Zoom goes big on fix for conferencing vulnerability

July 10 2019, by Nancy Cohen

Settle down in a comfortable chair; breaks with cool washcloths are allowed. This is one of those Zero-Day stories with discoveries, responses, still newer discoveries and assorted updates.

A security flaw alarm on Monday, July 8, was sounded about conferencing. "This is essentially a Zero Day," said the sofware engineer

who spotted it. CNET said the security flaw was major; it was in a video-conferencing app that could enable websites to join you in video calls without your permission.

CNET's Australia-based Daniel Van Boom reported that the security researcher to discover all this was Jonathan Leitschuh, a software engineer, who had turned to a post in *Medium* to explain what he found.

This involved Zoom's Mac app. It has a click-to-join feature, said CNET, "where clicking on a browser link takes you directly to a video meeting in Zoom's app."

How simple: "Joining a call is particularly easy; with the click of a meeting URL, the page automatically launches the desktop app, and you're in," said Lily Hay Newman in *Wired*.

Here is the problem. This vulnerability "would have allowed any webpage to DOS (Denial of Service) a Mac by repeatedly joining a user to an invalid call."

Simple to fix on your own, right? Just uninstall Zoom. That was not so simple.

"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," Leitschuh had said, "without requiring any user interaction on your behalf besides visiting a webpage."

As of July 9, and before the big fix, several critics had remarked they were not comfortable with Zoom's use of a local web server on Mac computers. *Wired*: "Zoom sets up a local web server on every user's Mac that allows call URLs to automatically launch the desktop app. Zoom says that this setup is in place as a 'workaround' to a feature of Safari 12

that would require users to approve Zoom launching every time they click a call link."

And, beyond Zoom and Leitschuh, *Wired* carried remarks from Thomas Reed, a Mac research specialist at security firm Malwarebytes. "The local web server is honestly the most concerning part, and it's not fixed," said Reed. "The web server is concerning, because of the possibility that someone could find a way to use it remotely to trigger remote code execution."

CNET as of Monday, July 8, reported that, "In regards to a potential denial of service attack, Zoom says it has no record of such a weakness being exploited, and says it fixed that security flaw in May."

(Zoom patched this DoS issue in a May update. The Zoom blog had stated they released a fix for this in May 2019, "though we did not force our users to update because it is empirically a low-risk vulnerability.")

What has been Zoom's responses as of later on, July 9? When it rains it pours.

By later that afternoon, July 9, *The Verge* headlined "Zoom fixes major Mac webcam security flaw with emergency patch" and "The company is now removing local Mac web servers."

Wired issued another July 9 update article later in the day saying "AFTER INITIALLY SAYING that it wouldn't issue a full fix for a vulnerability disclosed on Monday, the video conferencing service Zoom has changed course. The company now tells WIRED that it will push a patch on Tuesday to alter Zoom's functionality and eliminate the bug. You should update Zoom now."

Over to the Zoom blog, where the July 9 updates had this to say:

"[UPDATE 2:35 pm PT, Tuesday 7/9] The July 9 patch to the Zoom app on Mac devices detailed below is now live. You may see a pop-up in Zoom to update your client, download it at zoom.us/download, or check for updates by opening your Zoom app window, clicking zoom.us in the top left corner of your screen, and then clicking Check for Updates."

Zoom ultimately heard, and responded, to the "outcry."

"[UPDATED 1:15 pm PT, Tuesday 7/9] We appreciate the hard work of the security researcher in identifying security concerns on our platform. Initially, we did not see the web server or video-on posture as significant risks to our customers and, in fact, felt that these were essential to our seamless join process. But in hearing the outcry from our users in the past 24 hours, we have decided to make the updates to our service."

At the time of this writing) this was the update in *Medium* from Leitschuh: "UPDATE—July 9th (pm). According to Zoom, they will have a fix shipped by midnight tonight pacific time removing the hidden web server; hopefully this patches the most glaring parts of this vulnerability. The Zoom CEO has also assured us that they will be updating their application to further protect users privacy."

More information: medium.com/bugbountywriteup/zo … website-ac75c83f4ef5