Une faille de sécurité de Mac OS ouvre l'accès admin à tous

Par Steven J. Vaughan-Nichols | Mercredi 29 Novembre 2017 www.zdnet.fr

La dernière version de macOS, High Sierra, offre un moyen simple et infaillible de prendre le contrôle de n'importe quel Mac. Apple vient de pousser un patch.

Apple n'aura pas tardé à combler cette très embarrassante faille. Le géant vient en effet de pousser un correctif (Security Update 2017-001) qui ferme cette porte grande ouverte. Le correctif qui concerne les utilisateurs de macOS High Sierra 10.13.1 mais pas ceux de 10.12.6 est à installer de toute urgence...

Apple, Apple, Apple. Qu'allons-nous faire de vous ? Dans votre version la plus récente de High Sierra macOS, il s'avère que vous avez donné à un utilisateur local le moyen de prendre possession d'un Mac, et ce totalement.

Allez sur votre Mac sous High Sierra et essayez ceci : sur l'écran de connexion, cochez "Autre utilisateur" et saisissez root comme nom d'utilisateur et laissez le mot de passe vide. Cliquez plusieurs fois et vous pourriez alors découvrir que vous venez de vous connecter à votre système en tant qu'utilisateur root, c'est-à-dire en mode administrateur. Vous avez désormais tous les pouvoirs.

Cela signifie que si vous avez volé un Mac, ou si vous avez simplement accès physiquement à un Mac alors que le propriétaire est absent, vous avez accès à toutes les données qui s'y trouvent. Pensez-vous que ce soit problématique ? Oui, vous pouvez.

C'est un raté historique en matière de sécurité. Rien d'équivalent ne me vient à l'esprit. Tous les Mac exécutant une version à jour de MacOS sont exposés à ce type d'attaques. Cet exploit ne nécessite

aucune des redoutables compétences qu'on pourrait prêter à un hacker fou de la NSA. Si vous pouvez utiliser un clavier, vous pouvez entrer.

Dans la version originale de ce trou de sécurité, tout ce que vous deviez faire était de vous rendre dans les Préférences Système, puis Utilisateurs et Groupes, et de cliquer sur le verrou pour apporter des modifications. Ensuite, entrez "root" comme nom d'utilisateur sans mot de passe. Sésame, ouvre toi ! Vous y êtes.

Comme sur tout système basé sur Unix/Linux, l'utilisateur root peut contrôler toutes les fonctions d'administration et peut lire et écrire sur n'importe quel système de fichiers, y compris ceux des autres utilisateurs. En théorie, la racine est désactivée sur les systèmes Apple sauf autorisation expresse. Faux !
Une fois connecté, vous pouvez modifier vos propres autorisations. Par exemple, vous voulez vous donner des privilèges d'administrateur ? Bien sûr ! Ou, vous pouvez configurer de nouveaux comptes de niveau administrateur. Une fois que vous avez fait cela, vous pouvez faire tout ce que vous désirez dans le système.

Le développeur turc Lemi Orhan Ergin a découvert cette variation de la faille et a annoncé l'erreur de sécurité remarquablement stupide d'Apple sur Twitter.
De nombreux autres et moi avons vérifié. Nous avons constaté que le trou est aussi béant qu'il le paraît. Le problème a été confirmé sur macOS High Sierra 10.13.0, 10.13.1 (la version actuelle de High Sierra) et macOS High Sierra 10.13.2 beta.

Il est d'abord apparu qu'il n'était pas possible d'exploiter cette astuce triviale à distance. Depuis lors, Will Dormann, un analyste en vulnérabilités du CERT/CC, a rapporté : « Si vous avez exposé le 'partage d'écran', vous pouvez autoriser les utilisateurs à accéder à votre machine avec un accès complet à l'interface graphique sans utiliser de mot de passe ». En outre, Dormann a découvert que "Apple 'Remote Management' est lui aussi exposé. Si 'Contrôle' est activé, cela ouvre un accès distant root complet à un système, sans mot de passe."

Apple a reconnu l'existence du problème. Dans une déclaration, Apple précise que l'ajout d'un mot de passe pour le root permettrait d'y remédier. « Nous travaillons sur une mise à jour logicielle pour résoudre ce problème. En attendant, la définition d'un mot de passe root empêche tout accès non autorisé à votre Mac. Pour activer l'utilisateur racine et définir un mot de passe, suivez les instructions ici. Si un utilisateur root est déjà activé, , veuillez suivre les instructions de la section Changer le mot de passe root pour vous assurer qu'un mot de passe vide n'est pas défini ».

Cela fait quatre problèmes de sécurité liés au mot de passe depuis la sortie de High Sierra en septembre.
Pour le moment, vous devez - impérativement - définir un mot de passe pour le compte root. Vous pouvez le faire avec la commande suivante depuis le terminal :
sudo passwd -u root
Une fois que vous avez défini un mot de passe pour root, l'astuce du mot de passe vide ne fonctionnera plus.