Yealink

ZVC Room System for Zoom Rooms

Security Whitepaper

Yealink Network Technology CO., LTD

Contents

Overview

As one of Zoom's core hardware solution partners, Yealink has devoted significant efforts to providing industry-leading hardware solutions to meet intra- and inter-enterprise communication needs. Yealink has been a long-term strategic partner of Zoom. With the increasing market demand for Zoom Room System, Yealink has also launched new-generation ZVC Room System one after another. This white paper aims to illustrate and prove the security of Yealink ZVC Room System in design and daily use.

Product Introduction

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

- Zoom Room System and the Zoom Cloud services for communication.
- Yealink provides the hardware solution, which has been strictly tested and certified by Zoom.

Hardware Security

In Zoom 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 Zoom 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. If the signatures are valid, the PC boots, and the firmware gives control to the operating system. For more information, see Secure boot.

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

Kernel Direct Memory Access (DMA) Protection is a Windows 10 setting that is enabled on Zoom 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.

Software Security

Zoom Rooms App

Zoom Rooms

Zoom Rooms is Zoom's software-based conference room system. It features video and audio conferencing, wireless content sharing, and integrated calendaring running on off-the-shelf hardware. Communications are established using TLS encryption and meeting, webinar and messaging content is encrypted using AES encryption. The Zoom Rooms app is secured with App Lock Code. The App Lock Code for Zoom Rooms is a required 1-16 digit number or characters lock code that is used to secure your Zoom Rooms application. This prevents unauthorized changes to your Zoom Rooms application and settings on your accompanying hardware.

Zoom Meeting Connector

Zoom Meeting Connector is a hybrid cloud deployment method, which allows a customer to deploy a Zoom multimedia router (software) within the customer's internal network.

User and meeting metadata are managed in Zoom communications infrastructure, but the meeting itself is hosted in the customer's internal network. All real-time media traffic including audio, video, and data sharing go through the company's internal network. This leverages your existing network security setup to protect your meeting traffic.

Zoom Rooms People Counting

Zoom Rooms People Counting is a feature that is off by default, but can be turned on by room administrators. This feature allows administrators to view reports of in-room meeting participants joined from Zoom Rooms.

This feature works by capturing images throughout the duration of the meeting. Images are temporarily stored on the Zoom Rooms local hard-drive and are never sent to the cloud. Once the meeting ends, the locally-stored images are used to count the max number of visible in-room meeting participants. Throughout this process, face detection (without ties to personal information) is used to count individuals based on the images captured. Once the images are done being processed to capture the number of people, the images are permanently deleted.

Zoom Rooms Voice Commands

You can start a scheduled meeting in a Zoom Room by saying, "Hey Zoom, start meeting." We do not upload or store your voice; it is processed on your local device only. The Zoom Room will listen for commands starting 10 minutes before each scheduled meeting. It ignores your voice beginning when the meeting is started or after 20 minutes.

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 ZVC system and allow you to configure or upgrade firmware of the accessories.

Data Processing and Protection

By default, the following information of peripherals is only processed between peripherals and Yealink RoomConnect software 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 software to provide basic functionality and update purpose.

For Yealink Auto Update feature, the Yealink RoomConnect software detects and downloads available firmware of peripherals regularly from Yealink cloud-based platform.

Data transmitted via Yealink RoomConnect software 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

Management Security

Administrative Controls

The following security capabilities are available to the account administrator:

- Secure login options using standard username and password (with the option to enable two-factor authentication (2FA) as an added layer of security), or SAML SSO
- Add user and admin to account
- Upgrade or downgrade account subscription level
- Delete user from account
- Review billing and reports
- Manage account dashboard and cloud recordings

Pre-meeting Role-based user security

Selective meeting invitation: The host can selectively invite participants via email, IM, or SMS. This provides greater control over the distribution of the meeting access information. The host can also create the meeting to only allow members from a certain email domain to join.

Meeting details security: Zoom retains event details pertaining to a session for billing and reporting purposes. The event details are stored at the Zoom secured database and are available to the customer account administrator for review on the

customer portal page once they have securely logged-on.

Application security: Zoom can encrypt all real-time media content at the application layer using Advanced Encryption Standard (AES).

Zoom client group policy controls: It is specifically applicable to the Zoom Meetings client for Windows and Zoom Rooms for Windows, administrators can define a broad set of client configuration settings that are enforced through active directory group policy controls.

Advanced encryption: Advanced chat encryption allows for a secured communication where only the intended recipient can read the secured message.

End-to-end encryption: End-to-end encryption, when enabled, ensures that communication between all meeting participants in a given meeting is encrypted using cryptographic keys known only to the devices of those participants. This ensures that no third party — including Zoom — has access to the meeting's private keys. End-to-end encryption is available as a technical preview to all customers.

In-meeting Role-based user security

Host and client authenticated meeting: A host is required to authenticate (via HTTPS) to the Zoom site with their user credentials (ID and password) to start a meeting. The client authentication process uses a unique per-client, per-session token to confirm the identity of each participant attempting to join a meeting. Each session has a unique set of session parameters that are generated by Zoom. Each authenticated participant must have access to these session parameters in conjunction with the unique session token in order to successfully join the meeting.

Open or passcode protected meeting: The host can require the participants to enter a passcode before joining the meeting. This provides greater access control and prevents uninvited guests from joining a meeting. Edit or delete meeting: The host can edit or delete an upcoming or previous meeting. This provides greater control over the availability of meetings.

Host controlled joining meeting: For greater control of meetings, the host can require participants to only join the meeting after the host has started it. For greater flexibility, the host can allow participants to join before the host.

In-meeting security: During the meeting, Zoom delivers real-time, rich-media content securely to each participant within a Zoom meeting. All content shared with the participants in a meeting is only a representation of the original data. This content is encoded and optimized for sharing using a secured implementation as follows:

- Is the only means possible to join a Zoom meeting
- Is entirely dependent upon connections established on a session-by-session basis
- Performs a proprietary process that encodes all shared data
- Encrypts all real-time media (audio, video, screen sharing) using the AES encryption standard
- Encrypts other data using TLS encryption standard
- Provides a visual identification of every participant in the meeting

Network Security

The Zoom cloud is a proprietary global network that has been built from the ground up to provide quality communication experiences. Zoom operates in a scalable hybrid mode; web services providing such functions as meeting setup, user management, conference recordings, chat transcripts, and voice mail recordings are hosted in the cloud, while real-time conference media is processed in globally distributed tier-1 colocation and commercial cloud data centers with SSAE 16 SOC 2 Type 2 certifications.

Real-time media processing

A distributed network of low-latency multimedia software routers connects Zoom's communications infrastructure. With these Multimedia Routers (MMR), all session data originating from the host's device and arriving at the participants' devices is dynamically routed between endpoints.

Firewall compatibility

During session setup, the Zoom client connects via HTTPS to Zoom servers to obtain information required for connecting to the applicable meeting or webinar, and to assess the current network environment such as the appropriate Multimedia Router to use, which ports are open and whether an SSL proxy is used. With this metadata, the Zoom client will determine the best method for real time communication, attempting to connect automatically using preferred UDP and TCP ports. For increased compatibility and support of enterprise SSL proxies, connection can also be made via HTTPS. An HTTPS connection is also established for users connecting to a meeting via the Zoom web browser client.

Network Access Security

Yealink states that access to the internet for the part of the ZVC 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 software built into the ZVC system. The IP addresses involved in these accesses are listed in Table 6.3.1. In this regard, Yealink declares that **no** ZVC system that is used outside of mainland China would proactively access any IP address within mainland China.

Domain 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 Amazon Web Services (AWS) with data centers located in 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.

Testing Method and Result of Miercom

Key Findings

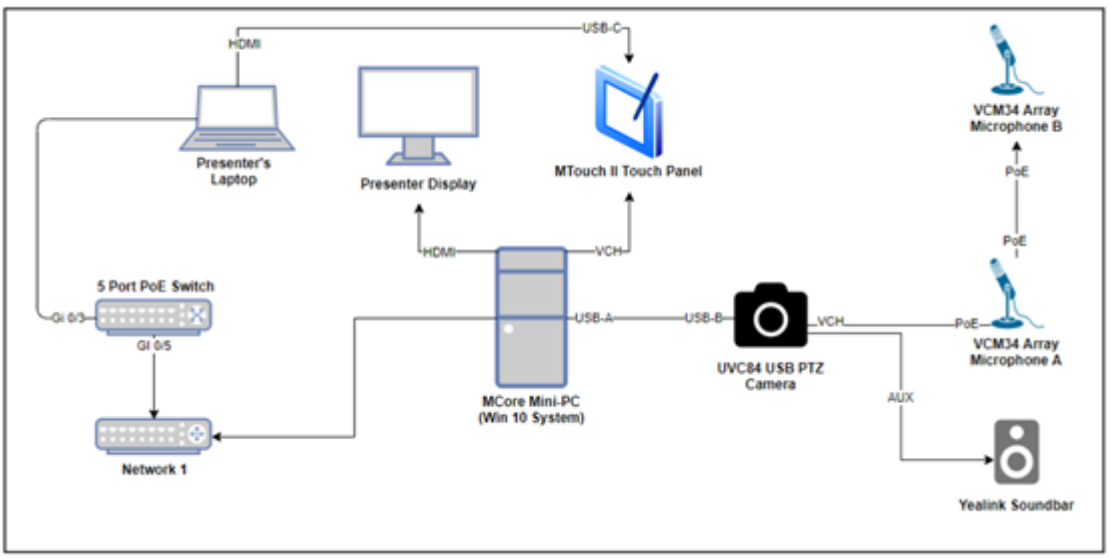
- Analysis of data in transit was proven encrypted
- Tamper resistant design verified on MCore and peripherals, including security locks to prevent theft and tampering
- No vulnerable APIs, Windows services or ports were found on the Yealink networked components in test

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

How They Did It

Using a simulated enterprise network environment, we tested ZVC840 and the ZVC400 for basic functionality while conducting monitoring and penetration testing activities.

Test Bed Overview 1



The network topology above was used for the ZVC840 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 Windows.

Endpoint Vulnerability Scanning and Assessment

Assessment

Bluetooth networking is enabled by default on the Yealink system. 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 ZVC840 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.

Appendixes

Reference documents:

- Zoom Security White Paper

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.

About Yealink

Yealink (Stock Code: 300628) is a global brand that specializes in video conferencing, voice communications and collaboration solutions with best-in-class quality, innovative technology and user-friendly experience. As one of the best providers in more than 140 countries and regions, Yealink ranks No.1 in the global market share of SIP phone shipments (Global IP Desktop Phone Growth Excellence Leadership Award Report, Frost & Sullivan, 2019).