Facing silly naming mistakes, 15,000 Zoom video conversations were exposed on the open web

This issue once again warns about the privacy and privacy settings of the Zoom app, especially as it becomes more and more popular.

According to a new report from The Washington Post, thousands of videos of Zoom meetings are being made public on the open web - allowing anyone to view them. These video calls include business talks, friends' conversations, telemedicine sessions, etc.These thousands of videos have been publicly uploaded due to Zoom's silly mistake.

Not only are they saved on Amazon's non-secure S3 cloud, these videos are also named by default in an identical way. Based on that, Washington Post security researcher Patrick Jackson was able to find 15,000 different videos with a simple search engine. However, the Washington Post does not disclose the default name Zoom uses for these videos.

To make matters worse, thousands of them were even uploaded to video sharing sites like YouTube and Vimeo - meaning everyone could watch them.

However, it is worth noting that these videos are uploaded due to a certain negligence from the user. These videos are usually saved in the user's computer, and seem to be accidentally uploaded onto the internet. Only paid users of Zoom can save videos on the company's cloud server, and the videos are not exposed like the clips above.

Even so, zooming names video so similarly that they are easily found on non-secure cloud platforms is a design flaw that is hard to ignore.

The Washington Post told Zoom about the issue, but it's not clear if this will change the way video titles are uploaded or whether they will be uploaded to Amazon's secure cloud services.

In a statement, Zoom said, " *Zoom will notify meeting participants when the meeting organizer chooses to record the meeting, and provide a safe, secure method for the organizer. video conference. The meeting on Zoom is only recorded at the organizer's choice, either on the organizer's computer or on Zoom's cloud* . "

" *If later, the meeting organizer chose to upload the videos anywhere, we advised them to be very careful and transparent with the meeting participants, carefully considering whether Does the meeting contain sensitive information and the reasonable expectations of the meeting participants* . "

While growing strongly due to everyone's need to work remotely, Zoom is experiencing a series of issues regarding its privacy and security capabilities. Just yesterday, Zoom had to fix issues related to malware that installed unauthorized software on MacOS, patched a flaw in the software, and suspected of revealing the user's LinkedIn profile. .

Zoom's security and privacy issues are so bad that the company has pledged to spend the next 90 days focusing on fixing these issues, instead of adding or developing new features.