smartdesc
smart decisions

Zoom Security Statement

A Review of Zoom Security Issues

Date: 21 May 2020

Andrew Coyle, Head of Information Security

Document control	Contact	Date
V1.0	Andrew Coyle, Head of Information Security	**14/05/20**
V1.1	James Field, Strategy Director [release]	**19/05/20**

Contents

Introduction

The rise in popularity of Zoom has coincided with several security issues being identified, causing organisations concern as to whether Zoom is a suitable option for their video conferencing requirements.

At the time of writing there have been several issues that have affected Zoom and come to light over recent months. Some have already been resolved, some we have seen affect our customer base whilst others are unlikely to be a cause for concern. Zoom is safe for most people and organisations, but these issues need consideration as to how and where Zoom should be used.

The information below provides a short amount of explanation of the issues that have been identified, the response from Zoom and information that will hopefully help to determine whether Zoom is suitable to use for a specific type of meeting situation.

Below the Security Statement is a brief FAQ and a user guide to setting up Secure Meetings accompanies this document.

1. Recent Security Issues Zoom have faced

Zoombombing

Zoombombing has become a significant issue, this is where unattended guests join a Zoom meeting to cause disruption with some of the worst cases being where disturbing images or videos have been displayed on screen.

We have seen Zoombombing taking place within our customer base and it is an issue that could affect other customers. Zoombombing takes advantage of meetings that haven't been setup securely and the risks can be vastly reduced by following the steps in the accompanying guidance to setup secure meetings.

The good news is that Zoom have now implemented Security policies by default including mandatory passwords, the use of waiting rooms and only hosts being able to share screens, all of which reduce the risk of Zoombombing.

End to End Encryption

Encryption is used to prevent unauthorised access to information by making it unreadable to those who are not authorised. End to end encryption should mean that only the meeting attendees would be able to access the information and that is what Zoom claimed to have in place.

There have been several articles written about Zoom's use of end to end encryption and it is widely reported that full end to end encryption is not actually in place.

In practice this means that meetings are encrypted but Zoom have the decryption keys so could access the data, and if zoom could access the data there is a chance that highly motivated attackers could too.

The risk around end to end encryption is likely to only affect organisations where secrecy is paramount but with Zoom now being used in high sensitivity settings such as Government and Healthcare consideration is needed for what types of meetings Zoom is suitable for hosting.

Zoom have also acknowledged that their definition of end to end encryption was inaccurate and have purchased a Security organisation who are working on implementing full end to end encryption.

Other Security Vulnerabilities

There have been security flaws that are legitimate bugs in Zooms software including ways in which users passwords could be stolen or malware could be installed if a meeting attendee could be tricked into clicking on a malicious link in the call. All live issues like this have been resolved in the latest version of Zoom.

There have also been several security flaws reported that are generic security issues that all software vendors face. For example there have been reports of Malware being included in Zoom install files but this can be the case with any software when it hasn't been downloaded from the original source – in this case Zooms website.

Mozilla, the non-profit maker of the Firefox web browser and strong Privacy advocate, have spent time reviewing Zoom as well as their competitors and Zoom now receives a score of 5/5 for encryption, password strength, updates, bug reporting and privacy – no doubt due to all of the scrutiny and necessity to fix the Security issues that have been identified. This rating is the same as Skype, Signal and Google Hangouts whilst being higher than the score that Apple FaceTime received which was 4.5/5.

Selling User Data

Zoom's Privacy Policy has come under the spotlight as it appeared to allow Zoom to pretty much do what it likes with Zoom user's personal data. When this was publicly scrutinised Zoom moved quickly to amend the Privacy Policy and have since publicly stated that they don't sell users personal data. It has also been stated that Zoom's competitors such as Google and Cisco have similar statements in their Privacy Policies.

2. Zoom Statement

Zoom have taken steps to try and correct the issues that have been identified, these include reaching an agreement with the New York Attorney General to improve Security through measures including making passwords mandatory, regular reviews of their code and annual penetration testing exercises.

Zoom have also bought a Security Company called Keybase to ensure that they can implement full end to end encryption.

Zoom will also enforce an update to their Desktop application at the end of May to ensure that everyone is on the latest most secure version. This is version 5 which is available now.

Zooms CEO provided a statement on a live Youtube stream to apologise for the Security issues that they have faced and their response to them which the BBC covered and you can read the article here.

3. Summary

As with all thing's security related there is a balance between usability and risk. Zoom provides a really useable system and a lot of the issues identified are unlikely to affect most individuals or organisations, that being said it is important that if zoom is being used, the context of a meeting is taken into consideration.

If the meeting is particularly sensitive then the issues above come into play, for example where a meeting may involve Children and Young people the risk of Zoom Bombing becomes more acute.

If organisations are deciding whether Zoom is the right solution, then they will need to assess how many of their meetings are sensitive and decide accordingly whether Zoom is a suitable solution for them.

Security Expert Graham Cluley has summarised these decisions in the paragraph below:

"Fixing these problems will take time. And those particularly high-risk users of Zoom, having highly sensitive discussions on the service, who might potentially be the target of state-sponsored attacks (for instance the UK cabinet), might be wise to find alternative, more secure methods of communication in the meantime."

4. Frequently Asked Questions

As an organisation should we be using Zoom?

Each organisation should go through a process of determining whether they should work with a third-party vendor and Zoom is no different. In terms of Security Zoom is suitable for most individuals and organisations. That being said there are scenarios where Zoom is not the right solution and this may be the case if video conferencing is going to be used for discussing information that is of a sensitive nature.

Where there are potential risks to individuals based on their personal information being processed a Data Protection Impact Assessment should be completed and can help to assess the risks to individuals and come to a good decision.

Is Zoom Secure?

Six months ago Zoom clearly had some Security issues that were yet to be identified and have indicated that they hadn't done enough to secure their software but due to necessity Zoom have now implemented significant Security improvements. I still wouldn't use Zoom for highly sensitive meetings discussing highly sensitive information but certainly feel that it is secure enough for use by most individuals and organisations.

A contrarian view from some well-regarded Security researchers is that with all the publicity around these Security issues Zoom may well find itself having the best Security out of the video conferencing solutions, a necessity as they have become the most prominent and targeted solution.

It is hard to say that other solutions don't have the same security issues that Zoom have faced, but Zoom is in a position where they are being targeted by Security researchers and pranksters which increases the risk of an Incident happening when using zoom, although the likelihood is far lower now with default security settings deployed in the latest versions.

It is of course imperative that everyone installs the latest version of zoom or uses the web browser version to make sure that the latest security settings are in place.

Should we use Zoom if our meeting involves disclosing sensitive information such as information about someone's health?

Recently we have seen organisations who provide healthcare services that have become more reluctant to use Zoom due to the risks around highly sensitive data. If Zoom is to be used for these services then it must be done with the upmost care using the full extent of Zooms Security capabilities.

Should we record Zoom meetings?

If there is a requirement to record Zoom meetings then steps should be taken to ensure that the recording is stored on the organisations systems rather than to the cloud which is the default option. Recordings are stored on servers in the US by default which is an issue for GDPR Compliance and there have also been incidents where Zoom recordings have been discovered by Security researchers without any protection. For information about how to change the default recording settings follow the instructions here and set your recording to save in a secure location (please contact IT to discuss where recordings should be saved.)

What is Zoombombing?

Zoombombing is where an uninvited third-party gains access to a Zoom room with the aim to cause disruption by sharing highly inappropriate and distressing content.

Why does Zoombombing happen?

Zoombombing happens because a third party has gained access to your meeting ID through a process of elimination and your meeting hasn't been password protected. If the option to password protect meetings has been enabled in the Zoom settings, it becomes very difficult for a third party to access the session. Enabling another setting called 'waiting room' will place all attendees in a holding room until the host of the session allows them to enter.

How can we prevent Zoombombing from happening?

The most effective way to prevent Zoombombing is to enable settings such as 'waiting room' and that password protection on meetings is in place. This will make it much more difficult for a third party to hack their way into your Zoom room.

The settings necessary to prevent unwanted guests entering your Zoom room can be found within the accompanying Setting up Secure Meetings guidance document.

How can we be sure that Zoom is compliant with the GDPR?

It is each organisations responsibility to ensure that they have completed your due diligence on any system being used to process personal information. If you anticipate using Zoom for high risk activity i.e. Service user engagement, then you must complete a Data Protection Impact Assessment (DPIA) which should consider all of the potential risks to individuals and this assessment must be completed at the earliest opportunity.

You must also make sure that a contract containing the relevant data protection clauses has been put in place between your organisation and Zoom to remain compliant with certain aspects of data protection legislation.

Should I send documents through Zoom

No. Zoom should not be used to send documents to anyone, please use the approved file sharing solutions that are in place within your organisation.