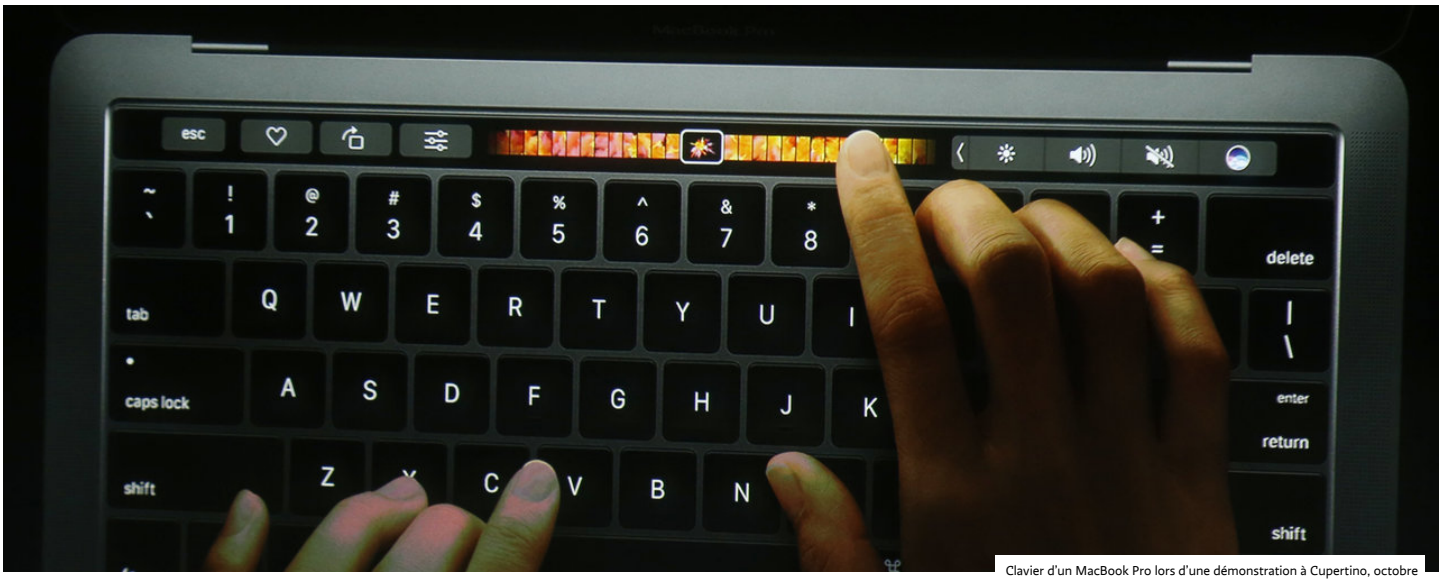
LE TEMPS



Clavier d'un MacBook Pro lors d'une démonstration à Cupertino, octobre 2016.
© Beck Diefenbach

TECHNOLOGIE

Une faille embarrassante pour Apple permet de pirater des Macs

Il est possible d'obtenir les droits complets sur un Mac équipé de la version 10.13.1 de High Sierra... sans aucun mot de passe

3 minutes de lecture

Technologies **sécurité**

Anouch Seydtaghia

Publié mercredi 29 novembre 2017 à 10:44, modifié mercredi 29 novembre 2017 à 11:40.

C'est une aubaine pour les pirates informatiques. Et une nouvelle très embarrassante pour Apple. Mardi soir, un chercheur turc, Lemi Ergin a publié sur Twitter un petit message de trois phrases montrant comment il est possible d'accéder, sans mot de passe, à un Mac. Apple, qui n'avait apparemment pas été prévenu assez tôt de cette faille, a immédiatement expliqué qu'un correctif allait être envoyé.

Il n'y a nul besoin d'être un expert en informatique pour exploiter cette faille. Il suffit de lire le tweet de Lemi Ergin: «Cher @AppleSupport, nous avons remarqué un immense problème de sécurité dans MacOS High Sierra. N'importe qui peut s'identifier avec «root» et sans mot de passe en cliquant sur le bouton login plusieurs fois. Etes-vous conscients de cela, @Apple?» demande le chercheur. Immédiatement, des sites spécialisés ont essayé de reproduire cette séquence. Avec succès.

Lemi Orhan Ergin
@lemiorhan

Dear @AppleSupport, we noticed a *HUGE* security issue at MacOS High Sierra. Anyone can login as "root" with empty password after clicking on login button several times. Are you aware of it @Apple?

19:38 - 28 nov. 2017

980 11 054 12 196

Il y a deux conditions. Il faut que le Mac dispose de la version 10.13.1 de High Sierra, et non des variantes précédentes. Il faut aussi que l'ordinateur ait été allumé avec une session ouverte. Ensuite, la machine demande un mot de passe. Ecrire «root» comme login et taper plusieurs fois sur «enter» permet d'accéder immédiatement à toutes les fonctions de l'ordinateur, et ainsi de changer le mot de passe pour en prendre totalement le contrôle. Il est possible d'accéder à tous les documents, d'installer des applications ou encore de désactiver les fonctions de sécurité. Et si le contrôle à distance est activé sur l'ordinateur, une personne peut faire tout cela à distance, note Steven Meyer, de la société de sécurité genevoise ZenData.

Lire aussi: Un incroyable système d'espionnage des internautes mis au jour

Apple a réagi, expliquant «travailler sur une mise à jour logicielle pour régler ce problème. En attendant, créer un mot de passe pour une session «root» permet d'éviter des accès non autorisés à votre Mac». Une marche à suivre a été mise en ligne. On ne sait pas encore quand la mise à jour sera effectuée, mais ce n'est sans doute qu'une question d'heures.

Pas le premier bug

Comme le résume le site spécialisé Techcrunch, «il va sans dire que c'est très, très mauvais. Ne laissez pas votre Mac sans surveillance jusqu'à ce que ce problème soit résolu». De son côté, Bloomberg relevait que «ce pépin est rare et il s'agit d'un échec potentiellement embarrassant pour Apple. Ses logiciels sont généralement connus pour être moins sujet au piratage et aux infections par malware que Windows, développé par Microsoft». «Ce n'est pas le premier bug trouvé dans OSX 10.13, note Steven Meyer. En octobre, il y avait déjà eu un bug qui affichait le mot de passe dans l'«indice de mot de passe» à la place de l'indice... Le problème a été corrigé depuis.»

Apple aurait en parallèle des raisons d'en vouloir au chercheur turc: normalement, lorsqu'une faille est détectée, la découverte est communiquée de manière discrète à l'éditeur du logiciel, qui a ainsi quelques jours pour régler le problème, avant qu'il ne soit communiqué de manière publique. Dans ce cas, Lemi Ergin a averti en même temps Apple et ses clients, ce qui pose des problèmes de sécurité plus importants.

Lire également cette chronique: iOS 11: Apple se moque de ses clients

Anouch Seydtaghia
@Anouch

Journaliste éco/finance, spécialisé dans les nouvelles technologies, intéressé par les voitures autonomes, la cybersécurité et les start-up