Le 9 avril 2020

RÉSUMÉ

Le présent courriel vise à vous faire part des problèmes de sécurité et des vulnérabilités qui sont activement exploités dans le logiciel de vidéoconférence Zoom.

Il est vivement recommandé aux organisations utilisant ou ayant utilisé le logiciel Zoom d'installer la plus récente version prise en charge et les plus récents correctifs et de suivre les pratiques exemplaires et les recommandations additionnelles énoncées dans le présent avis.

EN QUOI CET INCIDENT TOUCHE-T-IL MON ORGANISATION?

Les mesures de distanciation sociale mises en place afin de gérer la pandémie se sont traduites par une augmentation du nombre d'employés faisant du télétravail. Ce changement s'accompagne d'une utilisation accrue des outils de conférence en ligne tels que Zoom, qui permet à des équipes de collaborer et de se réunir à distance. Zoom est l'un des outils de conférence en ligne conviviaux dont la base utilisateur a connu une forte augmentation au cours des dernières semaines (hausse de 535 % du trafic quotidien au cours du dernier mois).

En raison de sa popularité et de sa large utilisation, Zoom est ciblé par des auteurs malveillants qui exploitent activement des séances mal configurées et non sécurisées. On offre des recommandations visant à atténuer ces risques et on recommande fortement aux utilisateurs de Zoom de les suivre.

QUE DEVRAIS-JE FAIRE?

Transmettez, dès que possible, cet avis au personnel responsable de la cybersécurité ou aux partenaires de TI afin qu'ils prennent des mesures immédiates.

DÉTAILS TECHNIQUES

Zoom a fait la manchette en raison des préoccupations liées à la protection des renseignements personnels et à la sécurité, notamment des comptes rendus de réunions Zoom interrompus par des utilisateurs non autorisés qui utilisent une technique appelée « Zoombombing », au moyen de laquelle les auteurs malveillants accèdent à des réunions Zoom sans mot de passe, les piratent et affichent du contenu inapproprié.

Le « Zoombombing » est rendu possible parce que les utilisateurs n'appliquent pas les mesures de sécurité disponibles pour leurs réunions, comme les mots de passe, et parce que les utilisateurs publient les codes de réunions et les renseignements relatifs à l'accès sur les médias sociaux. De plus, Zoom utilise les identifiants de réunion qui peuvent être énumérés au moyen d'outils disponibles en ligne, ce qui fait en sorte qu'il devient facile pour des auteurs malveillants d'accéder à des réunions Zoom qui ne sont pas protégées par un mot de passe.

Il y a aussi des préoccupations concernant une vulnérabilité grave et récemment corrigée qui peut entraîner une fuite des authentifiants Windows Active Directory, une brèche dans la protection des renseignements personnels avec le paramètre « Company Directory »

(Répertoire de l'entreprise), l'envoi de données d'analyse par Zoom à Facebook, la force du chiffrement de Zoom et le fait que Zoom manque de chiffrement de bout en bout.

Zoom comporte des plans payants offrant des fonctionnalités additionnelles. Il convient de noter que les versions payantes de Zoom (Pro Business et Entreprise) permettent d'enregistrer des conférences Zoom à partir de l'application Zoom elle-même. Les versions « Pro Business et Enterprise » de Zoom permettent également d'héberger toutes vos données de conférence sur votre propre serveur privé, contrairement à un serveur détenu et exploité par Zoom. Cette dernière option garantirait que Zoom ne serait pas en mesurer d'accéder à votre contenu.

MESURE RECOMMANDÉE

- Installer la dernière version de Zoom prise en charge.
- Envisager de ne pas utiliser Zoom pour organiser des réunions qui devraient comporter des renseignements sensibles. Si vous devez absolument utiliser Zoom pour tenir des conférences comportant des renseignements sensibles, envisagez d'utiliser les versions « Pro Business ou Enterprise » de Zoom pour profiter de la fonctionnalité vous permettant d'héberger des données de conférence sur votre propre serveur.
- Ajouter un mot de passe robuste à TOUTES les réunions et utiliser la fonction « Salle d'attente ».
- S'assurer que les utilisateurs ne publient pas les identifiants ou les mots de passe de la réunion sur les médias sociaux.
- Envisager de configurer le logiciel Zoom de sorte que seul l'hôte de la réunion puisse partager son écran.
- Verrouiller la réunion une fois que tous les participants s'y sont joints.
- Être conscient des messages d'hameçonnage imitant des invitations à des réunions Zoom.
- Être conscient que des participants à la conférence peuvent possiblement enregistrer des vidéoconférences et des audioconférences.
- Appliquer les fonctions de sécurité du logiciel de téléconférence et s'assurer qu'elles sont configurées correctement.

Guide de la NIST visant à empêcher l'écoute illicite et à protéger les renseignements personnels lors de la tenue de réunions virtuelles : https://www.nist.gov/blogs/cybersecurity-insights/preventing-eavesdropping-and-protecting-privacy-virtual-meetings (en anglais seulement)

Guide de Zoom sur les mots de passe des réunions et des webinaires : https://support.zoom.us/hc/en-us/articles/360033559832-Meeting-and-Webinar-Passwords- (en anglais seulement)

Mise en garde du FBI : https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic/layout_view(en anglais seulement)

POUR DE PLUS AMPLES RENSEIGNEMENTS

La Division de la cybersécurité organise chaque mois une téléconférence de la communauté de pratique pour l'ensemble de la fonction publique afin de discuter de sujets et d'enjeux liés à la cybersécurité. La téléconférence est ouverte à toute organisation de l'ensemble de la fonction publique qui souhaite y participer. Envoyez un courriel à cyeradvice@ontario.ca pour demander l'ajout de votre nom à la liste d'invitation. **On a augmenté la fréquence de ces téléconférences. Par conséquent, elles auront lieu une fois par semaine au lieu d'une fois par mois pour la durée de la pandémie et seront axées sur la COVID-19 et les problèmes liés à la cybersécurité.**

Si vous constatez des indicateurs de compromission (IC) sur vos réseaux, ou avez des renseignements connexes ou des questions, veuillez communiquer votre message à l'adresse cyberadvice@ontario.ca.

AUCUNE GARANTIE

Le présent avis de cybersécurité contient du contenu et des liens d'un tiers. La communauté de pratique sur la cybersécurité ne contrôle pas les liens ni ne les tient à jour, ne déclare pas ni ne garantit que le lien fonctionnera encore lorsque vous cliquerez dessus ou si le service ou le contenu est utile, approprié, à l'abri des virus ou fiable. Il vous incombe de déterminer si vous voulez suivre un lien ou accepter de recevoir un service ou un contenu qui vous est offert ou de vous y fier.

La communauté de pratique sur la cybersécurité fournit de l'information sur une menace connue qui pourra être utilisée à l'entière discrétion des bénéficiaires afin de se protéger contre les cybermenaces. Le présent avis est communiqué afin d'aider les organisations de l'ensemble de la fonction publique à se préparer à faire face à des cybermenaces et à faire preuve de résilience.

DÉFINITIONS

Les menaces ou les incidents de cybersécurité sont des événements qui présentent un risque à la sécurité (p. ex. confidentialité, disponibilité ou intégrité) des ressources d'information, des systèmes et des réseaux d'une organisation.

- L'avis de MENACE à la cybersécurité est communiqué lorsqu'AUCUNE EXPLOITATION ACTIVE n'est observée. But de l'avis : permettre aux organisations de se préparer à faire face à des cybermenaces et de les atténuer.
- L'avis d'INCIDENT de cybersécurité est communiqué lorsqu'une EXPLOITATION ACTIVE est observée. L'avis d'incident doit être communiqué rapidement afin d'informer des organisations partenaires de l'incident de cybersécurité en cours et de favoriser une intervention et une prise de mesures correctrices en temps opportun.