Le chiffrement Zoom

Introduction

L'objectif de ce document est de fournir des informations sur les méthodes de chiffrement utilisées pour la plateforme Zoom. Notre solution de chiffrement a pour objectif d'offrir le maximum de confidentialité tout en répondant aux divers besoins de notre clientèle.

Outre les différents scénarios d'utilisation, il existe, pour tout un chacun, plusieurs façons possibles de se connecter à Zoom. Le document suivant présente les différentes méthodes de chiffrement utilisées, selon les interfaces vers la plateforme.

Lors de l'utilisation du Client Zoom

Zoom offre un logiciel client riche en fonctionnalités pour Mac, Windows, iOS, Android et Linux qui exploite une gamme de technologies de chiffrement visant à favoriser la confidentialité et la sécurité des utilisateurs. **Toutes les données transmises par le client vers le cloud Zoom sont chiffrées via l'une des méthodes suivantes.**

TLS 1.2

Pour les connexions entre le client Zoom et le cloud de Zoom, HTTPS est la méthode de communication privilégiée. Ces connexions exploitent le protocole de chiffrement TLS 1.2 et des certificats délivrés par une autorité de certification commerciale agréée.
La connexion au client, la programmation d'une réunion, le chat, l'organisation/participation à un sondage, le partage de fichiers et les Q. et R. en réunion constituent les scénarios d'utilisation les plus fréquents. TLS 1.2 sert également de protocole de sauvegarde pour les autres flux de communication tels que le contenu de réunion en temps réel.

AES

Pour les applications telles que le contenu de réunion en temps réel (vidéo, voix et partage de contenu), où les données sont transmises avec le protocole User Datagram Protocol (UDP, en français « protocole de datagramme utilisateur »), nous utilisons l'algorithme AES-256 avec le mode ECB pour chiffrer ces flux de données compressés. Nous devrions bientôt faire une mise à niveau vers l'algorithme AES-256 avec mode de chiffrement GSM. De plus, à partir du moment où ils sont chiffrés AES, la vidéo, la voix, et le partage de contenu restent chiffrés même lorsqu'ils transitent par les serveurs des réunions Zoom, et jusqu'au client Zoom ou connecteur Zoom qui, quant à eux, aident à la conversion des données vers un autre protocole.

SRTP

Notre produit Zoom Phone utilise le protocole Secure Real-time Transport qui tire parti, quant à lui, de l'algorithme AES-128 BCE pour chiffrer et protéger les conversations téléphoniques en transfert vers et depuis nos centres de données. Cette fonctionnalité fera bientôt l'objet d'une mise à niveau vers AES-256 GSM.

Lors de l'utilisation d'un navigateur Web

Zoom offre une interface Web dotée de puissantes fonctionnalités, notamment une console d'administration complète, l'accès aux enregistrements sur le cloud, un nombre important de points de terminaison d'API et un client basé sur le Web pour les réunions. **Toutes les données transmises depuis le navigateur Web vers le cloud Zoom - y compris les données sur notre site Web et via notre client de réunion sur le Web - sont chiffrées via l'utilisation de l'une des méthodes suivantes.**

TLS 1.2

Les connexions vers le site Web de Zoom exploitent le protocole de chiffrement TLS 1.2 et des certificats délivrés par une autorité de certification commerciale agréée. Via ce portail, les utilisateurs peuvent accéder à la gamme de fonctionnalités associées à leur compte Zoom, gérer leurs opérations et s'intégrer à d'autres systèmes. La force du chiffrement et des chiffres de cryptologie utilisés spécifiquement dans le cadre des connexions vers le site Web dépendent du navigateur utilisé pour accéder au site et des résultats de la méthode de chiffrement standard négociée.

AES-256

Au-delà du chiffrement TLS, le site Web de Zoom exploite d'autres méthodes de chiffrement, lors de scénarios d'utilisation spécifiques. Par exemple, les données des clients, notamment les enregistrements sur le cloud, l'historique des chats, et les métadonnées de réunion, sont stockées avec chiffrement au repos AES-256 GSM ; les clés de chiffrement étant gérées par un système de gestion des clés (KMS) sur le cloud. Lorsque les utilisateurs se connectent à une réunion à l'aide du client Web Zoom, tirant parti du standard WebAssembly, Zoom envoie et reçoit le contenu de réunion en temps réel (vidéo, voix et partage de contenu) via le protocole User Datagram Protocol (UDP) directement depuis le serveur de réunion chiffré avec AES-256 ECB.

Lors de l'utilisation d'un service/appareil tiers

En tant que plateforme ouverte, Zoom offre plusieurs méthodes de connexion à son système, à destination de divers types de services et d'appareils. Parmi les scénarios d'utilisation, citons la prise en charge d'un appareil SIP/H323 connecté à une réunion Zoom, par exemple, la diffusion sur les services de streaming les plus répandus, et l'accès à une réunion par l'intermédiaire d'une ligne téléphonique standard (c.-à-d. pas via notre application). Étant donné que ces intégrations doivent tirer parti des protocoles de communication natifs au serveur ou à l'appareil tiers, les méthodes de chiffrement sont limitées aux possibilités inhérentes de l'appareil en question. **Par conséquent, tandis que nous encourageons l'utilisation du chiffrement avec des services et des appareils, les données clients transmises via ses services et appareils sont susceptibles de ne pas être chiffrées lors du transfert vers et depuis le système Zoom. Peu importe, ceci dit : à partir du moment où elles atteignent le système Zoom, les données sont chiffrées au niveau de ce point et le restent pendant tout le temps qu'elles transitent dans notre système.** S'il prend en charge le chiffrement, l'appareil tiers sera probablement chiffré via l'une des méthodes suivantes.

TLS 1.2

Si l'appareil est compatible avec le protocole TLS 1.2, Zoom négocie les données avec ce dernier. Par exemple, si le chiffrement est activé sur un appareil SIP, le protocole TLS est utilisé dans le cadre du signal.

AES

Si l'appareil est compatible, Zoom négocie le chiffrement du contenu de réunion tel que la vidéo, l'audio et le partage l'écran en utilisant le protocole AES sur un point de terminaison SIP ou H323.

Conclusion

Dans le monde d'aujourd'hui où collaboration rime avec plusieurs supports et plateformes de communication différents, Zoom s'engage à protéger ses clients. Lorsqu'un appareil tiers entre en scène, nous offrons à nos clients la possibilité d'étendre le chiffrement à un large éventail d'intégrations en dehors de notre plateforme. Au sein de notre plateforme, nous garantissons le chiffrement du contenu de nos clients.