FS-ISAC

Statement on Zoom

08 April 2020

Usage of Zoom and VC Technology Security Strategies

In response to the numerous media stories about the security and privacy features and capabilities of Zoom, FS-ISAC is providing our members the information we have on these issues and our recommendations for more secure ways to use and configure Zoom. FS-ISAC adopted Zoom as our primary video conferencing (VC) tools for staff and member meetings earlier this year and has implemented the recommendations below. Telephone dial-ins are available for all meeting attendees who cannot use the application or website versions.

Primary Issues of Concern

- Zoom Bombing – hijacking of video calls, including posting of lewd and offensive images or text
- Adequate encryption – lack of a true end-to-end encryption for calls (not including text chats)
- Routing of traffic and keys – reports of traffic going to servers based in China
- Vulnerabilities – multiple application vulnerabilities allowing for privilege escalation, credential theft and malware injection

We note that Zoom was quick to respond to the stories on the above issues. There are several techniques that can be used by the hosts of the meetings that can mitigate these issues. Zoom also issued patches for the stated vulnerabilities and resolved their geofencing rules to avoid the traffic routing issues.

FS-ISAC Use of Zoom

As part of our third-party vendor risk management process, we evaluated Zoom's Standard Information Gathering (SIG), SOC2, and Independent Practitioner's Report on Specific Controls and we found them satisfactory for our business needs. During our initial deployment of Zoom usage to staff, we established our security control posture to achieve a functional yet secure implementation. FS-ISAC staff hosting meetings or webinars use passcodes and restrict who can share their screens. As with all third-party products, we continue to review and evolve our Zoom security settings to reduce risk.

Every technology has operational and security risks, which we feature heavily in our vulnerability reporting to members. Common third parties have dedicated patch release cycles because there are regularly identified and mitigated vulnerabilities in their platforms. To address this reality, every business needs to assess the risk of using any technology, including Zoom, based on their security needs, risk appetite, and compliance requirements. Additionally, it is imperative to review and customize the settings based on your organizational needs. Out of the box configurations are almost never appropriate for the sector.

FS-ISAC and the sector are working with Zoom management to address concerns and notes the following actions taken by the company:

- Effort to ensure transparency to customers and the public on the security issues and actions taken (https://blog.zoom.us/)
- A weekly webinar with the CEO where he will address security and privacy related topics. You can register here: https://zoom.us/webinar/register/WN_9jdr63uuRuSRBX-yEJ2zVQ?zcid=1231
- Additional security testing to include furthering their bug bounty program

Video Conferencing Systems Security Strategies

To support members and provide guidance to participants of Zoom meetings and webinars, FS-ISAC recommends that firms implement specific controls already available in the Zoom product. This is not an exhaustive list and specifically focuses only on the recently reported risks. These are the controls FS-ISAC has implemented when hosting and attending Zoom meetings and webinars:

Risk	Responsibility	Security Configuration Considerations
Zoom Bombing	Hosts	*** The following are considerations for all VC products *** Use the existing feature to generate a random meeting ID and passcode on all meetings Require webinar registration, set a password and explicitly approve registrations For internal meetings, consider choosing (in Settings) to allow only authenticated users into the meetings, which forces users to login to their Zoom account Select the setting to identify external participants as "guests" Do not allow expelled participants to rejoin
	Participants	*** The following are considerations for all VC products *** If you have a Zoom account, consider logging in so you can be authenticated to the host Do not post meeting ID and passcode information publicly or send to individuals who should not be at the meeting/webinar Do not join meetings without passcodes
Content Sharing	Hosts	*** The following are considerations for all VC products *** Restrict sharing to just hosts and co-hosts (lower risk) Only permit host to share when someone else is sharing (higher risk) Only share the application or content you intend the audience to see; do not share whole desktop.
	Participants	If you know you will share something during the meeting, consider asking the host to assign co-host privileges to you Be diligent in what and how hosts and others share during meetings. If something looks like it should not be shared, say something
Desktop Application Vulnerabilities	Hosts' security teams	Apply security updates and patches to Zoom desktop and mobile applications as soon as possible Use browser to join meetings and webinars to avoid installing desktop applications.
Privacy	Hosts	Mask phone numbers
General Security	Hosts' security teams	Enforce Single Sign On/MFA Enforce multi-factor authentication (MFA) for local Zoom authentication.
Refer to Zoom's security page at https://zoom.us/security for additional setting and recommendations		