SWITCH-CERT

Privacy & Security @Zoom

updated on: 28.07.2020

Introduction

Online meeting software is in greater demand than ever before. One service in particular, Zoom, has attracted a lot of media attention in the first half of 2020, mostly due to potential privacy and/or security issues.
The list of data points collected by Zoom, according to its own "Zoom Privacy Statement", spans several pages or screens [1].

Update from the last version

Although the initial statement from Zoom regarding end-to-end encryption was quite dubious, Zoom will support proper end-to-end encryption in the future, although the productive release date for E2EE has not been confirmed yet. The key points are [2]

- Zoom plans to begin early beta of the E2EE feature in July 2020.
- All Zoom users will continue to use AES 256 GCM transport encryption as the default encryption, one of the strongest encryption standards in use today.
- E2EE will be an optional feature as it limits some meeting functionality, such as the ability to include traditional PSTN phone lines or SIP/H.323 hardware conference room systems. Hosts will toggle E2EE on or off on a per-meeting basis.
- Account administrators can enable and disable E2EE at the account and group level.

For more technical details, have a look at the E2EE whitepaper published on GitHub. [3]

Recommendations

- Have a clear cloud service usage concept beforehand. Outline topics such as data protection, data classification, what data shall not be processed/stored under any circumstances, etc.
- Make sure you always have the latest version of Zoom.
- Enable the camera and unmute the microphone when needed.
- Do not share Zoom meeting links publicly (e.g. Twitter, LinkedIn, etc.).
- Manage your meetings
  - Protect your meetings with a password.
  - Set up the waiting room for the participants and let them join the meeting one by one.
  - Start with your microphone muted and video disabled.
  - Click 'Lock Meeting' when all participants are in the meeting.
- Do not use the Facebook or Google login option; instead, create a dedicated login for Zoom.
- Share sensitive content like files and links securely using established services outside the video platform.
- Control your datacenter region (Paid account only).

Assessment

Every online service has some risk of user data collected (e.g. IP addresses, browser type, etc.).

Privacy Concerns:

- Attention tracking feature was permanently removed of April 1st.
- Zoom can access Facebook profile data (your name and profile picture and email address.), if Facebook login option is used → use a Zoom specific login.
- Zoom may display personalised advertisements on the website → as most online portals do.
- Personal information may be revealed through the use of the webcam (room, background) → disable the webcam and mute the microphone when not needed.
- Recordings might be shared outside of Zoom/the organization → record only when needed, use Audio Watermark, which helps you to identify the one who shared.
- Audio and video streams are currently not end-to-end encrypted → the data streams are, however, encrypted using TLS (TCP) or AES (UDP) using a shared session keys. In theory, Zoom would be able to decrypt the data. But, any attack on the network, i.e outside of the Zoom data centres, will not give attackers access to these keys, so they will not be able to decrypt the data streams.

Latest zoom security and privacy features:

You can find the latest security and privacy updates and also fixed bugs at the Zoom website [4]

New updates for the Zoom Web version

- New security heading for meeting settings: All password related settings, Waiting Room settings, and the settings to only allow authenticated users to join meetings will now be moved under the Security heading of the account, group, and user settings to allow users to more easily enable security options for their meetings and webinars. [5]

The newest updates for the Zoom Phone devices includes:

- Enable AES-256 bit encryption for devices Account owners and admins can upgrade to SRTP with AES-256 bit encryption for specific sites and models. By default, AES-128 bit is enabled. Admins must enable AES-256 bit in the web portal. [6]

New updates for Windows, Zoom version 5.1.3 (28656.0709)

- Fixes a security issue affecting users running Windows 7 and older [7]

The comment by the data protection officer by canton Zurich does not specify any details as to why it is not advised to use Zoom outside of the corona crisis. The statement has been updated with some good practice and the advise to sign the Global Data Processing Addendum has been removed.
https://dsb.zh.ch/internet/datenschutzbeauftragter/de/themen/digitale-zusammenarbeit.html#title-content-internet-datenschutzbeauftragter-de-themen-digitale-zusammenarbeit-jcr-content-contentPar-textimage_2

References:

[1] https://zoom.us/privacy
[2] https://blog.zoom.us/end-to-end-encryption-update/
[3] https://github.com/zoom/zoom-e2e-whitepaper/blob/master/zoom_e2e.pdf
[4] https://support.zoom.us/hc/en-us/sections/360008531132-Zoom-Releases-By-Date
[5] https://support.zoom.us/hc/en-us/articles/360045100092-New-updates-for-June-28-2020
[6] https://support.zoom.us/hc/en-us/articles/360045630812-New-updates-for-July-12-2020
[7] https://support.zoom.us/hc/en-us/articles/360046081271-New-updates-for-July-10-2020