Zoom Security & Privacy FAQs

Updated: April 13, 2020, v.4

With the onset of COVID-19, the Idaho Supreme Court issued an emergency order encouraging courts to use telephonic or video technology to conduct remote hearings. In 2019, the Idaho Supreme Court had already begun a limited deployment of Zoom for video remote hearings. Over the past 30 days, Zoom has now been deployed throughout the majority of Idaho courts as a tool for remote hearings.

Due to their massive growth over the past few months, Zoom has been placed firmly in the global spotlight – and rightfully so – regarding their security and privacy practices. The Idaho Supreme Court, along with courts across the globe, are equally concerned about any technology we deploy for court use. ***While there are very legitimate questions about Zoom security, it is important to understand that Zoom can and does provide a secure, usable platform for our courts when used correctly.*** Just like other cloud-based video solutions, Zoom has similar security capabilities and challenges. Zoom can be configured to meet various compliance requirements and has been used in various regulated industries for quite some time, but it does require an intentional approach.

As part of the response to COVID-19, Zoom has been quickly rolled out by many organizations – and some of those organizations moved forward without fully thinking through the security decisions needed for their Zoom instance. Additionally, due to its growing prevalence, the Zoom platform is now a larger target for attackers. This increased focus on Zoom's security and privacy practices is good and healthy, and the Idaho Supreme Court is actively reviewing any new claims regarding security or privacy concerns of this platform to fully understand the legitimacy and risk of each concern, what options are available to address the risk (if needed), and how best to mitigate the risks for each specific issue.

The purpose of this document is to highlight the most common and relevant issues highlighted about Zoom, and most importantly, what actions have been or need to be taken to address these risks.

"Zoom Bombing"

Issue: A third party could potentially "bomb" a public Zoom meeting and use the screen-sharing feature to project graphic content to meeting participants.

Configuration Changes to Mitigate Risk:

- Zoom is configured to require a password for entry to the session. This password may be embedded in the invitation link and/or sent separately to session invitees.
- Individuals are not allowed to join a meeting until the Host starts the session.
- ***Update (4/13/20):*** The Waiting Room feature is required for all meetings. This feature enables the capability to virtually stage entry into the session, allowing Hosts to control entry into the meeting.

User Actions Required:

- Hosts are trained to share meeting links to those who are invited to the session.
    - Note: The Idaho Supreme Court is working on a solution to live stream Zoom meetings so members of the public can view public hearings.
- Hosts are trained on how to remove unwanted or disruptive participants.
- ***Update (4/13/20):*** Hosts are encouraged to use a randomly generated meeting ID for external meetings. Use of a personal meeting ID should be used infrequently and only for internal meetings.
- Hosts can turn someone's video and/or audio off to block unwanted, distracting, or inappropriate comments.

Zoom Chat Could Lead to Compromising a User's Windows Account

Issue: An attacker could launch a "Universal Naming Convention" (UNC) path attack to capture a user's Windows username and password "hash" that could be decrypted, and gain access to the user's Windows account.

Zoom Response to Mitigate Risk:

- Upon learning of this vulnerability, Zoom updated their software to prevent this attack from being successful.

User Actions Required:

- Zoom automatically pushes updates of their software to clients. When starting Zoom, a dialogue box will be presented to the user informing them of these updates (when available).
    - Some of these updates are Mandatory and must be installed before the user can proceed further.
        - Critical security issues often fall into this category.
    - Other updates are Optional and will install when the user clicks on update. The user can proceed by postponing the update until a later time.
        - It is highly recommended that all users to accept Optional updates as soon as possible.
        - The Idaho Supreme Court will monitor Zoom client versions to identify systems that need to be updated and will take action as warranted.

An Attacker can Take Over a Mac User's Camera and Mic

Issue: An attacker could take over the camera and microphone on a Mac by designing a method to remove and reinstall Zoom with malicious code.

Zoom Response to Mitigate Risk:

- Upon learning of this vulnerability, Zoom updated their software to prevent this attack from being successful.

User Actions Required:

- Zoom automatically pushes updates of their software to clients. When starting Zoom, a dialogue box will be presented to the user informing them of these updates (when available).
    - Some of these updates are Mandatory and must be installed before the user can proceed further.
        - Critical security issues often fall into this category.
    - Other updates are Optional and will install when the user clicks on update. The user can proceed by postponing the update until a later time.
        - It is highly recommended that all users to accept Optional updates as soon as possible.
        - The Idaho Supreme Court will monitor Zoom client versions to identify systems that need to be updated and will take action as warranted.

Zoom's Claim of using End-to-End Encryption is Misleading

Issue: Zoom has stated it supports end-to-end encryption, but the service actually only encrypts data in transit when using the Zoom application.

Zoom Response regarding this Risk and Mitigation Actions:

- Zoom clarified that it has always strived to use encryption to protect content in multiple scenarios but acknowledged that it does not always fully apply end-to-end encryption if users connect, *without the Zoom app,* by a traditional telephone line or from a SIP/H.323 room-based system.
- When using the Zoom app on a computer, tablet, or phone, all client data sent to other Zoom users is encrypted.
    - Zoom servers do not decrypt any encrypted communication before it reaches the receiving Zoom user.
- When using a traditional telephone line or a SIP/H.323 room-based system, the communication becomes encrypted in the Zoom cloud through the use of Zoom's Connectors or Gateways.
    - When not using the Zoom app, the communication of the phone conversation from a user's phone over the public switch telephone network (PSTN) is unencrypted between the phone and the Zoom Telephony

Connector. This is similar to most non-Zoom telephonic phone calls (either landline or cellular) which are not encrypted.
    - When not using the Zoom app, the communication from a SIP/H.323 room-based system is unencrypted between the device and the Zoom Cloud Room Connector.

User Actions Recommended:

- When using a phone to connect to a Zoom session, users are encouraged to connect using the Zoom app for their device.
- The use of a SIP/H.323 room-based system is not currently in use for Idaho's Courts, so there is no risk at this time.

Zoom's Encryption Algorithm is not of the Highest Quality

Issue: A security research organization identified that Zoom's documentation states the app uses "AES-256" encryption for meetings when possible; however, in their research, they determined the app often uses "AES-128" in ECB (electronic codebook) mode which is not as strong. Specifically, ECB is a first generation block cipher which can present patterns and make it more susceptible to encryption compromise attacks.

Zoom Response regarding this Risk and Mitigation Actions:

- Although encryption is in place when using the Zoom app, Zoom acknowledged the need to "do better with (Zoom's) encryption design" (Zoom CEO Eric S. Yuan) and is expected to announce improvements in the near future.
- ***Update (4/13/20):*** Zoom is working to upgrade their encryption from AES-256 ECD to AES-256 GCM. They have begun testing this change with limited customers and plan to expand to all customers over the next several months.

User Actions Recommended:

- None at this time. While this finding is accurate the risk is moderately low as encryption is used, and it would require an attacker to successfully compromise the Zoom meeting by executing an attack on the meeting's encryption algorithm during transit.

Zoom Routed Non-Chinese Meetings through China Networks

Issue: Some Zoom calls were routed through China as new customers were added to the Zoom platform. Additionally, a security research organization identified that Zoom calls between users in North America were occasionally communicating with servers in China.

Zoom Response regarding this Risk and Mitigation Actions:

- Zoom acknowledged that when they added server capacity in response to increased demand stemming from COVID-19, they began this buildout in China "where the outbreak began. In that process, (Zoom) failed to fully implement (their) usual geo-fencing best practices.
    - As a result, it was possible certain meetings were allowed to connect to systems in China, where they should not have been able to connect." (Zoom CEO Eric S. Yuan).
    - Per Zoom, this issue has been remediated and geo-fencing best practices are now enabled.

User Actions Recommended:

- ***Update (4/13/20):*** None at this time. Zoom's CEO, Eric S. Yuan, stated in a live webcast with customers on 4/8/2020 that Zoom has taken action to ensure no communication for North America meetings will be transmitted with servers in China. Zoom has implemented geo-fencing and whitelist controls mentioned to prevent this from occurring.

Zoom Sent iOS User Profiles to Facebook when Using iPhone or iPad Zoom Apps

Issue: When using the "log in with Facebook" feature in the iPhone or iPad Zoom apps, Zoom sent iOS user profile information to Facebook.

Zoom Response regarding this Risk and Mitigation Actions:

- Zoom stated that it was not aware of the profile-sharing aspect of the "log in with Facebook" feature and updated the iOS Zoom apps to address this issue.

User Actions Recommended:

- The Idaho Supreme Court does not recommend using the "log in with Facebook" feature for authentication.
- iOS users should ensure they have downloaded and installed the most recent update from the iOS App Store.

Zoom Data Usage / Privacy *(Update: 4/13/2020)*

Issue: Some individuals have expressed concerns that Zoom may provide user data to other companies or entities.

Zoom Response regarding this Risk and Mitigation Actions:

- Zoom stated that they "never share any user data from meetings." Zoom's CEO stated, "To process our online payments, we needed to use a third-party billing engine." However, no other data is provided to a 3rd party. He further stated, "The only data that we use internally from…meetings is the metadata, or the data about the performance of the meeting. This helps us with analytics and improving the meeting experience. … But selling data has never been part of our business model."