SWITCH-CERT

Privacy@Zoom

updated on: 13.05.2020

Introduction

Online meeting software is in greater demand than ever before. One service especially, Zoom, has recently attracted a lot of media attention, mostly due to potential privacy and/or security issues.
The list of data points collected by Zoom, according to its own privacy policy, spans several pages or screens (see the link below). Additionally, Zoom has already fallen victim to a major hack; and, if that wasn't enough, dataloft.ch reports that investigative journalists at 'The Intercept' claim that Zoom's statement "meetings use end-to-end encryption" is based on Zoom's own definition of end-to-end encryption. Indeed, deeper analysis did reveal a few privacy concerns, as well as security flaws posing a particular security risk on both Windows and Mac OS. Other supposed "security issues" like "Zoom bombing" are not really security issues and can easily prevented by the user by choosing secure settings for the meeting.
Despite this, Zoom is perfectly suitable for large online meetings and lectures and many people still don't want to or cannot do without the web-based service.

Update

Zoom is enhancing constantly their product with security options. For more information please read the 90-Day Security Plan Progress Report. With the release of Zoom 5.0 client, Zoom added the support for the more efficient encryption algorithm GCM (Galois/Counter Mode), which will be enabled system-wide on May 30, 2020. So only Zoom clients on version 5.0 or later will be able to join Zoom Meetings starting that day. Also they enhanced the power of the hosts in webinars to prevent disruptions and they are currently working on a feature where users are only allowed to use pre-approved virtual backgrounds.

Recommendations

- Have a clear cloud service usage concept beforehand. Outline topics such as data protection, data classification, which data shall not be processed/stored under any circumstance, 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 (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, 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.
- iOS app shared data with Facebook → the FB SDK to facilitate FB logins has been removed as it shared data with FB, even if the user had no FB login or account.
- Audio and video streams are 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.

Fixed Security Bugs:

- Safari 12 allowed an attack to activate the video camera; flaw was fixed by Zoom.
- The Windows client converts UNC paths to clickable URLs, allowing attackers to send the Windows username and NTLM password hash if the user clicks on such an URL.
- Mac OSX installer circumvents the password dialog; the user must be in the administrator group for this attack vector to work.
- With paid accounts, you are able to opt out data center regions for data routing. For routing to China you have to opt in until April 25th.
- Mac OS client enable loading libraries, allowing a local attacker to inject any library into the Zoom client.

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

Read more:
https://zoom.us/privacy
https://blog.zoom.us/wordpress/2020/05/07/90-day-security-plan-progress-report-may-6/
https://support.zoom.us/hc/en-us/articles/360000126326-Offi cial-Statement-EU-GDPR-Compliance
https://zoom.us/docs/doc/Zoom_GLOBAL_DPA_December_19.pdf
https://securityboulevard.com/2020/03/using-zoom-here-are-the-privacy-issues-you-need-to-be-aware-of/
https://www.vice.com/en_us/article/qjdqgv/hackers-selling-critical-zoom-zero-day-exploit-for-500000