Circular

National Stock Exchange of India Limited

DEPARTMENT : CYBER & INFORMATION SECURITY	
Download Ref No: NSE/CIS/44170	Date : April 20, 2020
Circular Ref. No: 03/2020	

To All Members,

Cyber Security Advisory: Zoom video conferencing app Issues

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.

In regards with the above and the ICT threat received from regulators, all members are hereby notified and requested to undertake appropriate actions as applicable to their environment. A brief description and immediate steps to be taken are mentioned below.

1. **Description of the threat:**
   a. 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.
   b. 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,

2. **Key actions to be taken to mitigate the threat**
   a. It is advised that officials may refrain from using Zoom meeting for discussion involving sharing of classified/sensitive information.
   b. If it is absolutely necessary to discuss official meetings/discussions, then sufficient precautions needed to be taken to avoid leakage of personally identifiable information or other details of sensitive nature.

i. Keep your Zoom software patched and up-to-date.
ii. Always set strong, difficult-to-guess and unique passwords (make your password at least eight characters long and use at least three of the following types of characters: lowercase letters, uppercase letters, numbers, symbols) for all meetings and webinars. This is especially recommended for any meetings where sensitive information may be discussed.
iii. Enable "Waiting Room" Feature so that the call manager will have a better control over participants. All participants can join a virtual “Waiting Room” but they will be approved by call manager to be part of the actual meeting.
iv. Disable Join Before Host Feature: The “Join Before Host” option lets others to continue with a meeting in the absence of an actual host, but with this option enabled, the first person who joins the meeting will automatically be made the host and will have full control over the meeting. Alternatively, “Scheduling Privilege" may be given to a trusted participant to host the meeting in the absence of an actual host.
v. If not required, restrict/disable file transfers
vi. From settings and controls, ensure removed participants are unable to re-join meetings.
vii. If not required, limit Screen Sharing to the Host only.
viii. Lock the meeting session once all your attendees have joined.
ix. Restrict the call record feature "Allow Record" to trusted participants only.

c. For additional details, please refer the advisory issued by CERT-In attached as Annexure A.

3. Reference Links:

a. https://www.cert-in.org.in
b. https://blog.checkpoint.com/2020/03/26/whos-zooming-who-guidelines-on-how-to-use-zoom-safely/
c. https://it.cornell.edu/zoom/keep-zoom-meetings-private
d. https://www.inc.com/jason-aten/zoom-has-a-major-security-flaw-that-could-let-malicious-websites-literally-spy-on-you.html
e. https://www.foxbusiness.com/technology/securely-host-zoom-meeting
f. https://www.forbes.com/sites/zakdoffman/2020/01/28/new-zoom-roulette-security-warning-your-video-calls-at-risk-from-hackers-heres-what-you-do/

4. Disclaimer:

a. The information contained in this notice has been extracted from regulatory sources and has been published only as guidance to members. As the future course of events with regards to this threat are not known, members are advised to keep a close watch on their systems to identify timely detection and remediation of this threat.
b. Members shall act upon this notice at their own discretion after conducting appropriate impact/risk analysis to their specific environment.
c. Please note that the other exploit kits are also widely in circulation and available for download for free on the Internet and there are possibilities of attack vectors other

than this threat which may exist/emanate. It is critical to perform a self-assessment against these zero-days/ exploit kits released in the wild in a controlled environment.

d. This notice is for informational purpose only.

For and on behalf of

Chief Information Security Officer
National Stock Exchange of India Limited

Toll Free No	Telephone No	Email ID
1800–266–0053	+91–22–26598100 | Extn:22114	soc_im@nse.co.in