California Community Colleges | Information Security Center

Security Practices for Zoom Video Conferencing: A Guide for California Community Colleges | April 2020

Table of Contents

Introduction

As many California Community College district employees and staff are working remotely, there have been growing concerns around security and privacy when using the video conferencing application Zoom. This paper will outline the major security risks and concerns, and recommend steps that can be taken to remedy them.

Privacy & Security Concerns with Tips

"ZoomBombing" - Meeting Room Hijacking

There have been many cases of unwelcomed individuals joining meeting rooms and sharing inappropriate material via chat or webcam. This has become known as "Zoom bombing," and meetings hosted by education institutions have been the primary target.

The recommended solutions will be briefly covered and a link will be provided to the relevant Zoom Support article.

Recommendations to avoid "ZoomBombing"

> General Guidelines

- Use a unique Zoom ID for each meeting, avoid using your Personal Meeting ID.
- Do not post meeting links on social media.
- Do not share links to meetings you are invited to join without the host's approval. The host can send more invites to the relevant individuals or parties.
- Do not use your Personal Meeting ID when hosting public meetings or webinars.

> Manage Participants as the Host

As of April 6, 2020, Zoom has enabled waiting rooms and meeting passwords by default on free accounts, education accounts, and single-license accounts.

April 2020 Updates

1) Do not make meeting rooms open to the public. Require a password for attendees to join.

Meeting and Webinar Passwords

2) Utilize waiting rooms. This will enable the control and management of guests.
Waiting Room Configuration

3) If appropriate for a meeting, change the screen-sharing option to “Host Only.”
Manage Participants in a Meeting

4) Lock the meeting after a desired amount of time has passed. This will prevent new participants from joining, even if they have the meeting ID and password. This can be done through Host Controls.
Host and Co-Host Controls in a Meeting

5) Require participants to join a meeting using the same email they were invited with.

6) If there is no need to share files during a meeting, you can turn this capability off.
In Meeting File Transfer

7) If there is no need to annotate a screen share, you can turn off Annotation.
Annotation Tools

8) Disable private chat to prevent participants from chatting with each other. This can be very useful in an education environment.
Controlling and Disabling In-Meeting Chat

9) You should also consider making your meetings Screen Share only. This will disable webcam access, which will prevent participants from sharing inappropriate behavior.
Screen Share Only Meeting

To further enhance security, it is recommended to set up Single Sign-On authentication.
Configuring Zoom with Shibboleth

Examples of Security Concerns

Vulnerability to Automated Attempts at Finding Open Meetings

Randomly generated numbers result in actual meeting IDs allowing access to meetings that did not have a password requirement (Ex: War Dialing). Zoom has enabled the password requirement and waiting room by default for scheduled meetings.

Windows NTLM Credential Theft via UNC Links (Patched)

> ***Please note that a patch was released on April 2, 2020, which prevents Zoom from automatically hyperlinking UNC paths in the chat window. Please download or update to the latest version.***
>
> ***Zoom continues to utilize the NTLM protocol. It is still recommended to restrict its capacity as outlined in the "Recommended Solution" section.***

When a user clicks on a Zoom host link to attend a meeting, or clicks on a link provided in the chat window, NTLM traffic is sent through. This contains the user name and the password hash of a Windows account.

During a meeting, an attacker can steal these credentials via UNC path injection. The attacker will send a Windows networking UNC path, which Zoom automatically converts into a clickable link (i.e. \\my.server.com\images\cat.jpg). Once a meeting member clicks the link, Windows will attempt to connect to the site through an SMB file protocol, in this case to open that JPEG file. The victim's Windows user name and NTLM password hash are sent to the attacker's server. The hash can then be cracked through tools such as Hashcat or John the Ripper. The attacker can use the victim's credentials to access network resources and the file system of the victim's device or server.

Recommended Solution:

> Restricting NTLM: Outgoing NTLM traffic to remote servers
As of time of writing, Zoom has not patched the issue. You can use this temporary hotfix. Note that this solution only works for devices running Windows 10.

A. If you have administrator privileges:
1) Open the Group Policy Editor and select Computer Configuration.
2) Go to Windows Setting → Security Options → Network security: "Restrict NTLM: Outgoing NTLM traffic to remote servers." Select the Deny all option and save changes.

B. If you do not have access to the Group Policy Editor, try this instead:
1) Run the registry editor (Press and hold or right-click the Start button, then select Run. Enter regedit in the Open: box and select OK.)
2) Select:HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa \MSV1_0. Right-click on the screen, select "New", and then select "DWORD (32-bit) Value". Rename the newly created DWORD value to

RestrictSendingNTLMTraffic. Double-click on the renamed parameter and assign it the value “2”.

Video is not End-to-End Encrypted

End-to-End encryption, also known as E2EE, ensures that only users directly communicating with one another can read information shared with each other. The message is encrypted by the sender and decrypted by the guest; there is no middleman involved with the ability to decrypt the message. While Zoom’s security white paper states that a meeting host has the ability to enable End-to-End encryption, this option enables E2EE for chat messages only. Video is still handled by Transport Layer Security (TLS).

With TLS, the message is still encrypted by the sender; however, this connection is initiated with the vendor’s server. Think of the server as the middleman between you and the individual(s) you are in a call with. TLS terminates once communication is sent back to the server, and the company owning the server can view call information since it is not encrypted. The communication may be encrypted through TLS again once it is sent over to the recipient.

While this may not be a concern for most end users, Zoom has the capacity to look at private meetings and can provide recordings or details of meetings to governmental organizations or to companies interested in data collection. It should be noted that while Zoom possesses the ability to distribute user information, its official privacy policy states that “We do not allow marketing companies, advertisers or similar companies to access personal data in exchange for payment.”

macOS Security Flaws and Patches

This issue has been patched by Zoom as of April 2, 2020. Please update Zoom right away.

Root Privilege Escalation

The Zoom installer uses the deprecated AuthorizationExecuteWithPrivileges API to successfully complete installation tasks. This enables users without administrator privileges to install Zoom on their machines. This can be worrisome if your organization uses MacOS devices on an enterprise level.

As a further note, AuthorizationExecuteWithPrivileges was deprecated nearly a decade ago due to the risk of an attacker with file system access to escalate their own privileges by tampering with applications using this API.

For more information on the contents of this guide, please contact:

Omer Usmani
Security Analyst
Information Security Center
California Community Colleges Technology Center
ousmani@ccctechcenter.org

References

https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf

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

https://support.zoom.us/hc/en-us/articles/360041591671-March-2020-Update-to-sharing-settings-for-Education-accounts

https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

https://www.nytimes.com/2020/03/30/technology/new-york-attorney-general-zoom-privacy.html

https://www.bloomberg.com/news/articles/2020-03-31/zoom-sued-for-allegedly-illegally-disclosing-personal-data

https://securityboulevard.com/2020/03/using-zoom-here-are-the-privacy-issues-you-need-to-be-aware-of/

https://objective-see.com/blog/blog_0x56.html

https://developer.apple.com/documentation/security/1540038-authorizationexecutewithprivileg (Deprecated API Call)