Special Advisory CIAD-2020-S2

Zoom video conferencing app Issues

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.

It is observed that some of these apps are not secured and are vulnerable to be exploited thus revealing users identity, location or content of the discussion.

Zoom is getting more popular video conferencing platform these days and it is noticed that a large number of people are using Zoom meeting for communication.

Zoom video meetings use a combination of TCP and UDP for end to end encryption. The encryption that Zoom uses to protect meetings is TLS, is known as transport encryption, which is different from end-to-end (E2E) encryption. With TLS, the video and audio content will stay private from anyone spying on Wi-Fi, but it won't stay private from the Zoom company itself. Without E2E encryption, Zoom has the technical ability to spy on private video meetings. In other words, although a third-party can't eavesdrop on Zoom video or audio conversation, the Zoom company can access the contents. The only content that is end-to-end encrypted on Zoom is the text in chats.

Further, the Zoom Windows client is vulnerable to UNC (Universal Naming Convention) path injection in the client's chat feature that could allow attackers to steal the Windows credentials of users who click on the link.

In view of this, it is advised that officials may refrain from using Zoom meeting for discussion involving sharing of classified/sensitive information and also if it is absolutely necessary to discuss other official meetings/discussions, then sufficient precautions needed to be taken to avoid leakage of personally identifiable information or other details of sensitive nature.

References

https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0010

https://theintercept.com/2020/03/31/zoom-meeting-encryption/

https://www.bleepingcomputer.com/news/security/zoom-client-leaks-windows-login-credentials-to-attackers/