Zoom Security Recommendations

Prepared by: Matthew Jennings, IT Security Architect 3/26/2020

Purpose

Organizations ranging from corporations to homeschools are now meeting up with people online using Zoom amid the quarantine and stay-at-home orders that have rolled out globally in the wake of the coronavirus' rapid spread. Like any other internet-connected tool, Zoom can be used with malicious intent to disrupt business or subvert security efforts and create added risk to the organization. Increasingly popular in the news, unauthorized access to Zoom meetings has become prevalent because of misconfigurations in security settings. It has been reported that threat actors have been upending Zoom meetings with hate speech such as racist messages, threats of sexual harassment, and pornographic images. Some of the attacks have even gone so far as to threaten those attending the meeting with physical harm.

It is the purpose of this report to suggest some setting configurations to thwart such possibilities and harden the security of meetings conducted using this app to convey sensitive information or perform AOC business functions. The Security Setting Highlights section will walk through some general best practices pertaining to all versions of the Zoom application. The Setting Walkthrough section lists specific setting recommendations for the free version of Zoom.

Security Setting Highlights

- Be careful when sharing links via social media and try to ensure only trusted colleagues or participants can join the meeting.
- Avoid using Zoom Personal Meeting ID (PMI) to host events. The PMI is basically one continuous meeting and you do not want random people having access to it after the meeting.
- Use the Waiting Room feature, which allows hosts of the meetings to see participants in a virtual staging area so they can be vetted and cannot join the meeting until the host gives them permission.
- Only allow participants to log into Zoom with an email, through which they were specifically invited to the event.
- Don't forward meeting links if you have "Embed password in meeting link for one-click join" turned on.
- Lock the meeting once all invited participants have joined so no one else can jump on.
- Use the "remove" feature to kick off unwanted participants that do manage to join.
- Generate a random Meeting ID when scheduling an event, and require a password to join. Do not send out a public link for users to participate.
- Enable an end-to-end (E2E) encrypted meeting using the Advanced Encryption Standard (AES) 256-bit algorithm.
- Enable Zoom E2E chat encryption, which allows for secured communication. Session keys are generated with a device-unique hardware ID to avoid data being read from other devices. This ensures that the session cannot be eavesdropped on or tampered with.
- Utilize Screen share watermarks and audio signatures.

Setting Walk-Through

Schedule Meeting

Join before host	Off
Use Personal Meeting ID (PMI) when scheduling a meeting	Off
Use Personal Meeting ID (PMI) when starting an instant meeting	Off
Require a password when scheduling new meetings	On
Require a password for instant meetings	On
Require a password for Personal Meeting ID (PMI) (if used, set to “all meetings using PMI”)	On
Embed password in meeting link for one-click join (share password via secure channel, i.e. phone)	Off
Require password for participants joining by phone	On

In Meeting (Basic)

Require Encryption for 3rd Party Endpoints (H323/SIP)	On
Play sound when participants join or leave	On
File transfer (if turned on, limit to .doc and .xls if possible. Avoid allowing executable extensions - .exe, .bat, .vbs, .ps, etc)	
Allow host to put attendee on hold	On
Allow removed participants to rejoin	Off

In Meeting (Advanced)

Far end camera control	Off
Identify guest participants in the meeting/webinar	On
Auto-answer group in chat	Off
Only show default email when sending email invites	On
Use HTML format email for Outlook plugin	Off
Waiting Room	On

Email Notification

When attendees join meeting before host	On

Other

Blur snapshot on iOS task switcher	On
Schedule Privilege (Assign scheduling privilege to)	No One

References

https://threatpost.com/as-zoom-booms-incidents-of-zoombombing-become-a-growing-nuisance/154187/

https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf

Additional Resources

https://www.cmu.edu/canvas/teachingonline/zoom/zoombombing.html

https://support.zoom.us/hc/en-us/search?utf8=%E2%9C%93&query=Disable+desktop%2Fscreen+share+for+users