# Zoom boosts security features, encryption amid coronavirus crisis video conferencing boom

24 April 2020, by Mike Snider, Usa Today

Credit: CC0 Public Domain

Zoom is fine-tuning its video conferencing software and upgrading security features to help prevent zoom-bombing and other privacy intrusions.

The San Jose, California-headquartered online video provider said Wednesday that it will make available a new 5.0 version of its software later this week. In addition to improved security features, Zoom will use more advanced encryption that will better protect meeting data and prevent tampering with online meetings.

Earlier this month, Zoom CEO Eric Yuan said the company would spent the next 90 days tightening the platform's security to help prevent instances of video conferences being interrupted by "zoom-bombing" incidents.

Some of the most notorious cases involve educational classes and local government meetings being disrupted with images of pornography and racist symbols including swastikas. On Tuesday, an online Holocaust Remembrance Day event conducted by the Israeli embassy in Germany was disrupted with pictures of Adolf Hitler and the shouting of anti-Semitic and pro-Palestinian slogans, the Israeli newspaper Haaretz reported.

The new version of Zoom will make it harder for meetings to be zoom-bombed with passwords and waiting rooms, which require passwords and a host to admit an attendee, being default settings. For educational users, screen sharing will default to the host only. An improved Security feature will be accessible from an icon on the host's interface and will include a "Report a User" option that notifies Zoom of intruders.

Longer passwords and PIN numbers (for those calling in by phone) can also be created.

""I am proud to reach this step in our 90-day plan, but this is just the beginning," Yuan said. "We will earn our customers' trust and deliver them happiness with our unwavering focus on providing the most secure platform."

By the end of May, Zoom plans for its entire platform to use tougher encryption, AES 256-bit GCM encryption, which Zoom says "offers increased protection of your meeting data in transit and resistance against tampering." The standard can take effect once all Zoom accounts are updated, the company says.

The move can help combat potential attacks from hackers. Zoom has already released fixes for several issues brought to its attention including flaws that could be exploited to hijack a user's Mac computer and access the webcam and microphone.

"From our network to our feature set to our user

experience, everything is being put through rigorous scrutiny," said Zoom chief product officer Oded Gal.

As people have stayed at home during the coronavirus pandemic, more have begun using Zoom to connect via video and audio chats for work and to catch up with family and friends. Zoom has seen usage "balloon," Yuan said recently, as the nation has shut down since March.

Zoom now has about 300 million daily meeting participants, the company says. That's up from last month, when it surpassed more than 200 million daily meeting participants on its free and paid versions, compared to a high in 2019 of 10 million.

Zoom's upgrades "represent a renewed commitment to helping users safeguard confidentiality" and should make most users feel more secure, said Jonathan Knudsen, senior security strategist for cybersecurity company Synopsys, headquartered in Mountain View, California. "For the most part, you can configure a reasonable degree of confidentiality by using a meeting password, monitoring participants, locking meetings after they start, and managing recordings carefully."

But Zoom's departure from what is commonly considered "end-to-end encryption," should continue to raise concerns for government users and for private industries that are potential targets for espionage, Knudsen says. In most cases, end-to-end security means information is encrypted at one end before it is sent over the network and is then decrypted at the other end.

But Zoom encrypts information, then it is decrypted "and encrypted again as it passes through Zoom's meeting infrastructure," he said. "This means that a compromise of parts of Zoom's infrastructure could give an attacker access to plaintext Zoom meeting content."

Even though Zoom 5.0 is strengthening its encryption standard, "this still does not change the fundamental architecture of Zoom, which does not fully implement end-to-end encryption," Knudsen said.

True end-to-end encryption is in the works, Zoom says. But currently, if a meeting is not being recorded and all of the participants are using Zoom software, the content is not decrypted at any point, the company says.