Relativity®

Working Securely with Zoom

As many companies have shifted to a fully remote workforce in recent weeks, Zoom, a popular option for video conferencing software, has become more prevalent than ever. Unfortunately, this increase has made Zoom particularly attractive to bad actors seeking to disrupt meetings or hack into sensitive business data.

The bottom line is that any piece of software that received this kind of surge in use would draw increased attention from those who would exploit its vulnerabilities. No tool can be completely impenetrable, as the threat landscape is always evolving. The good news is that Zoom has been hard at work to identify their vulnerabilities, address them, and **support concerned users** along the way.

There are also a number of ways that users can protect themselves from hackers while using Zoom for business and personal conversations. The following tips from **Calder7**, Relativity's security team, can help.

Minimize "Zoom Bombing" Exposure

Recent news stories have reported people crashing into Zoom rooms uninvited, also called "Zoom bombing." This issue is of top concern for many when it comes to privacy, but it can be thwarted.

Set up your personal meeting room as follows to enable greater security.

1. Disable "Enable join before host" to ensure no one can use your room without you present.
2. Enable the password requirement on your personal meeting room. Only give out the password as needed and change it frequently.
3. Enable "Only authenticated users can join" to rely on Zoom's built-in process for authenticating users before allowing them to join your meeting.

End-to-End Encryption

You may have seen **media coverage** suggesting that Zoom is misleading customers with claims of end-to-end encryption. It's a complicated topic.

Zoom software implements what is called "encryption in transit." This is where data flowing over their network is encrypted from client to server, server to server, and server to client. The alternative is to terminate encryption at some boundary point, like a firewall, and proceed unencrypted from there. This type of encryption in transit is ubiquitous in the SaaS sector at this point.

So why would Zoom advertise their encryption capabilities, if encryption in transit is ubiquitous? The answer is that Zoom also integrates with phone technology to encrypt data on the client side. While most of a phone system is unencrypted, newer IP phones also offer the option of encrypting all the way to the device.

That's what Zoom is advertising. They have the capability to enforce the use of encryption on newer phones where that feature is available. In both cases, the Zoom servers are able to read the data unencrypted as part of servicing the meeting.

Regardless of settings, calls from the old phone system are never encrypted. To understand whether your implementation of Zoom is able to take advantage of end-to-end encryption, you'll need to find out whether the phone with which you're using Zoom—and those used by others on your call—is capable of doing so. For business devices, your IT team can provide insight on this matter.

Zoom Software Vulnerabilities

Zoom has identified a handful of vulnerabilities in their software, which their team has provided an update to resolve. Here's a list of vulnerabilities they've publicly disclosed:

Vulnerability	Protection	What can I do?
CVE-2019-13567 CVE-2019-13450 CVE-2018-15715 CVE-2014-5811 CVE-2004-0680	Update Zoom version	Check your Zoom version number. Any Zoom application running 4.4.53932.0709 or newer is in the clear.

It's important to note that the desktop Zoom client does not update automatically. If you haven't already, check your Zoom application for updates by following **these instructions**. Ensure the app is updated on your mobile devices as well.

Windows Credential Theft Vulnerability

On April 1, 2020, it was **reported** that a security researcher identified a new vulnerability in Zoom that allows an attacker to steal Windows credentials from a user. This vulnerability is not specific to Zoom software (unlike those listed at left), and can also be exploited through phishing or malicious web pages. As always, consider the sender before clicking on links regardless of where they appear.

For your Zoom room to be impacted by this vulnerability, each of the following conditions must be met:

1. An attacker would enter your Zoom room without invitation and post a clickable link in the meeting chat.
2. You would click the malicious link.
3. Upon following that link, your Windows computer will attempt to connect to a remote IP on the internet using the SMB file sharing protocol.
4. Your Windows username and password would be captured during this process and sent to the attacker.

If you've updated your Zoom application on Windows to version 4.6.1.19253.0401 or above, this vulnerability has been patched.

Bottom Line: Work Defensively

It can be frightening to see negative headlines about a piece of software you suddenly find yourself using every day. But, as with many cybersecurity vulnerabilities, you are far from powerless to protect yourself from the Zoom exposures currently making the news.

Knowledge is power. Use what you've learned here and follow **other security best practices** to keep yourself and your data protected as you adapt to the world of remote work.

NOTE: This guide was first published on April 9, 2020.

Relativity

231 South LaSalle Street | 8th Floor | Chicago, Illinois 60604
+1 (312) 263-1177 | relativity.com

© Relativity. All rights reserved.