Serious Zoom security flaw could let websites hijack Mac cameras

Today, security researcher Jonathan Leitschuh has publicly disclosed a serious zero-day vulnerability for the Zoom video conferencing app on Macs. He has demonstrated that any website can open up a video-enabled call on a Mac with the Zoom app installed. That's possible in part because the Zoom app apparently installs a web server on Macs that accepts requests regular browsers wouldn't. In fact, if you uninstall Zoom that web server persists and can reinstall Zoom without your intervention.

Using Leitschuh's demo, we have confirmed that the vulnerability works — clicking a link if you have previously installed the Zoom app (and haven't checked a certain checkbox in settings) auto joins you to a conference call with your camera on. Others on Twitter are reporting the same:

Leitschuh details how he responsibly disclosed the vulnerability to Zoom back in late March, giving the company 90 days to solve the problem. According to Leitschuh's account, Zoom doesn't appear to have done enough to resolve the issue. The vulnerability was also disclosed to both the Chromium and Mozilla teams, but since it's not an issue with their browsers, there's not much those developers can do.

Turning on your camera is bad enough, but the existence of the web server on their computers could open up more significant problems for Mac users. For example, in an older version of Zoom (since patched), it was possible to enact a denial of service attack on Macs by constantly pinging the web server: "By simply sending repeated GET requests for a bad number, Zoom app would constantly request 'focus' from the OS,"

Leitschuh writes.

You can “patch” this issue yourself by ensuring the Mac app is up to date and also disabling the setting that allows Zoom to turn your camera on when joining a meeting, illustrated below. Again, simply uninstalling Zoom won’t fix this problem, as that web server persists on your Mac. Turning off the web server requires running some terminal commands, which can be found at the bottom of the Medium post.

Jonathan Leitschuh

We have reached out to Zoom for comment and will update when we hear back directly. In comments to *ZDNet*, Zoom says that the web server is a “legitimate solution to a poor user experience, enabling our users to have seamless, one-click-to-join meetings.” *ZDNet* also says that Zoom will take further actions:

> *Zoom said in its July release, it would save whether the user turns off video in their first call and apply it to future meetings, with these changes will occur on all its platforms.*
>
> *Thanks to the report from Leitschuh, Zoom also removed the ability for a call host to automatically have participants join with video enabled.*

Updated 9:40PM ET with comments Zoom provided to ZDNet.

https://www.theverge.com/2019/7/8/20687014/zoom-security-flaw-video-conference-websites-hijack-mac-cameras