Université de Montréal | Technologies de l'information
Centre de services

DATE : **Le 13 décembre 2017**

DESTINATAIRE : **Communauté UdeM**

OBJET : **Vulnérabilité MacOS High Sierra 10.13**

Chers membres,

En septembre dernier, les Technologies de l'information mettaient en garde les utilisateurs d'ordinateurs *Apple* à l'endroit de la mise à niveau MacOS High Sierra 10.13. Malgré la mise en garde, il y a des utilisateurs qui ont installé la version de MacOs High Sierra 10.13 sur leurs postes.

Nous tenons à informer ces utilisateurs qu'une faille de sécurité affectait le système d'exploitation MacOS High Sierra 10.13. Cette vulnérabilité permet de se connecter au compte administrateur (« root ») d'un ordinateur opérant ce système d'exploitation. Un utilisateur malicieux, ayant un accès physique à l'ordinateur vulnérable, peut obtenir toutes les informations contenues dans l'ordinateur, exécuter du code de son choix, modifier les réglages et installer un logiciel (possiblement malicieux) à l'insu de l'utilisateur. La faille peut aussi être exploitée à distance, par la fonction d'écran partagé.

La compagnie *Apple* a publié une mise à jour de sécurité qui corrige cette vulnérabilité. Les Technologies de l'information demandent aux utilisateurs de postes fonctionnant déjà sous le système d'exploitation MacOS High Sierra 10.13 d'installer cette mise à jour : https://support.apple.com/fr-ca/HT208315.

Il est important de noter que le correctif désactive le compte d'administration sur le poste. Si ce compte est requis, il faut le réactiver et changer le mot de passe suite à l'application du correctif. Des instructions pour réactiver le compte d'administration sont disponibles à l'URL suivant : https://support.apple.com/fr-fr/HT204012. De plus, suite à l'application du correctif, la compagnie *Apple* avise que les partages de fichiers peuvent être affectés. Pour y remédier, les utilisateurs sont invités à consulter l'URL suivant : https://support.apple.com/fr-ca/HT208317. Enfin, pour éviter une exploitation du poste à distance par un autre compte, il est recommandé de désactiver la fonction d'écran partagé.

Nous tenons également à vous informer que la version de l'antivirus McAfee présente dans la logithèque est maintenant fonctionnelle et compatible avec cette version de MacOS. Vous pouvez dès maintenant procéder à la mise à niveau MacOs High Sierra 10.13 et au téléchargement de la dernière version de l'antivirus McAfee.

Pour plus d'informations au sujet de cette faille de sécurité, veuillez consulter le lien suivant : https://www.macg.co/os-x/2017/11/macos-high-sierra-la-root-est-ouverte-tous-une-solution-100551.

Pour toutes questions concernant ce message, veuillez communiquer avec le Centre de services des Technologies de l'information au 514-343-7288 ou par le formulaire d'aide.

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