Zoom 암호화

개요

본 문서는 Zoom 플랫폼의 암호화 방법에 대한 정보를 제공하기 위해 작성되었습니다. 당사 암호화 설계의 목표는 고객의 다양한 요구를 지원하는 동시에 개인 정보를 최대한 보호하는 것입니다.

사용자가 줌에 연결하는 방법에는 여러 활용 사례와 잠재적인 방법이 있습니다. 다음에서는 잠재적 인터페이스가 플랫폼에 사용하는 암호화 방법을 간략하게 소개합니다.

Zoom 클라이언트를 사용하는 경우

Zoom은 다양한 암호화 기술을 사용하여 사용자의 개인정보보호 및 보안을 지원하기 위해 맥, 윈도우, iOS, 안드로이드 및 리눅스를 위한 다양한 기능의 클라이언트 소프트웨어 패키지를 제공합니다. **클라이언트에서 Zoom 클라우드로 전송되는 모든 고객 데이터는 다음 방법 중 하나를 사용하여 전송 중 암호화됩니다.**

TLS 1.2

Zoom 클라이언트와 Zoom 클라우드를 연결하기 위해서 선호하는 통신 방법은 HTTPS입니다. 이 연결에는 TLS 1.2 암호화 및 신뢰할 수 있는 상업용 인증 기관에서 발급한 PKI 인증서를 활용합니다. 일반적 사용 사례는 클라이언트로 로그인, 회의 일정잡기, 채팅, 투표, 파일 공유 및 회의 중 Q&A 를 포함합니다. TLS 1.2는 또한 실시간 콘텐츠 회의와 같은 다른 통신 스트림을 위한 백업 프로토콜 역할도 담당합니다.

고급 암호화 표준

비디오, 오디오 및 공유 콘텐츠와 같은 실시간 콘텐츠 회의 같은 경우 사용자 데이터그램 프로토콜(UDP)을 통해 데이터가 전송되며 Zoom은 ECB 모드에서 AES-256을 사용하여 압축 데이터 스트림을 암호화합니다. 당사는 빠른 시일 내에 이를 AES-256 GCM으로 업그레이드 할 예정입니다. 또한 AES로 암호화된 비디오, 오디오 및 공유 콘텐츠의 경우 일단 암호화가 된 후에는 다른 Zoom 클라이언트 또는 Zoom 커넥터에 도달할 때까지는 Zoom 미팅 서버를 통화할 때 암호화 상태를 유지하기 때문에 데이터를 다른 프로토콜로 변환할 수 있습니다.

실시간 전송 프로토콜(SRTP)

Zoom 전화 제품은 AES-128-ECB를 활용한 실시간 전송 프로토콜(SRTP)을 사용하여 데이터 센터에 전송중 이거나 주고받는 통화 내용을 암호화하고 보호합니다. 이 기능은 빠른 시일 내에 AES-256 GCM로 업그레이드 예정입니다.

웹 브라우저를 사용하는 경우

Zoom은 다양한 기능을 가진 웹 인터페이스를 제공합니다. 이 기능은 완벽한 관리 콘솔, 클라우드 기록에의 접근, 광범위한 API 엔드포인트 세트 및 회의를 위한 웹 기반 클라이언트를 포함합니다. **웹 브라우저에서 웹 사이트 및 웹 미팅 클라이언트를 포함하여 Zoom Cloud로 전송되는 모든 고객 정보는 아래의 방법 중 하나를 사용하여 전송 중 암호화됩니다.**

TLS 1.2

Zoom 웹사이트로의 연결에는 TLS 1.2 암호화 및 신뢰할 수 있는 상업용 인증 기관에서 발급한 PKI 인증서를 활용합니다. 이 포털을 통해 사용자는 본인 Zoom 계정과 관련된 여러 기능에 접근, 작동을 관리하며 다른 시스템과 통합할 수도 있습니다. 웹사이트 연결에 사용하는 특정 암호 및 암호화의 강도는 사이트 접속에 사용하는 브라우저 및 일반적인 암호화 방법 선택 결과에 따라 달라집니다.

AES-256

TLS 암호화 이외에도 Zoom 웹사이트는 특정 사용 사례에 대해 추가적인 암호화 방법을 활용합니다. 예를 들어 클라우드 기록, 채팅 히스토리 및 회의 메타데이터를 포함한 고객 데이터는 클라우드의 키 관리 시스템(KMS)이 관리하는 키와 AES-256 GCM을 사용하여 휴면 상태로 저장됩니다. 사용자가 웹 어셈블리를 활용한 Zoom 웹 클라이언트로 회의에 접속한 경우, Zoom은 비디오, 오디오 및 공유 콘텐츠와 같은 실시간 콘텐츠를 사용자 데이터그램 프로토콜(UDP)을 통해 AES-256 ECB로 암호화된 미팅 서버에서 직접 주고받습니다.

제 3자 기기/서비스를 사용하는 경우

개방형 플랫폼인 Zoom은 다양한 종류의 서비스와 기기가 당사의 시스템에 접속할 수 있는 방법을 제공합니다. 이 방법은 H323/SIP 기기를 통한 Zoom 회의 연결, 인기 스트리밍 서비스를 사용한 방송 및 당사 앱을 사용하지 않고 일반 전화선을 이용한 회의 접속과 같은 사용 사례 지원을 포함합니다. 이러한 통합은 특정 제 3자 기기 또는 서버와의 통신 프로토콜을 활용해야 하기 때문에 해당 기기에서 사용 가능한 암호화 방법으로 암호화 방법이 제한됩니다. **따라서 제 3자 기기 및 서비스에 암호화 사용을 장려하지만 이러한 기기와 서비스를 통해 전송되는 고객 데이터는 Zoom 시스템으로 전송, 송출되는 과정 중 암호화가 되지 않을 수 있음을 염두에 둬야 합니다. 그럼에도 불구하고 데이터가 일단 Zoom 시스템에 도착하면 그 시점에 바로 암호화되고 Zoom 시스템을 통과하는 내내 암호화 상태를 유지합니다.** 제 3자 기기가 암호화를 지원하는 경우 아래의 방법 중 하나를 사용하여 암호화 됩니다.

TLS 1.2

기기가 이 방식을 지원하는 경우 Zoom은 TLS 1.2를 사용한 암호화를 진행합니다. 예를 들어 SIP 기기에서 암호화가 활성화되어 있다면 TLS를 사용해 신호를 만들어냅니다.

고급 암호화 표준

기기가 이 방식을 지원하는 경우 Zoom은 비디오, 오디오 및 화면 공유와 같은 미팅 콘텐츠를 SIP 또는 H323 엔드포인트의 AES를 사용하여 암호화를 진행합니다.

결론

다양한 매체 및 통신 플랫폼을 통해 협업이 이루어지는 현실 세계에서 Zoom은 고객 보호를 위해 심혈을 기울이고 있습니다. 제 3자 기기가 개입될 경우 Zoom은 당사 플랫폼 외부에서도 다양한 종류의 통합에 암호화를 확장할 수 있는 기능을 제공합니다. Zoom 플랫폼 안에서는 고객의 콘텐츠가 안전하게 암호화될 수 있도록 최선을 다하고 있습니다.