

## CERT-In Advisory Note CIAD-2020-0010

### Secure usage of Zoom video conferencing application

Original Issue Date: March 30, 2020

#### Description

Many organizations have allowed its staff to work from home to stop the spread of Coronavirus disease (COVID-19). Online communication platforms such as Zoom, Microsoft Teams and Teams for Education, Slack, Cisco WebEx etc. are being used for remote meetings and webinars.

Zoom is a popular video conferencing platform. Insecure usage of the platform may allow cyber criminals to access sensitive information such as meeting details and conversations. Following measures are advised for increasing the security of Zoom meetings and reducing risks-

- Keep your Zoom software patched and up-to-date.
- Always set strong, difficult-to-guess and unique passwords (make your password at least eight characters long and use at least three of the following types of characters: lowercase letters, uppercase letters, numbers, symbols) for all meetings and webinars. This is especially recommended for any meetings where sensitive information may be discussed.

#### Require a password when scheduling new meetings

A password will be generated when scheduling a meeting and participants require the password to join the meeting. The Personal Meeting ID (PMI) meetings are not included.

Require a password for meetings which have already been scheduled ⓘ



#### Require a password for instant meetings

A random password will be generated when starting an instant meeting



#### Require a password for Personal Meeting ID (PMI)

Only meetings with Join Before Host enabled

All meetings using PMI






#### Require password for participants joining by phone

A numeric password will be required for participants joining by phone if your meeting has a password. For meeting with an alphanumeric password, a numeric version will be generated.




- Enable "Waiting Room" Feature so that the call manager will have a better control over participants. All participants can join a virtual "Waiting Room", but they will be approved by call manager to be part of the actual meeting.

**Waiting room**  

Attendees cannot join a meeting until a host admits them individually from the waiting room. If Waiting room is enabled, the option for attendees to join the meeting before the host arrives is automatically disabled. 


**Choose which participants to place in the waiting room:**

All participants

Guest participants only 

Allow internal participants to admit guests from the waiting room if the host is not present

**Save** **Cancel**

Customize the title, logo, and description 

- Disable Join Before Host Feature: The "Join Before Host" option lets others to continue with a meeting in the absence of an actual host, but with this option enabled, the first person who joins the meeting will automatically be made the host and will have full control over the meeting. Alternatively, "Scheduling Privilege" may be given to a trusted participant to host the meeting in the absence of an actual host.

**Join before host**  

Allow participants to join the meeting before the host arrives

## Schedule Privilege


You can assign users in your account to schedule meetings on your behalf. You can also schedule meetings on behalf of someone that has assigned you scheduling privilege. You and the assigned scheduler must be on a Paid plan within the same account.

Assign scheduling privilege to  
No one



I can schedule for

Assign scheduling privilege ✕

example: sales.ea@company.com,marketing.ea@company.com 

Enter the email addresses of those who can schedule meetings on your behalf.  
Use a comma to separate multiple email addresses.

**Assign** Cancel

- If not required, restrict/disable file transfers.
- From settings and controls, ensure removed participants are unable to rejoin meetings.
- If not required, limit Screen Sharing to the Host only.
- Lock the meeting session once all your attendees have joined.
- Restrict the call record feature "Allow Record" to trusted participants only.

## References

<https://blog.checkpoint.com/2020/03/26/whos-zooming-who-guidelines-on-how-to-use-zoom-safely/>

<https://it.cornell.edu/zoom/keep-zoom-meetings-private>

<https://www.inc.com/jason-aten/zoom-has-a-major-security-flaw-that-could-let-malicious-websites-literally-spy-on-you.html>

<https://www.foxbusiness.com/technology/securely-host-zoom-meeting>

<https://www.forbes.com/sites/zakdoffman/2020/01/28/new-zoom-roulette-security-warning-your-video-calls-at-risk-from-hackers-heres-what-you-do/#591e905d7343>