other Microsoft Teams client. Specific to Teams Rooms, the categories listed as \"required\" for Teams must be open on your firewall. Teams Rooms also needs access to Windows Update, Microsoft Store, and Microsoft Intune (if you use Microsoft Intune to manage your devices).
If you want to use the auto-update feature of YealInk RoomConnect, make sure that your device can access https://dm.yealink.com via TCP port 443.
To understand more on Network Security, please refer to https://learn.microsoft.com/en-us/microsoftteams/rooms/security-windows#network-security.

Network Access Security

Yealink states that access to the internet for the part of the MVC system, for which Yealink is responsible, is only limited to the access to the Yealink firmware upgrade server and the access to the Yealink Management Cloud Service by the Yealink RoomConnect application built into the MVC system. The IP addresses involved in these accesses are listed in Table 6.3.1.

Domian Name	Usage	IP Address Location
dm.yealink.com	The Main Domain Name of Yealink Management Cloud Service	The United States
global.dm.yealink.com	Web Access Address	The United States
dmtcp.yealink.com	Device Connection Address	The United States
yl-us-dmfile.yealinkops.com	File server address	The United States

The Yealink Management Cloud Service is hosted in Microsoft Azure with data centers located in Australia, Virginia, USA and Frankfurt, Germany. YMCS operations will store data separately in accordance with local legal and regulatory requirements. In addition, Yealink has implemented technical and physical controls, such as "data fencing", to prevent unauthorized access or disclosure of customer content and to ensure data security and user privacy.

Independent Penetration Security Test by Leading Lab Miercom

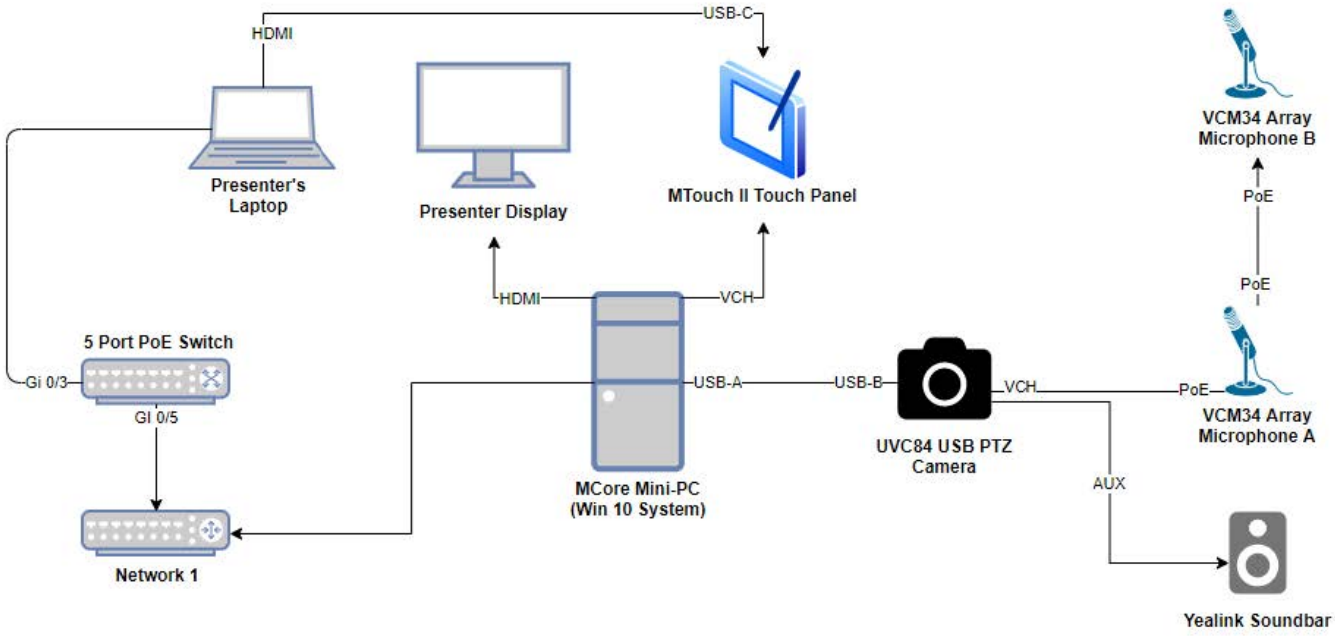
Key Findings

- 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.

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.

Test Tools

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

Tools	Description
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.

Endpoint Vulnerability Scanning and Assessment

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 ' ".

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.

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.

For detailed security assessment report, refer to Yealink MVC Series Room System for Microsoft Teams Certified Secure Assessment.

Appendixes

Reference documents:

- Microsoft Teams Rooms on Windows security
- Yealink MVC Series Room System for Microsoft Teams Certified Secure Assessment

About Miercom

Miercom is a global leader in independent network and security testing with 30 years of hands-on testing experience with network performance and security evaluations, reports, and webinars. Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. By using cutting-edge test tools and innovative engineering, Miercom keeps its reputation with the industry's most thorough and trusted assessment method.

About Yealink

Yealink (Stock Code: 300628) is a global-leading provider of Unified Communication & Collaboration Solutions specialized in video conferencing, voice communications, and collaboration, dedicated to helping every person and organization embrace the power of "Easy Collaboration, High Productivity".

With best-in-class quality, innovative technology, and user-friendly experiences, Yealink is one of the best providers in more than 140 countries and regions, ranks No.1 in the global market share of IP Phone, and is the Top 5 leader in the video conferencing market (Frost & Sullivan, 2021).