Université de Montréal | Technologies de l'information

Centre de services

DATE : Le 16 juillet 2019

DESTINATAIRES : Responsables TI des unités
Utilisateurs de postes Mac

OBJET : **Avis de sécurité**
Failles majeures de sécurité dans l'application de vidéoconférence *Zoom* (version 4.4.2 et antérieures) sur postes MacOS

Portée de l'avis de sécurité

- *Type d'avis* : Failles majeures dans l'application de vidéoconférence client Zoom, version 4.4.2 et antérieures.
- *Type d'équipements affectés* : Tout ordinateur ou système Mac OS X utilisant l'application de vidéoconférence *Zoom*.
- *Systèmes d'exploitation affectés* : Tout système d'exploitation Mac OS X utilisant l'application de vidéoconférence *Zoom*.

Chers membres,

Les Technologies de l'information souhaitent informer les responsables informatiques et les utilisateurs de postes Mac qui utilisent l'application de vidéoconférence *Zoom* (version 4.4.2 et antérieures) qu'un avis de sécurité a été publié.

Plusieurs failles majeures de sécurité ont été découvertes dans cette application :

- Un attaquant distant pourrait induire un utilisateur Mac à accéder à un site web malicieux et ce dernier pourrait lancer un « chat » vidéo *Zoom* sur le client Mac, sans la permission de son propriétaire.

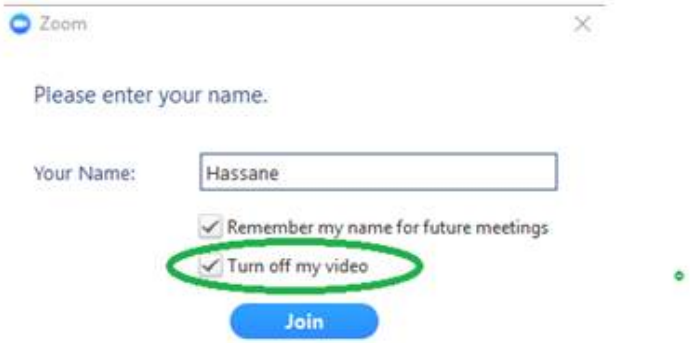
- Lors de l'installation de ce logiciel sur un poste Mac, un serveur web local est installé, permettant à l'application d'initier des conversations. Par conséquent, ceci permettrait à n'importe quel utilisateur malveillant de lancer la caméra et de voir ce qui se passe sur le poste, donc d'espionner son utilisateur. À noter que même en cas de désinstallation de l'application Zoom, le serveur web local demeure actif sur le poste Mac, permettant à tout moment de réinstaller l'application sans l'accord de l'utilisateur.

- Un attaquant pourrait potentiellement viser un utilisateur d'un client Mac en lui envoyant des requêtes de visioconférence sans fin, causant un déni de service et en rendant éventuellement le poste inutilisable.

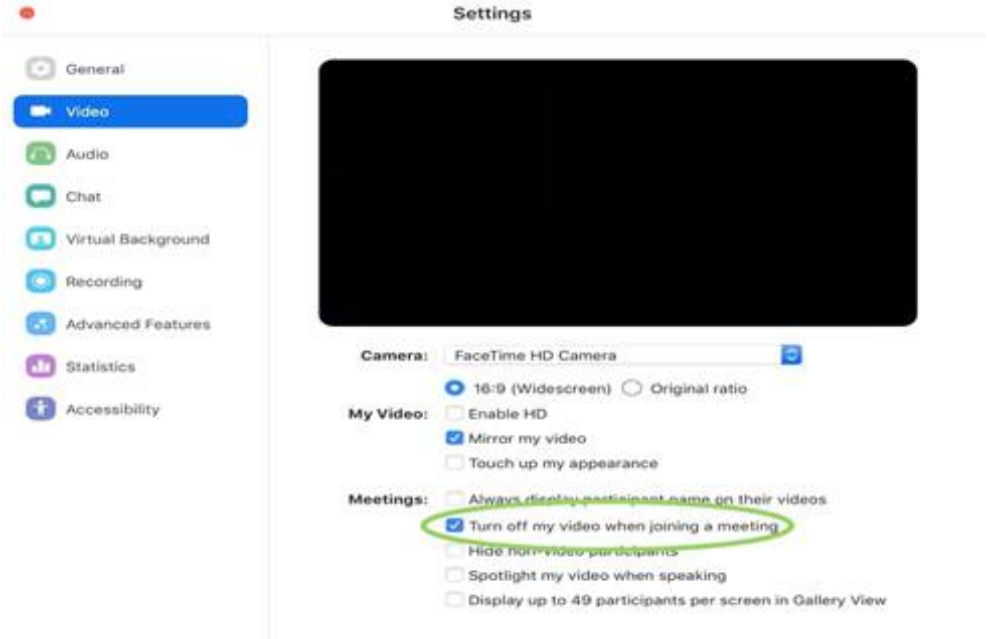
Pour remédier à cette situation, veuillez :

1. *Mettre à jour la version de l'application Zoom*
   Pour le téléchargement d'une version corrigée de l'application *Zoom*, veuillez consulter le lien suivant :
   https://zoom.us/download?zcid=1231&_ga=2.146474486.354117011.1562771211-630912407.1557165814

2. *Désactiver la vidéo*
   - S'il s'agit de la première fois que vous vous joignez à une vidéoconférence via l'application *Zoom*, cocher la case « *Turn off my Vidéo* ».



   - Si l'application *Zoom* a déjà été utilisée sur le poste, cocher la case « *Turn off my video when joining a meeting* » dans les préférences du client MacOS de *Zoom*. À noter que vous devrez activer la webcam, dans un deuxième temps, après avoir rejoint une vidéoconférence.



Pour plus d'information concernant ces vulnérabilités critiques, veuillez consulter les liens suivants :

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13449
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13450
- https://www.macg.co/logiciels/2019/07/le-client-macos-de-zoom-peut-activer-la-webcam-de-votre-mac-sans-votre-accord-106963
- https://iphonesoft.fr/2019/07/09/zoom-faille-permet-activation-camera-macos
- https://blog.zoom.us/wordpress/2019/07/08/response-to-video-on-concern/
- https://assets.zoom.us/docs/pdf/Zoom+Response+Video-On+Vulnerability.pdf

Pour toutes questions d'ordre technique, veuillez communiquer avec l'équipe *Sécurité* des Technologies de l'information, par courriel à l'adresse « securite@umontreal.ca ».

Pour rester informé des actualités concernant la sécurité informatique (alertes, vulnérabilités, failles, recommandations), veuillez vous abonner au blog de la Sécurité des Technologies de l'information.

Dans l'éventualité où vous avez reçu ce message et que vous n'êtes pas le responsable informatique de votre unité, veuillez SVP le transmettre à votre responsable technique ou administratif.

Les Technologies de l'information vous remercient de votre collaboration.