Zoom bolsters security offering with the inclusion of post-quantum end-to-end encryption in Zoom Workplace

May 21, 2024

Post-quantum E2EE now available for Zoom Meetings, making Zoom the first UCaaS provider to offer the new security feature

SAN JOSE, Calif., May 21, 2024 (GLOBE NEWSWIRE) -- Today, Zoom Video Communications, Inc. (NASDAQ: ZM) announced that post-quantum end-to-end encryption (E2EE) is now globally available for Zoom Workplace, specifically Zoom Meetings, with Zoom Phone and Zoom Rooms coming soon. The launch of the new security enhancement makes Zoom the first UCaaS company to offer a post-quantum E2EE solution for video conferencing.

As adversarial threats become more sophisticated, so does the need to safeguard user data. In certain circumstances, attackers may have the ability to capture encrypted network traffic now, with the intent to decrypt it later when quantum computers become more advanced — a scenario often referred to as “harvest now, decrypt later”. So, while powerful quantum computers with this capability are not yet generally available, Zoom has taken a proactive stance by upgrading the algorithms designed to be able to withstand these potential future threats.

“Since we launched end-to-end encryption for Zoom Meetings in 2020 and Zoom Phone in 2022, we have seen customers increasingly use the feature, which demonstrates how important it is for us to offer our customers a secure platform that meets their unique needs,” said Michael Adams, chief information security officer at Zoom. "With the launch of post-quantum E2EE, we are doubling down on security and providing leading-edge features for users to help protect their data. At Zoom, we continuously adapt as the security threat landscape evolves, with the goal of keeping our users protected.”

How post-quantum E2E encryption works
When users enable E2EE for their meetings, Zoom’s system is designed to provide only the participants with access to the encryption keys that are used to encrypt the meeting; this is the behavior for both post-quantum E2EE and standard E2EE. Because Zoom’s servers do not have the necessary decryption key, encrypted data relayed through Zoom’s servers is indecipherable. In addition, to defend against “harvest now, decrypt later” attacks, Zoom’s post-quantum E2E encryption uses Kyber 768, an algorithm being standardized by the National Institute of Standards and Technology (NIST) as the Module Lattice-based Key Encapsulation Mechanism, or ML-KEM, in FIPS 203.

Visit our support article to understand which versions and platforms of Zoom Workplace support using post-quantum E2EE.

About Zoom
Zoom’s mission is to provide one platform that delivers limitless human connection. Zoom Workplace — our AI-powered, open collaboration platform built for modern work — streamlines communications, improves productivity, increases employee engagement, optimizes in-person time, and offers customer choice with third-party apps and integrations. Zoom Workplace, powered by Zoom AI Companion, includes collaboration solutions like meetings, team chat, phone, scheduler, whiteboard, spaces, Workvivo, and more. Together with Zoom Workplace, Zoom’s Business Services for sales, marketing, and customer care teams, including Zoom Contact Center, strengthen customer relationships throughout the customer lifecycle. Founded in 2011, Zoom is publicly traded (NASDAQ:ZM) and headquartered in San Jose, California. Get more info at zoom.com.

Zoom Public Relations
Bridget Moriarty
press@zoom.us

Source: Zoom Video Communications, Inc.