Un bug dans le Wi-Fi touche Apple

Un chercheur en sécurité vient de publier un code arbitraire qui serait selon lui : *« capable d'exploiter une nouvelle vulnérabilité découverte dans le logiciel en charge du sans-fil sur les machines de la marque à la pomme. »*

Cette vulnérabilité trouve son origine dans le driver *« Apple AirPort «* , c'est du moins ce qu'affirme HD.Moore, un développeur de l'outil de sécurité Metasploit. Ce bug ne concernerait que les pilotes qui ont été livrés avec des cartes « wireless » vendues sur la période 1999/2003 avec les PowerBooks et les iMacs.

Pour lancer une attaque, le cracker doit se trouver sur le même réseau sans-fil que le Mac vulnérable qu'il cible. L'objectif de l'attaque est de lancer une corruption de la mémoire de la machine en envoyant vers la cible des paquets contenant du code arbitraire.

D'après Moore cette attaque est complexe à mettre en route, d'ailleurs, le chercheur lui-même n'arrive toujours pas à prendre un « contrôle total » sur la machine cible…

Du côté d'Apple, on reconnaît l'existence de la faille tout en minimisant son impact : *« Cette vulnérabilité ne touche que de vieux PC et elle ne va pas être simple à reproduire sur les machines plus récentes, mais cela reste possible. »*

Apple mène actuellement une enquête sur les affirmations de HD.Moore, un porte-parole du groupe a déclaré : *« Ce problème ne concerne qu'un faible pourcentage de nos machines utilisant une version ancienne du driver AirPort et ne touche pas les machines récentes équipées du AirPOrt Extreme driver. »*

La *« preuve de concept »* présentée par Moore a été ajoutée à l'outil de sécurité Metasploit Framework 3.0. Un outil très apprécié des professionnels et des particuliers qui permet de vérifier la santé d'un écosystème « wireless ».