Departamento de Segurança da Informação – **DSI** *dsic.planalto.gov.br/*
Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo – **CTIR Gov** *www.ctir.gov.br/*

Utilização do Software Zoom

1. Descrição do Problema

Data de Publicação: 09/04/2020
Data de Atualização: 09/04/2020

Devido à situação global da disseminação do Coronavírus (COVID-19), a plataforma Zoom, serviço que combina recursos de videoconferência, reuniões online, bate-papo e colaboração móvel, tem ganhado popularidade entre pessoas de todo o mundo. Sua utilização vem sendo feita especialmente para web conferências, permitindo que seus usuários permaneçam trabalhando de suas casas, indo ao encontro do que vem sendo recomendado pela Organização Mundial da Saúde e das autoridades locais de saúde da maioria dos países.

Análises realizadas pelo Citizen Lab, da Universidade de Toronto, no Canadá, identificaram que o protocolo de criptografia utilizado para proteger as videoconferências é o Transport Layer Security (TLS). Desta forma, a conexão entre cliente e servidor é protegida, porém, cabe ressalvar, entretanto, que sem a adoção de criptografia de ponta a ponta para as videoconferências, a própria infraestrutura do serviço tem, em última análise, a capacidade técnica de acessar o conteúdo de áudio e vídeo e áudio não criptografados, podendo inclusive gravar os vídeos, o que pode ser uma grave falha de segurança.

Para além disso, os pesquisadores identificaram que o algoritmo de criptografia utilizado é o Padrão Avançado de Criptografia - AES (do inglês Advanced Encryption Standard), com chaves de tamanho de 128 bits, utilizando o modo de operação ECB (Electronic CodeBook). O ECB, por ser de baixa difusão, é um modo simples de criptografia, sendo, portanto, desaconselhado seu uso para operações sensíveis.

2. Sistemas afetados

A análise investigou o software Zoom instalado como cliente nos seguintes sistemas operacionais: Windows, MacOS e Linux.

3. Impacto

O estudo identificou, ainda, a possibilidade de que a chave de criptografia seja transmitida para outro usuário, não necessariamente participante da web conferência. De posse desta chave, um usuário externo, com conhecimento suficiente, poderá acessar em claro os conteúdos de áudio e vídeo transmitidos em uma dada sessão.

4. Recomendações

Não é recomendado o uso do Software Zoom para videoconferências que contenham, em suas pautas, assuntos sensíveis ou os que constam nos casos do item 5.2 da Norma Complementar nº 14/IN01/DSIC/GSIPR, até que uma versão atualizada seja lançada e faça a correção dessas vulnerabilidades.

5. Referências

- The Citizen Lab: A Quick Look at the Confidentiality of Zoom Meetings. Disponível em: <https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/>.
- Advanced Modes in AES: Are they Safe from Power Analysis based Side Channel Attacks? Disponível em: <https://ieeexplore.ieee.org/document/6974678>.
- Zoom Video Communications, Inc. Disponível em: <https://zoom.us/>.

Equipe do CTIR Gov – *ctir@ctir.gov.br*