

Silent Mac update nukes dangerous webserver installed by Zoom



reader comments

79 with 47 posters participating

Share this story

Apple said it has pushed a silent macOS update that removes the undocumented webserver that was installed by the Zoom conferencing app for Mac.

The webserver accepts connections from any device connected to the same local network, a security researcher disclosed on Monday. The server continues to run even when a Mac user uninstalls Zoom. The researcher showed how the webserver can

be abused by people on the same network to force Macs to reinstall the conferencing app. Zoom issued an emergency patch on Tuesday in response to blistering criticism from security researchers and end users.

Apple on Wednesday issued an update of its own, a company representative speaking on background told Ars. The update ensures the webserver is removed—even if users have uninstalled Zoom or haven't installed Tuesday's update. Apple delivered the silent update automatically, meaning there was no notification or action required of end users. The update was first reported by TechCrunch.

Apple's update causes Zoom users who click on a conference link to receive a prompt requiring them to confirm they want to join. Previously, clicking on a link—or even encountering a link hidden in a malicious website—automatically opened Zoom and put them into the conference. Zoom developers came under criticism for this behavior as well, because it had the potential to catch users off-guard and expose them to hackers.

Apple occasionally issues silent updates to block malware that's actively circulating on the Internet. It's less common for the company to issue silent updates that block or remove something installed by an app users installed by choice. The Apple representative said company took this action to protect users against risks posed by the webserver. The Zoom app is installed on about 4 million Macs, researcher Jonathan Leitschuh estimated.

Representatives from Zoom didn't respond to an email seeking comment for this post.

<https://arstechnica.com/?p=1534287>