Criptografia Zoom

Introdução

O objetivo deste documento é informar sobre os métodos de criptografia usados na plataforma Zoom. O objetivo do nosso design de criptografia é fornecer a máxima privacidade possível, além de oferecer suporte às diversas necessidades da nossa base de clientes.

Existem vários casos de uso diferentes e maneiras pelas quais uma pessoa pode se conectar à Zoom. No documento a seguir, descrevemos os métodos de criptografia usados por possíveis interfaces com a plataforma.

Ao utilizar o Cliente Zoom

A Zoom oferece um pacote de software de cliente com recursos completos para Mac, Windows, iOS, Android e Linux, que utiliza uma variedade de tecnologias de criptografia para ajudar na privacidade e segurança do usuário. **Todos os dados do cliente transmitidos para a nuvem Zoom são criptografados em trânsito usando um dos métodos a seguir.**

TLS 1.2

Para conexões entre o Cliente Zoom e a nuvem Zoom, o HTTPS é o método preferido de comunicação. Essas conexões são protegidas pela criptografia TLS 1.2 e pelos certificados PKI emitidos por uma autoridade de certificação comercial confiável. Alguns dos casos de uso comuns incluem efetuar login no cliente, agendar uma reunião, participar de chats, criar enquetes, compartilhar arquivos e participar de perguntas e respostas na reunião. O TLS 1.2 também serve como um protocolo de backup para outros fluxos de comunicação, como o conteúdo em tempo real da reunião.

AES

Para casos de uso, como o conteúdo em tempo real da reunião (compartilhamento de vídeo, voz e conteúdo), em que os dados são transmitidos pelo Protocolo de Datagrama do Usuário (UDP), usamos o AES-256 no modo ECB para criptografar esses fluxos de dados compactados. Atualizaremos em breve para o AES-256 GCM em breve. Além disso, para compartilhamento de vídeo, voz e conteúdo criptografado com o AES, os dados permanecem criptografados à medida que passam pelos servidores de reunião da Zoom até chegar a outro Cliente Zoom ou a um Conector Zoom, que ajuda a convertê-los em outro protocolo.

SRTP

Nosso produto Zoom Phone usa o Protocolo de Transporte Seguro em Tempo Real (SRTP) e o AES-128-ECB para criptografar e proteger conversas telefônicas em trânsito de e para nossos data centers. Essa funcionalidade será atualizada para o AES-256 GCM em breve.

Ao utilizar um navegador Web

A Zoom oferece uma interface Web que fornece vários recursos avançados, incluindo um console de gerenciamento completo, acesso a gravações em nuvem, um amplo conjunto de pontos de extremidade de API e um cliente baseado na Web para reuniões. **Todos os dados do cliente transmitidos de um navegador Web para a nuvem Zoom, inclusive em nosso site e por meio do nosso cliente de reunião via Web, são criptografados em trânsito usando um dos métodos a seguir.**

TLS 1.2

Todas as conexões com o site da Zoom são protegidas pela criptografia TLS 1.2 e pelos certificados PKI emitidos por uma autoridade de certificação comercial confiável. Por meio desse portal, os usuários podem acessar vários recursos associados à sua conta Zoom, gerenciar suas operações e fazer a integração com outros sistemas. A força da criptografia e as cifras específicas usadas nas conexões com o site dependerão do navegador usado para acessá-lo e dos resultados do método de criptografia comum negociado.

AES-256

Além da criptografia TLS, o site da Zoom utiliza criptografia adicional em casos de uso específicos. Por exemplo, os dados do cliente, incluindo gravações em nuvem, histórico de chat e metadados da reunião, são armazenados em repouso usando o AES-256 GCM com chaves gerenciadas por um sistema de gerenciamento de chaves (KMS) na nuvem. Quando os usuários ingressam em uma reunião usando o Cliente Web Zoom com WebAssembly, a Zoom envia e recebe conteúdo em tempo real da reunião (compartilhamento de vídeo, voz e conteúdo) pelo Protocolo de Datagrama do Usuário (UDP), diretamente do servidor de reunião criptografado com AES-256-ECB.

Ao utilizar um dispositivo ou serviço de terceiro

Como uma plataforma aberta, a Zoom oferece métodos para que uma variedade de serviços e dispositivos se conectem ao nosso sistema. Isso inclui suporte para casos de uso, como um dispositivo H323/SIP que se conecta a uma reunião da Zoom, faz transmissões por meio de serviços populares de streaming e ingressa em uma reunião com uma linha telefônica padrão e não pelo nosso aplicativo. Essas integrações devem aprimorar os protocolos de comunicação nativos para o dispositivo ou servidor específico de terceiros, de forma que os métodos de criptografia serão limitados às possibilidades desse dispositivo. **Portanto, embora incentivemos o uso de criptografia com dispositivos e serviços de terceiros, os dados do cliente transmitidos por esses dispositivos e serviços não podem ser criptografados em trânsito de e para o sistema da Zoom. Independentemente disso, ao chegar ao sistema da Zoom, esses dados são e permanecem criptografados o tempo todo em que estão em trânsito.** Se um dispositivo de terceiro oferecer suporte à criptografia, os dados provavelmente serão criptografados usando um dos métodos a seguir.

TLS 1.2

Se suportado pelo dispositivo, a Zoom usará o TLS 1.2. Por exemplo, se um dispositivo SIP usar criptografia, o TLS será utilizado para sinalização.

AES

Se suportado pelo dispositivo, a Zoom utilizará a criptografia do conteúdo da reunião, como o compartilhamento de vídeo, áudio e tela, usando o AES em um ponto de extremidade SIP ou H323.

Conclusão

No mundo atual, em que a colaboração ocorre em várias mídias e plataformas de comunicação, a Zoom está comprometida em proteger nossos clientes. No que diz respeito a dispositivos de terceiros, oferecemos a capacidade de estender a criptografia para uma ampla variedade de integrações fora da nossa plataforma. Entendemos que é nosso dever garantir que o conteúdo do cliente seja criptografado dentro da nossa plataforma.