Recomendação de Segurança 001/2020 - Cogetic

Em 8 de abril de 2020

Para: Gestores de TI das unidades da Fiocruz

Assunto: Vulnerabilidades no aplicativo Zoom

Prezados Gestores de TI,

Recentemente foram descobertas e amplamente divulgadas na mídia quatro vulnerabilidades da ferramenta Zoom consideradas altamente críticas.

Principais vulnerabilidades

a) CVE-2020-11500

Data do registro: 03/04/2020

Descrição: O cliente de conferência Zoom na versão 4.6.9 usa o modo ECB da criptografia AES para áudio e vídeo. Dentro de uma reunião, todos os participantes usam uma chave simples de 128-bit.

Referência: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11500

Essa vulnerabilidade foi descoberta pelo SecKC, um grupo de pesquisa em cibersegurança, que desenvolveram a ferramenta denominada zWarDial, que tem a capacidade de testar até 100 IDs de reuniões por hora e 2,4 mil reuniões por dia. A ferramenta tem uma taxa de 14% de descoberta de identificação de conferência remota, correspondendo a 336 salas de reuniões virtuais por dia, sendo capaz de extrair informações como o link da reunião, data e hora de sua realização, o usuário organizador e o conteúdo discutido. Segundo SecKC, o zWarDial é ineficaz para reuniões protegidas por senha.

b) CVE-2020-11469

Data do registro: 01/04/2020

Descrição: O cliente de conferência Zoom na versão 4.6.8 do iOS copia um *script bash* chamado *runwithroot* para um diretório temporário gravável do usuário durante a instalação, que permite uma

execução local com o privilégio do usuário para obter acesso de *root* por meio da realocação do runwithroot.

Referência: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11469

Essa vulnerabilidade foi descoberta pelo pesquisador Patrick Wardle, ex-hacker da NSA. E permite que o Zoom se auto instale no iOS, sem intervenção do usuário. Sabendo-se disso, um invasor pode injetar um malware no instalador do aplicativo para ganhar acesso ao root do sistema, efetivamente obtendo controle do computador.

c) CVE-2020-11470

Data do registro: 01/04/2020

Descrição: O cliente de conferência Zoom na versão 4.6.8 do iOS tem o direito ao disable-library-validation, que permite uma execução local com o privilégio do usuário para obter acesso não solicitado a uma câmera e microfone, por meio do carregamento de uma biblioteca e deste modo herdar o acesso da câmera e do microfone no cliente Zoom.

Referência: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11470

Patrick Wardle descobriu essa vulnerabilidade, assim como a anterior. E permite que o malware herde as permissões de câmera e microfone do iOS. Assim, caso tenha consentido acesso aos dispositivos de captura do computador, o invasor também terá acesso a esses mesmos dispositivos, sem que a autorização do usuário.

d) UNC path injection

A vulnerabilidade de UNC *path injection* afeta computadores Windows, e consiste em usar caminhos remotos UNC para converter URLs recebidos por meio do chat. Atacantes sabendo desse comportamento, aproveitam para incluir links que infectam o computador do usuário.

e) Vazamento de vídeos desprotegidos

Patrick Jackson, diretor da empresa Disconnect, especializada em software de privacidade, relatou ter encontrado cerca de 15 mil vídeos no serviço de armazenamento da Amazon, sem proteção por senha. Os vídeos continham vídeo-chamadas de sessões de terapia, treinamentos, reuniões de

pequenas empresas e aulas do ensino fundamental, de cunho íntimo e pessoal, ou corporativo e sensível. Ainda não está claro se este caso se refere a uma vulnerabilidade do Zoom, ou falha humana dos usuários da ferramenta.

Além das vulnerabilidades acima, há ainda relatos de vazamento de milhares de e-mails de usuários, coleta e transmissão de dados para fins de publicidade, transmissões que foram invadidas e passaram a exibir pornografia e outros vídeos indevidos (zoombombing).

Posicionamento das empresas usuárias

Algumas empresas estão procurando usar ferramentas similares para conferência remota, tal como: Microsoft Teams, Google Hangouts e Cisco Webex. Empresas de segurança como a Kaspersky e Trend Micro se restringiram a conceder orientações de uso aos usuários do Zoom.

O Departamento de Educação da cidade de Nova York recomendou aos diretores das escolas que deixassem de usar o Zoom e sugeriu o uso do Microsoft Teams como uma alternativa adequada, em parte porque é compatível com a FERPA (Lei de Privacidade e Direitos Educacionais da Família).

No Brasil, a Agência Nacional de Vigilância Sanitária – ANVISA, bloqueou o uso da ferramenta Zoom, enquanto Elon Musk – fundador da SpaceX e Tesla Motors, recomendou a seus funcionários que evitem seu uso. O Ministério da Justiça e Segurança Pública, por meio da Secretaria Nacional do Consumidor (Senacon), abriu investigação contra o aplicativo Zoom. A empresa foi notificada, na segunda-feira (6), pelo Departamento de Proteção e Defesa do Consumidor (DPDC) para esclarecer dúvidas sobre o compartilhamento de dados de usuários do aplicativo com o Facebook, especialmente no que se refere à versão para o sistema iOS.

Posicionamento da Zoom Video Communications sobre as vulnerabilidades

Segundo a empresa Zoom, a ferramenta passou de 10 milhões para 200 milhões de usuários diários em março, início do isolamento social ao redor do mundo. Ao longo dos próximos dias, o Zoom diz que estar interrompendo temporariamente o desenvolvimento de novos recursos, e focando na resolução de falhas de segurança: “Nos próximos 90 dias, estamos comprometidos em dedicar os recursos necessários para melhor identificar, abordar e corrigir problemas de forma

proativa. Também estamos comprometidos em ser transparentes durante todo esse processo. Queremos fazer o que for necessário para manter sua confiança."

O fundador do Zoom, Eric Yuan, reconhece que não ter atingido as expectativas de privacidade e segurança da comunidade e da própria empresa, e disse: "Aprendemos nossas lições e recuamos um passo para focar na privacidade e segurança".

No dia 01 de abril de 2020, a Zoom publicou em seu blog ter resolvido as vulnerabilidades CVE-2020-11469, CVE-2020-11470 e UNC path injection, além de oferecer treinamento e tutoriais para melhorar uso da ferramenta. Com relação ao vazamento de vídeos, Yuan disse: "O Zoom notifica os participantes quando um anfitrião grava uma reunião e oferece uma forma segura para que eles guardem essas gravações. As reuniões do Zoom são gravadas apenas a pedido do anfitrião e gravadas localmente na máquina do anfitrião ou na nuvem do Zoom." E completa que o anfitrião escolher enviar as gravações para outro lugar posteriormente, sendo cuidadosos com os dados e transparentes com os outros participantes. Ainda é aguardado uma solução com relação à vulnerabilidade CVE-2020-11500.

Recomendações de segurança (medidas para mitigação)

Apesar do Zoom ter solucionando alguns problemas e estar atuando na resolução de outros, alguns cuidados são importantes para garantir sua utilização adequada e segura:

a) Todos os participantes devem dar preferência ao cliente web. Para quem precisa usar o aplicativo, devem usar instalador disponibilizado no site oficial do Zoom e garantir que estão com a última versão instalada.
b) O anfitrião deve configurar opções de segurança no momento de agendar uma reunião, por exemplo:
   - Incorporar senha no link da reunião;
   - Usar um Personal Meeting ID (PMI) aleatório;
   - Enviar links de convite diretamente ao participante, pessoa a pessoa;
   - Definir uma senha para a sala; e
   - Ativar o recurso de "sala de espera";
c) Antes do início da reunião, o anfitrião deve considerar as seguintes situações:

- — Mutar todos os participantes (desativando o microfone assim que entrarem e impedindo que liberem o próprio microfone automaticamente);
- — Desativar salvamento automático do chat;
- — Desativar transferência de arquivos;
- — Desativar compartilhamento de tela para não-anfitriões;
- — Desativar controle remoto;
- — Desabilitar anotações; e
- — Desabilitar recurso de "entrar antes que o anfitrião";

d) O anfitrião deve considerar designar pelo menos mais um co-anfitrião, para:
- — Ajudar no controle da sala virtual;
- — Conferir participantes, excluindo estranhos; e
- — Trancar a sala assim que todos entrarem;

e) O apresentador deve compartilhar apenas a tela essencial para a apresentação, com o recurso de "*Portion of Screen*";

f) Todos os participantes devem proteger sua câmera fisicamente, com *post-its* ou bloqueadores próprios para câmeras, liberando somente quando necessário; e

g) Todos os participantes devem redobrar o cuidado com links e arquivos compartilhados.

Vale ainda ressaltar que a Fiocruz disponibiliza outras ferramentas para conferência, entre eles o Microsoft Teams e serviço de web conferência da RNP.

Referências:

— https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

— https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/

— http://portal.anvisa.gov.br/noticias/-/asset_publisher/FXrpx9qY7FbU/content/solucao-zoom-bloqueada-na-anvisa/219201

— https://www.reuters.com/article/us-spacex-zoom-video-commn/elon-musks-spacex-bans-zoom-over-privacy-concerns-memo-idUSKBN21J71H

— https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/

— https://olhardigital.com.br/noticia/milhares-de-gravacoes-de-videoconferencias-do-zoom-sao-expostas-online/99024

— https://www.kaspersky.com/blog/zoom-security-ten-tips/34729/

— https://blog.trendmicro.com/using-zoom-heres-how-to-keep-your-business-and-employees-safe/

— https://canaltech.com.br/hacker/zoom-pode-ser-varrido-por-software-que-captura-ate-100-ids-de-reunioes-por-hora-162858/

— https://macmagazine.uol.com.br/post/2020/04/01/especialista-descobre-mais-falhas-no-zoom-para-macos-possibilitando-acesso-indevido-a-camera-e-ao-microfone/

— https://blog.wesecure.pt/nova-vulnerabilidade-no-zoom-pode-levar-a-roubo-de-credenciais

— https://www.techtudo.com.br/listas/2020/04/zoom-e-seguro-veja-dicas-para-usar-o-programa-de-videoconferencia.ghtml

— https://medium.com/@future4/abril-2020-como-se-proteger-das-vulnerabilidades-do-zoom-aa77ecee841c

— https://www.laptopmag.com/articles/block-windows-10-programs-connecting-to-internet

— https://www.cyberscoop.com/zoom-fbi-teleconference-hijacking/

— https://www.novo.justica.gov.br/news/ministerio-da-justica-e-seguranca-publica-notifica-o-aplicativo-zoom

Coordenação de Gestão de Tecnologia da Informação
Segurança da Informação e Comunicações