An Ethics Assignment for Cybersecurity courses
Assessing a Zoom Vulnerability Disclosure Report

August 2020

Shiva Houshmand, PhD
Assistant professor of Computer Science
Santa Clara University

Step1: Reading assignment before class discussion

Please read the “Framework for Ethical Decision Making” by Markkula Center for Applied Ethics. The framework describes five approaches which will help you identify and analyze the ethical issues that arise in a particular set of circumstances, before making an ethical decision. You might want to print out the pdf at the bottom of the page, to consult in the subsequent portions of this exercise.

After reviewing the framework, read the “Zoom zero day vulnerability report” attached at the end of this assignment. This is a summary of an article published in July 2019 by a security researcher.

Question: Who are the stakeholders in this scenario? In other words, who are the people or groups impacted by the vulnerability found in the product and by the way that vulnerability was handled? You do not need to submit a written response at this time; just read the article and come to class prepared to answer this question.

We will discuss the article and the framework in class.

Step2: In-class discussion

Your instructor will help answer questions you might have about the ethical decision-making framework. Afterward, in small groups, please work to answer the following questions. We will then reconvene and discuss your responses with the class overall.

Discussion Questions:

- Do you identify any ethical issues in the way Zoom responded to the vulnerability disclosure? If yes, why do you think Zoom responded the way it did?
- How did responding in this way hurt/or help the company?
- What should be the ethical response by a company in regard to the disclosure of a vulnerability?

To learn more, read these two short articles about the aftermath of the vulnerability disclosure and what Zoom ultimately decided to do in response.

Zoom CEO apologizes for security problems on public live stream
Zoom to revamp bug bounty program, bring in more security experts

Step 3: Written assignment after in-class discussion

Each student is assigned a company. Research on whether the company has a guide for responsible disclosure of vulnerabilities or a vulnerability disclosure policy (VDP). Try to find this information on the company's website first, rather than a third-party website. You can use the third-party website information if needed in answering the following questions.

Answer the following questions in regard to this company. Answer to each question should be brief and in a few sentences.

1. Does the company have a guide for responsible disclosure vulnerabilities? If yes please provide the link to the policy.
2. Is there a clear set of instructions on how to submit the vulnerability? If yes, summarize the policy for submitting a vulnerability in a few sentences.
3. Do they promise to resolve or confirm the issue within a period of time?
4. Does the company provide any compensations or incentives for the report?
5. Did the company provide or mention the VDP directly on their website, or was it only mentioned on a third-party website?
6. How do you think the company can improve their VDP? Explain briefly.

Zoom Zero day Vulnerability Report

This article is a summary of Zoom Zero Day: 4+ Million Webcams & maybe an RCE (Remote Code Execution)? Just get them to visit your website!
You are not required to read the actual article, but feel free to take a look at it if you are interested.

Foreword

Jonathan, a security software Engineer and Researcher found a vulnerability in the Mac Zoom Client. A vulnerability in the Mac Zoom Client allows any malicious website to enable your camera without your permission. The flaw potentially exposes up to 750,000 companies around the world that use Zoom to conduct day-to-day business. Jonathan describes the steps he took to disclose the vulnerability to Zoom and how Zoom responded.

The vulnerability

This vulnerability allows any website to forcibly join a user to a Zoom call, with their video camera activated, without the user's permission. On top of this, this vulnerability would have allowed any webpage to DOS (Denial of Service) a Mac by repeatedly joining a user to an invalid call. Additionally, if you've ever installed the Zoom client and then uninstalled it, you still have a localhost web server on your machine that will happily re-install the Zoom client for you, without requiring any user interaction on your behalf besides visiting a webpage.

This vulnerability leverages the amazingly simple Zoom feature where you can just send anyone a meeting link and when they open that link in their browser their Zoom client is magically opened on their local machine.

Disclosure and Timeline:

Here are the timeline and steps taken by the researcher (Jonathan) to disclose the vulnerability, and Zoom's response. The following sections are all written by the researcher.

Day 0: March 26, 2019: This vulnerability was responsibly disclosed. Contacted Zoom Inc via email with 90-day public disclosure deadline. Offered a "quick fix" solution.

Day 1: March 27, 2019: - Requested confirmation of reception.
- Informed that Zoom Security Engineer was Out of Office.
- Offered and declined a financial bounty for the report due to policy on not being able to publicly disclose even after the vulnerability was patched.

Day 10: Apr 5, 2019 — Response from Zoom Security Engineer confirming and discussing severity. Settled on CVSSv3 score of 5.4/10. It took Zoom 10 days to confirm the vulnerability.

Day 23: Apr 18, 2019 — I disclosed the vulnerability to Chromium Security team and Updated Zoom with the suggestion from Chromium team.

Day 31: Apr 26, 2019 — I discussed the vulnerability with Mozilla Firefox security team. Video call with Mozilla and Zoom Security Teams.

Day 77: June 11, 2019 — Video call with Zoom Security team about impending disclosure. Discussed how Zoom's planned patch was incomplete. The first actual meeting about how the vulnerability would be patched, only 18 days before the end of the 90-day public disclosure deadline. During this meeting, the details of the vulnerability were confirmed and Zoom's planned solution was discussed. Jonathan was very easily able to spot and describe bypasses in Zoom's planned fix.

Day 86: June 20, 2019 — I was contacted by Zoom security team to have a video call with them but he declined due to calendar conflicts.

Day 87: June 21, 2019 — Zoom reports vulnerability was fixed.

Day 90: June 24, 2019 — Vulnerability confirmed fixed with 'quick fix' solution. After 90 days of waiting, the day of the public disclosure deadline, Jonathan discovered that Zoom had only implemented the 'quick fix' solution originally suggested.

Day 103: July 7, 2019 — Regression in the fix causes the video camera vulnerability to work again.

Day 104: July 8, 2019

- Regression fixed.
- Workaround discovered & disclosed.
- Public Disclosure.

Zoom's Proposed Fixes (written by Jonathan):
The fix proposed by the Zoom team was to digitally 'sign' the request made to the client. However, this simply means that an attacker would have to have a backend server that makes requests to the Zoom site first to gain a valid signature before forwarding the signature on to the client.

They also proposed locking the signature to the IP that made the request. This would mean that as long as the attacker's server was behind the same NAT router as the victim, the attack would still work.
I described to the Zoom team how both of these solutions were not enough to fully protect their users. Unfortunately, this left the Zoom team with only 18 days before public disclosure to come up with some better solution.

Unfortunately, even after my warning, this was the solution they chose to go with. This new signature or token is embedded in a new parameter called confid. This confid check can simply be bypassed (as described in the article). Alternatively, if you and the victim are behind the same NAT router, you can make a request for the join page, extract the #lhs_launch_parames field from the HTML document and embed it in the HTML response from the malicious page.

Conclusion (written by Jonathan):
As of 2015 Zoom had over 40 million users. Given that Macs are 10% of the PC market and Zoom has had significant growth since 2015 we can assume that at least 4 million of Zoom's users are on Mac. Tools like Zoom, Google Meet or Skype for Business is a staple of today's modern office.

Any vulnerability in an application with this many users must be considered a serious threat to all those users. All of the vulnerabilities described in this report can be exploited. Many times during my conversation with the Zoom security team they seemed to argue that the seriousness of this vulnerability was limited because it would require "user interaction" to exploit these. My response to this was finally "I would highly suggest that you not hang your hat on 'user interaction required' for protecting your users given that this 'user interaction' is simply clicking a link or visiting a webpage."

Consequences (written by Jonathan):
This is essentially a Zero Day. Unfortunately, Zoom has not fixed this vulnerability in the allotted 90-day disclosure window I gave them, as is the industry standard. As such, the 4+ million users of Zoom on Mac are now vulnerable to an invasion of their privacy by using this service.

[Note from instructor: The term "zero-day" refers to a newly discovered software vulnerability. Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn't been released. So, "zero-day" refers to the fact that the developers have "zero days" to fix the problem that has just been exposed — and perhaps already exploited by hackers. The software vendor may fail to release a patch before hackers manage to exploit the security hole. That's known as a zero-day attack.]]
[Note from instructor: Current recommendations for a healthy program is as follows: - time to first response = 1 day, time to resolution = 30 days]

Additionally, due to a lack of sufficient auto-update capabilities, many users continue to run outdated versions of Zoom for months after new releases are shipped leaving them vulnerable to exploits like these.

Notes For Researchers (written by Jonathan):
Given the massive install base for Zoom, I highly recommend that other researchers take the time to explore this Zoom web server to see what other vulnerabilities exist. This being said, I also recommend that any researcher that finds a vulnerability in Zoom's software does not directly report the vulnerability to Zoom. Instead, I recommend that researchers report these vulnerabilities via the Zero Day Initiative (ZDI). The ZDI disclosure program gives vendors 120 days to resolve the vulnerability, the ZDI will pay researchers for their work, and researchers have the ability to publicly disclose their findings.