Are Zoom Meetings Secure Enough for My Organization?

Published 21 May 2020 - ID G00725809 - 14 min read

By Analysts Patrick Borka, Patrick Hevesi

Initiatives: Security Technology and Infrastructure for Technical Professionals and 1 more

An increase in Zoom security concerns is driving organizations to reevaluate the platform as a long-term solution to the increased demand for a remote workforce. This research can help security and risk management technical professionals determine if Zoom is secure enough for their organization.

Overview

Key Findings

■ Disparities between Zoom's marketing and documentation, and its actual security posture, have created a void in trust in Zoom by security organizations.

■ When configured properly, and when using enterprise features such as SSO, Zoom is a reasonably secure meeting platform for organizations.

■ The free version of Zoom does not have administrative-definable meeting policy controls.

■ A significant number of Gartner recommended settings are “off” and/or “unlocked” (user definable) by default, leaving meeting options unsecure or giving the user the ability to alter meeting settings to be unsecure.

Recommendations

To secure Zoom, security and application technical professionals must:

■ Choose Zoom's Business meeting plan to enable MFA or Enterprise meeting plan to enable SSO and the MFA licensing level. Then, adjust meeting policies and settings to increase security beyond default configuration.

■ Prevent “Zoombombing” by configuring Zoom meeting options such as using randomized meeting codes and waiting rooms and requiring passwords.

■ Upgrade all clients to version 5.0 to move up to the latest encryption standards.
Analysis

In recent months, Zoom has come under increased scrutiny over security and privacy practices. Gartner has also observed discrepancies between marketing materials, documentation and security standards used by Zoom. Although some of the issues surfaced are legitimate security concerns, some are preventable configuration issues.

Overall, Zoom has reacted quickly to most security concerns and demonstrated the developmental agility to push out most fixes in a timely manner. The deeper concern now is one of trust. Zoom has not subjected its platform to unrestricted audit by independent third parties. Without an independent verification, Gartner cannot fully evaluate how secure Zoom is.

This research will identify known past and current issues, their status, and remediation steps. It is intended to be concise and help clients determine if Zoom is secure enough for their environment. This research is based on information available to Gartner as of 11 May 2020 and covers major recent security and privacy concerns. It is not an exhaustive issue register.

Zoombombing (Configuration)

Status: Reasonably resolved (still possible if misconfigured)

By focusing on making the meeting solution easy for the attendees to get in and operate, organizations that accepted Zoom’s default configuration settings inadvertently left meetings open with little or no controls on who entered or their permissions once inside. This led to the practice of “Zoombombing,” where a malicious user could, through systematically guessing meeting IDs, connect to a user’s meeting room. Once inside, the unwanted guest can use audio and video and share content if the meeting configuration is not set to forbid it (with options such as “Only the Host Can Share”). Although Zoom has since put controls in place to significantly reduce Zoombombing, there are still those who share meeting URLs without any meeting options configured to prevent unwanted entry.

Therefore, the practice of Zoombombing is more of a configuration issue than a security vulnerability. Organizations that put controls in place for meeting entry — such as passcode requirements, virtual lobbies and randomized meeting IDs — are not vulnerable to Zoombombing. Organizations were exposed to the risk because they did not install reasonable precautions for meeting entry.

For more information on Zoombombing, see “Beware of ‘ZoomBombing’: Screensharing Filth to Video Calls” (TechCrunch).

Encryption Issues (Security)

Status: Resolved as of version 5.0 (rolling out)

- Use adoption programs to train your users on meeting controls, classification and etiquette.
Zoom’s encryption standards have been called into question recently. Although Zoom’s security white paper indicated 256-bit AES encryption as the standard for its meeting solution, a report by the University of Toronto’s “Citizen Lab” found that 128-bit AES is used in Electronic Codebook (ECB) mode. Although the key length is still considered sufficiently strong, the ECB mode is a legacy standard.

Figure 1 shows how ECB is inefficient to mask images and video streams.

Figure 1. Example of ECB Mode Encryption

Source: Gartner (May 2020)

As of 27 April 2020, Zoom has stated it modernized its encryption practices in its 5.0 release. Zoom also stated that 5.0 uses 256-bit AES GCM encryption. Zoom also announced that it intends to allow only 5.0 or later versions across PC, mobile and Zoom Rooms to join meetings after 30 May.

The Citizen Lab also found that, in some cases, meeting users would be routed through Beijing, China. Even though the encryption technology being employed was the same, the encryption key used in meetings that are routed through China potentially could be requested by Chinese authorities and used to intercept meeting traffic (although for the average user, this would be unlikely to happen).

Zoom stated that it maintains a whitelist of available servers to establish geofencing around mainland China to ensure that users outside of China do not have their meeting data routed through there. The routing issues described in Citizen Lab’s research were caused when Zoom failed to fully implement its usual geofencing best practices.

This issue has since been resolved. Additionally, paid Zoom customers are now able to further customize which data center regions their account can use for real-time meeting traffic.

For more information on the Citizen Labs report, see “Move Fast and Roll Your Own Crypto” (Citizen Lab).
Waiting Room Vulnerability (Security)

Status: Resolved

While investigating Zoom security, Citizen Lab also discovered another vulnerability within the meeting's virtual waiting room. In this case, Citizen Lab showed that, when using the virtual meeting room, the session key was exposed along with a video stream. Although the stream did not include audio and was not displayed on the users’ screen, having the 128-bit AES key and the video stream available meant that someone could have decrypted and viewed the video stream.

Zoom has since resolved this issue with a server-side patch.


The fix was also confirmed via Citizen Lab.

End-to-End Encryption (Security)

Status: Open (in development)

Although Zoom has stated its meetings are encrypted end to end, this is misleading. The definition of end-to-end encryption means the data is not decrypted at any point in the path between the users. In this case, Zoom is using TLS (Transport Layer Security) to encrypt sessions between users and the Zoom meeting servers. Because the information is encrypted only in transport, Zoom could, in theory, intercept meetings.

Although Zoom’s end-to-end encryption stance was misleading, it’s not uncommon. Zoom approaches the blending of real-time communications (RTC) like audio and video streams by using services it calls “multimedia routers.” These services combine and package multiple RTC streams into a single stream by combining them rather than using a more traditional multipoint control unit (MCU) as a central participant aggregation point.

Zoom now faces a trust issue and plans to remediate this by giving third parties full system access to audit its systems and publish independent audit finding reports. These reports are standard in the industry to help provide trust in the underlying infrastructure, people and processes being used to protect the service. Based on the previous inconsistencies found in what Zoom had stated in its marketing and documentation, and the actual security capabilities, this has led to a lack of trust that Zoom will have to work at gaining back with security organizations. As of May 2020, Gartner does not know who the security auditors will be, nor has there been a firm timeline for the reports.

As Zoom strives to gain traction in the enterprise market for videoconferencing and collaboration platforms, a strong security posture is critical. Zoom has recently become the subject of intense security scrutiny. It is commendable that Zoom’s position was not to deflect attention away from its problems but instead admit that it needed to become better.
Incorporating Keybase’s encryption mechanism will allow Zoom to offer something that hasn’t been done before, presuming the technologies can be properly integrated. The result — multiparty end-to-end encryption controlled by the meeting host — will shield participants from eavesdropping by anyone, including Zoom.

Combined with improved default security settings to reduce customer misconfiguration, the outcome might very well set a new standard for private conversations. Zoom’s decision to release a public draft of its planned cryptographic design later in May is a necessary step toward improved transparency. Zoom should go further, though, and work toward obtaining independent third-party attestations, which are increasingly common for cloud-provided applications.

For more information on the Keybase acquisition, see “Zoom Acquires Keybase and Announces Goal of Developing the Most Broadly Used Enterprise End-to-End Encryption Offering” (Zoom blog).

UNC Path Exploit (Security)

**Status: Resolved**

Users of the Zoom for Microsoft Windows client could use a universal naming convention (UNC) path exploit. In this vulnerability, users of Zoom’s Windows client could send a malicious UNC path, such as “\namorip\file,” to other users via the chat interface. In this case, if the recipient clicked the link, the sender or attacker could capture authentication data intended for the recipient. The passwords are not plain text, but they are NT LAN Management (NTLM) and still easy to decipher using common password-cracking tools such as Hash Crack or Ophcrack.

Zoom has since resolved this issue with its 2 April 2020 version 4.6.9 (19253.0401) release of the Zoom for Windows client.

For more information on the UNC path issue, see “New Zoom Hack Lets Hackers Compromise Windows and Its Login Password” (The Hacker News).

Macintosh Zoom Client Exploit (Security/Configuration)

**Status: Resolved**

Around July 2019, Jonathan Leitschuh discovered a web service running on his machine in support of the Zoom client. He was able to force the software to join a meeting with video. It was also discovered that the web server would reinstall the client if it was removed.

Because default video can and should be disabled, this was a bit of both a security vulnerability and a configuration issue, and Zoom has since removed the web server from Macs.

For more information on Jonathan Leitschuh’s post, see “Zoom to Patch Flaw That Enabled Access to Mac Webcams” (AppleInsider).

Facebook iOS Client (Privacy)
Status: Resolved

For the iOS version of its client, Zoom used the Facebook SDK to access Facebook's Graph API and enable authentication to Zoom with Facebook credentials. The Zoom client also shared data back to Facebook, such as user information and detailed device information like location, carrier and a unique device code. The sharing of this information may violate user privacy.

Zoom has since removed this capability and switched the Facebook authentication to a web version.

For more information on the Facebook consumer data issues, see “Zoom iOS App Sends Data to Facebook Even If You Don't Have a Facebook Account” (Vice).

Recommendations

Gartner recommends using the Business or Enterprise meeting plans to enable administrative controls and to gain access to the SSO options.

The first step should be to configure user authentication. Organizations already using single sign-on tools — such as Azure AD, Okta and Ping Identity — should enable the Zoom SSO integration. This is to control account access to corporate Zoom meetings. This also helps ensure disabled corporate accounts no longer have access to Zoom. Consider disabling the Facebook and Google sign-in integration unless it is a part of your organization's SSO strategy.

Once enabled for Business or Enterprise plans, the below settings are a recommendation for a new baseline for Zoom meetings. These are recommendations to help add additional meeting safeguards and authentication and security capabilities above the default settings. These settings should be reviewed by the security team to ensure alignment with current security policies for each organization before adoption (see Tables 1 through 3).

Account Settings>Meetings>Schedule Meeting

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Recommended</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host video</td>
<td>Off/Unlocked</td>
<td>Off/Locked</td>
<td>Start meeting with host video on.</td>
</tr>
<tr>
<td>Participants</td>
<td>Off/Unlocked</td>
<td>Off/Locked</td>
<td>Start meetings with participant video on.</td>
</tr>
<tr>
<td>video</td>
<td></td>
<td></td>
<td>Participants can change this during the meeting.</td>
</tr>
</tbody>
</table>

Gartner, Inc. | 725809
<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Recommended</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Personal Meeting ID (PMI) when scheduling a meeting</td>
<td>Off</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>Use Personal Meeting ID (PMI) when starting an instant meeting</td>
<td>Off</td>
<td>Off</td>
<td></td>
</tr>
<tr>
<td>Only authenticated users can join meetings</td>
<td>Off/Unlocked</td>
<td>On/Locked</td>
<td>The participants need to authenticate from a web client prior to joining meetings.</td>
</tr>
<tr>
<td>Require a password when scheduling new meetings</td>
<td>On/Unlocked</td>
<td>On/Locked</td>
<td>A password will be generated when scheduling a meeting, and participants require the password to join the meeting.</td>
</tr>
<tr>
<td>Require a password for instant meetings</td>
<td>On/All Meetings/Unlocked</td>
<td>On/All Meetings/Locked</td>
<td></td>
</tr>
<tr>
<td>Require a password for Room Meeting ID (Applicable for Zoom Rooms only)</td>
<td>Off/Unlocked</td>
<td>On/Locked</td>
<td>A password will be generated for Room Meeting ID, and participants require the password to join the meeting.</td>
</tr>
<tr>
<td>Embed password in meeting link for one-click join</td>
<td>On/Unlocked</td>
<td>Off/Unlocked</td>
<td>The meeting password will be encrypted and included in the join meeting link to allow participants to join with just one click without having to enter the password.</td>
</tr>
<tr>
<td>Option</td>
<td>Default</td>
<td>Recommended</td>
<td>Notes</td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Require password for participants joining by phone</td>
<td>Off/Unlocked</td>
<td>On/Locked</td>
<td>A numeric password will be required for participants joining by phone if your meeting has a password.</td>
</tr>
<tr>
<td>Enforce to use OAuth 2.0 only to authenticate Office 365 calendar integration</td>
<td>Off</td>
<td>On</td>
<td>Enabling this setting will force users and Zoom Rooms to authenticate the calendar service.</td>
</tr>
</tbody>
</table>

Source: Gartner (May 2020)

Account Settings>Meetings>In Meeting (Basic)

Table 2: Account Settings>Meetings>In Meeting (Basic)

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Recommended</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require encryption for third-party endpoints (H.323/SIP)</td>
<td>Off/Unlocked</td>
<td>On/Locked</td>
<td>Zoom requires encryption for all data between the Zoom cloud, Zoom client and Zoom Room. Require encryption for third-party endpoints (H.323/SIP).</td>
</tr>
<tr>
<td>Chat</td>
<td>On/Saving Off/Unlocked</td>
<td>On/Saving Off/Locked</td>
<td>Allow meeting participants to send a message visible to all participants.</td>
</tr>
<tr>
<td>Screen sharing</td>
<td>All Participants/Host Only/Unlocked</td>
<td>Host Only/Host Only/Locked</td>
<td>Allow host and participants to share their screen or content during meetings.</td>
</tr>
<tr>
<td>Far-end camera control</td>
<td>Off/Unlocked</td>
<td>Off/Locked</td>
<td>Allow another user to take control of your camera during a meeting.</td>
</tr>
</tbody>
</table>
Gartner recommends using a single sign-on option for password management. The use of a single sign-on solution will supersede sign-in configuration, password policies and multifactor authentication settings in the Zoom admin console.

**Conclusion**

Based on the information available to Gartner, Zoom is a reasonably secure meeting platform for meetings that do not have sensitive content. Zoom has shared its chosen partners of Trail of Bits, Bishop Fox and NCC Group, with a time frame of mid-July 2020 for an independent security verification report. The partners selected are deemed by Gartner to be reputable and thorough. Until the findings of those partners are made available, Gartner cannot issue a complete security posture.

---

**Table 3: Account Settings>Meetings>Admin Options**

<table>
<thead>
<tr>
<th>Option</th>
<th>Default</th>
<th>Recommended</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify guest participants in the meeting/webinar</td>
<td>Off/Unlocked</td>
<td>On/Locked</td>
<td>Participants who belong to your account can see that a guest (someone who does not belong to your account) is participating in the meeting/webinar.</td>
</tr>
<tr>
<td>Waiting room</td>
<td>Off/All Participants/Unlocked</td>
<td>On/All Participants/Locked</td>
<td>Attendees cannot join a meeting until a host admits them individually from the waiting room.</td>
</tr>
<tr>
<td>Blur snapshot on iOS task switcher</td>
<td>On/Unlocked</td>
<td>On/Locked</td>
<td>Enable this option to hide potentially sensitive information from the snapshot of the Zoom main window. This snapshot displays as the preview screen in the iOS tasks switcher when multiple apps are open.</td>
</tr>
</tbody>
</table>

Source: Gartner (May 2020)

**Advanced>Security**

Gartner recommends using a single sign-on option for password management. The use of a single sign-on solution will supersede sign-in configuration, password policies and multifactor authentication settings in the Zoom admin console.
Organizations are faced with keeping their employees connected and productive as they are working from home, but that should not sacrifice best practices. Zoom has a historical focus on ease of use. Zoom was able to reduce meeting join friction by not setting default meeting controls like meeting lobbies and meeting passwords.

The free version of Zoom should never be used for enterprises and businesses because it does not have as many security options and does not support SSO, and because configuration is not administratively definable. Although Zoom has more security controls in the Business and Enterprise versions, they are disabled by default. Organizations planning to use Zoom should follow the Gartner-prescribed settings as a baseline. By enabling additional features like SSO, meeting passcodes, virtual waiting rooms and rotating meeting codes, Zoom meetings lose their ease-of-use differentiator from other solutions.

Almost as important as proper configuration settings are change management and adoption planning strategy. Organizations’ first line of security is at the user. In addition to knowing how to use the meeting solution, users should understand risk and etiquette that can lead to security issues.

After adjusting the security settings, Zoom can be used reasonably securely. However, Zoom has not undergone a proper security audit. For this reason, Gartner does not recommend Zoom where highly secure communications is a concern.

**Acronym Key and Glossary Terms**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Glossary Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
</tr>
<tr>
<td>ECB</td>
<td>Electronic Codebook</td>
</tr>
<tr>
<td>GCM</td>
<td>Galois/Counter Mode</td>
</tr>
<tr>
<td>MCU</td>
<td>multipoint control unit</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>SSO</td>
<td>single sign-on</td>
</tr>
<tr>
<td>RTC</td>
<td>real-time communications</td>
</tr>
</tbody>
</table>

**Recommended by the Authors**

*How to Evaluate Cloud-Based Meeting Solutions*