SWITCH-CERT

Privacy@Zoom

state: 16.04.2020

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 their own privacy policy, spans over several pages or screens (see the link below). Additionally, Zoom has already fallen victim to a major hack; and, if all that wasn't already enough, dataloft.ch reports that investigative journalists of '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 revealed a few privacy concerns, as well as security flaws posing a certain security risk on both Windows and Mac OS. Other so called "security issues" like "Zoom Bombing" are not really security issues and can easily prevented by the user by choosing secure settings for the meeting.
On the other hand, Zoom is perfectly suitable for large online meetings and lectures, many people still don't want to or cannot do without the web-based service.

Update

In the last couple of weeks, Zoom has updated improved the default settings, fixed several security flaws and privacy options, e.g. stronger password requirements for all accounts, random session IDs; these significantly improving privacy and security. For more details see the next page or the Zoom Blog.
More improvements are steadily coming every few days. Starting April 18th it will be possible for paid accounts to choose the data center location.

Recommendations

- Have a clear cloud service usage concept beforehand. Outline topics such as data protection, data classification, especially 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.
  - Setup the waiting room for the participants and let them join the meeting one by one.
  - Start with your microphone muted and video stopped.
  - 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 over established services outside the video platform.

Assessment

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

Privacy Concerns:

- Attention tracking has been permanently removed by April 1st.
- Zoom can read Facebook profile, when Facebook login option is used → use a Zoom specific login
- Zoom can present personalised advertisements on the website → as most online portals do
- Reveal personal information 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
- 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, does not have access to these keys and therefore cannot decrypt the data streams.

Fixed Security Bugs:

- Safari 12 allowed an attack to activate the video camera, was closed by Zoom
- The Windows client converts UNC paths to clickable URLs, allowing for an attack sending 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

Open Security Bugs:

- Mac OS client enable loading libraries, allowing a local attacker to inject any library to the Zoom client.
- Session encryption keys may be exchanges over servers standing in China (or other countries) pending fix April 18th

The comment of the data protection officer of canton Zurich does not specify any details, why it is not advised to use Zoom outside of the corona crisis. The recommendation is to sign the Global Data Processing Addendum and send it to Zoom.
https://dsb.zh.ch/internet/datenschutzbeauftragter/de/themen/digitale-zusammenarbeit.html#title-content-internet-datenschutzbeauftragter-de-themen-digitale-zusammenarbeit-jcr-content-contentPar-textimage_2

Géant and SWITCH (together with other European NRENs) is talking about an umbrella contract with Zoom. The agreement automatically includes the Global Data Protection Addendum of Zoom assuring from a legal perspective GDPR, EU General Clauses, EU-US Privacy Shield and CH-US Privacy Shield compliance.

Read more:
https://zoom.us/privacy
https://blog.zoom.us/wordpress/
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://dataloft.ch/security/end-to-end-verschluesselung-von-zoom-unter-beschuss
https://securityboulevard.com/2020/03/using-zoom-here-are-the-privacy-issues-you-need-to-be-aware-of/