Zoom security feature let unapproved users view meetings, researchers find

April 10 2020, by Suhauna Hussainstaff Writer, Los Angeles Times

Credit: CC0 Public Domain

Zoom, the videoconferencing service that has exploded into the vacuum created by the COVID-19 outbreak, has endured the revelation of a string of privacy and security flaws in recent days. Now researchers have

identified just such a flaw in a feature marketed specifically as a way to make meetings more secure.

Zoom said Wednesday it had fixed a vulnerability with its Waiting Room feature.

The feature allows meeting hosts to keep would-be participants in a digital queue pending approval. Medical professionals could use it to host multiple telehealth appointments in a row, and hiring managers could conduct stacked video interviews, the company suggested in a February blog post.

As users have encountered problems with "zoombombing"—whereby participants interrupt and derail meetings, often by using offensive imagery or racist slurs—the company has pointed to the waiting room feature as a way to protect from this type of intrusion.

But security researchers examining the desktop client for vulnerabilities found that Zoom servers would automatically send a live video data to users in the meeting's waiting room, even if they had not yet been approved to join by the person holding the meeting. These users were also sent the meeting's decryption key—the code needed to unlock secure communications. Users could hypothetically extract the video live stream, researchers said.

"If you were moderately technically sophisticated, you could watch what was going on while in the waiting room," said Bill Marczak, a fellow at the Citizen Lab and a postdoctoral researcher at UC Berkeley who found the vulnerability. An audio stream of the call, however, was not accessible.

Marczak said he and John Scott-Railton of the Citizen Lab notified Zoom last week. They detailed their findings in a report published

Wednesday, after they receive an email from the company saying the issue had been fixed.

On Wednesday, Zoom Chief Executive Eric Yuan mentioned during a webinar held to address privacy concerns that Zoom had fixed an issue with its waiting room feature.

"We updated our server. Our waiting room vulnerability is already fixed," Yuan said on the webinar. "From a server side, we did not send audio and video data to the waiting room client. However, we did send the session key ... . We did not think that was safe, so we changed our server."

Yuan's comment did not align with what Marczak and Scott-Railton found, they wrote. The video stream was previously accessible, though the issue has since been fixed, Marczak said.

Zoom did not immediately respond to a request for comment about this discrepancy.

©2020 Los Angeles Times
Distributed by Tribune Content Agency, LLC.