Increasing Zoom Demand Brings Security Issues

Written by Marco Attard
03 April 2020

Videoconferencing is seeing a surge in demand following the coronavirus (aka Covid-19) pandemic, with the chief solution being Zoom-- a solution that, while popular, is currently beset by a bevy of security issues.

A Zoom white paper on the topic of security states the videoconferencing service can secure meetings through end-to-end (E2E) encryption, something hosts can set up while creating a meeting. However, according to an investigation by The Intercept, Zoom does not actually feature E2E encryption. Instead it uses TLS transport encryption, the kind web servers use to secure HTTPS websites. This means that while meetings are private from anyone spying the users' network, the company can actually access the unencrypted video and audio content of meetings taking place on the service.

The lack of E2E encryption leads to the issue of "zoom bombing," or people jumping into Zoom meeting without an invite in the name of harassment. In addition, users on the iOS app can send meeting data to the Facebook app, and share the email address and photos of thousands of Zoom members. Such privacy and security issues have lead organisations such as NASA and SpaceX to prohibit the use of Zoom, while agencies including the FBI are looking into the aforementioned problems.

In a reply to the Intercept article, Zoom admits it uses TLS in video meetings, with E2E encryption only finding use for in-meeting text chat. As a result, the company retains the ability to spy on meetings, and governments or law enforcement agencies can compel it to hand over meeting recordings. Furthermore, while the likes of Google, Microsoft and Facebook publish transparency reports detailing the government requests for user data, Zoom does nothing of the sort.

Admittedly, Zoom is not designed for the number of users it is currently hosting. A company blog post points out daily Zoom meeting participants (both free and paid) total over 200 million in March 2020, far more than the 10m daily participants of December 2019. It also says the company is shifting all engineering resources to focus on trust, safety and privacy issues, and will get 3rd party experts to conduct a comprehensive review. Finally, Zoom insists that while it collects basic technical information (such as IP address, OS details and device details), it does not sell data "of any kind" to 3rd parties.

Go Zoom Meetings Aren't End-to-End Encrypted, Despite Misleading Marketing (The Intercept)

Go Zoom Security Guide

Go Zoom: Message to Our Users