Cifrado de Zoom

Introducción

El objetivo de este documento es aportar información sobre los métodos de cifrado utilizados en la plataforma de Zoom. El objetivo del diseño de nuestro cifrado consiste en proporcionar el mayor nivel posible de privacidad a la hora de satisfacer las diversas necesidades de nuestra base de clientes.

Existen distintos casos de uso y maneras posibles de conexión a Zoom por parte del usuario. En el siguiente documento se describen los métodos de cifrado que utilizan con la plataforma las posibles interfaces.

Al utilizar el cliente de Zoom

Zoom ofrece un paquete de software de cliente con numerosas características para Mac, Windows, iOS, Android y Linux, y que hace uso de distintos tipos de tecnologías para ayudar con la privacidad y la seguridad del usuario. **Todos los datos del cliente que se transmiten a la nube de Zoom se cifran en tránsito mediante uno de los siguientes métodos.**

TLS 1.2

Para las conexiones entre el cliente de Zoom y la nube de Zoom, HTTPS es el método de comunicación de preferencia. Estas conexiones utilizan cifrado TLS 1.2 y certificados PKI emitidos por una autoridad de certificación comercial de confianza. Algunos de los casos de uso ordinario incluyen el inicio de sesión en el cliente, la programación de una reunión, el chat, las encuestas, el intercambio de archivos y las preguntas y respuestas durante la reunión. TLS 1.2 también actúa como protocolo de seguridad para otras transmisiones de comunicación, como el contenido en tiempo real de las reuniones.

AES

Para casos de uso como el contenido en tiempo real de las reuniones (vídeo, voz y contenido compartido), en que los datos se transmiten a través del protocolo de datagramas de usuario (UDP), usamos AES-256 en modo ECB para cifrar estas transmisiones de datos comprimidos. Tenemos previsto actualizarlo en breve a AES-256 GCM. Además, para vídeo, voz e intercambio de contenidos cifrados con AES, una vez cifrados, permanecen así mientras atraviesan los servidores de reuniones de Zoom hasta que llegan a otro cliente de Zoom o a un conector de Zoom, que ayuda a traducir los datos a otro protocolo.

SRTP

Nuestro producto Zoom Phone utiliza un protocolo de transporte seguro en tiempo real que utiliza AES-128 ECB para cifrar y proteger las conversaciones telefónicas en tránsito con destino y origen en nuestros centros de datos. Esta función se actualizará en breve a AES-256 GCM.

Al utilizar el navegador web

Zoom ofrece una interfaz web con varias características interesantes que incluyen una completa consola de gestión, acceso a grabaciones en la nube, un amplio conjunto de puntos de conexión de API y un cliente para reuniones basado en web. **Todos los datos del cliente transmitidos desde un navegador web a la nube de Zoom, incluidos los de nuestro sitio web y a través de nuestro cliente de reuniones web, se cifran en tránsito con uno de los siguientes métodos.**

TLS 1.2

Las conexiones al sitio web de Zoom utilizan cifrado TLS 1.2 y certificados PKI emitidos por una autoridad de certificación comercial de confianza. A través de este portal, los usuarios pueden acceder a una serie de características asociadas a su cuenta de Zoom, gestionar sus operaciones e integrar otros sistemas. La potencia del cifrado y los tipos de cifrado específicos que se utilizan para las conexiones con el sitio web dependerán del navegador con el que se acceda al sitio y de los resultados del método de cifrado común negociado.

AES-256

Más allá del cifrado TLS, el sitio web de Zoom utiliza cifrado adicional en casos de uso específicos. Por ejemplo, los datos de los clientes, incluidos las grabaciones en la nube, el historial de chat y los metadatos de reuniones, se almacenan en reposo mediante AES-256 GCM con claves gestionadas por un sistema de gestión de claves (KMS) en la nube. Cuando los usuarios se conecten a una reunión a través del cliente web de Zoom, aprovechando el sistema instalado en web, Zoom enviará y recibirá el contenido en tiempo real de la reunión (vídeo, voz y contenido compartido) a través del protocolo de datagramas de usuario (UDP), directamente desde el servidor de reuniones cifrado con AES-256 ECB.

Al utilizar un dispositivo/servicio de terceros

Al tratarse de una plataforma abierta, Zoom ofrece métodos para que se conecten con nuestro sistema diversos servicios y dispositivos. Se incluye soporte para casos de uso como la conexión de un dispositivo H323/SIP a una reunión de Zoom, la transmisión a través de conocidos servicios de streaming y la llamada a una reunión a través una línea fija estándar (es decir, no a través de nuestra aplicación). Como estas integraciones deben usar los protocolos de comunicaciones nativos del dispositivo o servidor específico de terceros, los métodos de cifrado se limitarán a lo que se permita en dicho dispositivo. **Por tanto, aunque fomentamos el uso de la codificación con dispositivos y servicios de terceros, los datos de los clientes transmitidos a través de estos dispositivos y servicios no se pueden codificar en tránsito con destino y origen en el sistema de Zoom. Sin embargo, una vez que los datos lleguen al sistema de Zoom, se cifran en ese punto y permanecen cifrados mientras estén en tránsito por nuestro sistema.** Si un dispositivo de terceros admite el cifrado, es probable que se efectúe mediante uno de los siguientes métodos.

TLS 1.2

Si es compatible con el dispositivo, Zoom negociará sobre TLS 1.2. Por ejemplo, si un dispositivo SIP ha habilitado el cifrado, se utilizará TLS para la señalización.

AES

Si es compatible con el dispositivo, Zoom negociará el cifrado del contenido de la reunión, como vídeo, audio y pantalla compartida, mediante AES en un punto de conexión SIP o H323.

Conclusión

En el mundo actual, en el cual la colaboración se lleva a cabo a través de varios medios y plataformas de comunicaciones, Zoom se compromete a proteger a nuestros clientes. Cuando entren a formar parte de la ecuación dispositivos de terceros, ofrecemos la posibilidad de extender el cifrado a una amplia gama de integraciones fuera de nuestra plataforma. Dentro nuestra plataforma, nos aseguramos de que el contenido de los clientes esté cifrado.