OCISO DIR

Office of the
CHIEF INFORMATION
SECURITY OFFICER
State of Texas

Virtual Collaboration Tools Exploitation - Best Practices for Zoom Video Conferencing Services

Date: April 03, 2020

Introduction

The Coronavirus pandemic has resulted in increased telework, enabled largely by video-teleconferencing (VTC) services such as Zoom, WebEx, and others. This swell in usage has created an unusually large target for malicious hackers. Attacks include call interruption/disruption (aka “Zoom-bombing”), using fake web addresses to entice unsuspecting conference attendees to download malicious software, and exploiting multiple newly discovered zero-day vulnerabilities.

Video Conferencing Services

In recent weeks, there have been a number of ongoing attacks and newly discovered exposures including two zero-day vulnerabilities, malicious domain registrations, and teleconference session hijacking. The Coronavirus pandemic and subsequent expansion of telework requirements has resulted in an increased use of Zoom and other VTC platforms. Consequently, fake domain registrations have spiked, especially those containing ‘zoom,’ which have a considerably greater potential in phishing unsuspecting users.

Best Practices for Zoom Video Conferencing

Users should be aware of the following best practices for configurations and settings when using the ZOOM Video Conferencing Platform.

- Lock meetings once everyone has joined. This will prevent unauthorized users from gaining entry while the call is in session.
- After locking the meeting, review the list of participants and expel any unknown participants before beginning to share your content.
- Expel disruptive individuals from your meeting.
- Disable “Allow Removed Participants to Rejoin” so expelled attendees can’t slip back in.
- Disable participants ability to record the meeting.
- Disable participant screen sharing or file sharing. This will prevent your meeting from being hijacked by others and allowing the sharing of inappropriate content.
- Avoid posting photos or screenshots of your Zoom meetings. This could provide threat actors with the associated meeting ID and information on who is attending your meetings.
- Disable the Chat feature prior to the meeting.
- Put all attendees in mute mode and suspend privileges for participants to unmute themselves.
- Pin or Spotlight Speaker Video. https://support.zoom.us/hc/en-us/articles/201362743-Pin-Video

    - Pinning a video allows you to disable active speaker view and only view a specific speaker.
    - Alternatively, you can spotlight a video. Spotlight video puts a participant as the primary active speaker for all participants. All participants will only see this speaker as the active speaker. These features will keep others from seeing an intruder’s screen or background.
- Consider not publishing the link on public websites or calendars, rather email the link to the desired attendees.
- Consider requiring a password to join the meeting. Distribute password separately via email to attendees.

Users of any Virtual Collaboration Tool or video teleconference system who experience a disruption or security incident are encouraged to report it to their organization’s IT staff to coordinate their agency’s response.

Zoom security issues may also be reported here: https://support.zoom.us/hc/en-us/requests/new

DIR.TEXAS.GOV

Assistance/Feedback/Questions?

Office of the Chief Information Security Officer

DIRSecurity@dir.texas.gov

Texas Department of Information Resources

Transforming How Texas Government Serves Texans