Apple corrige une autre faille SSL dans iOS et Mac OS X

Apple vient de publier des mises à jour pour iOS et Mac OS X. Parmi elles, plusieurs correctifs de sécurité ont été apportés. Ils corrigent notamment **une faille importante concernant le protocole SSL**. Il ne s'agit pas de la vulnérabilité Heartbleed rendue publique le 7 avril dernier, mais d'un autre bug qui offrirait à un attaquant la possibilité de voler des données lors d'une connexion SSL. Apple utilise en effet un protocole dédié, Secure Transport.

La faille concerne OS X Mountain Lion 10.8.5 , OS X 10.9.2 Mavericks , ainsi que iOS 7.1 et les versions antérieures et a été nommée par les expert « Triple Handshake » (triple association). Dotée du nom de code CVE-2014-1295 dans la nomenclature des incidents de sécurité, Apple explique que la vulnérabilité a la capacité de créer deux connexions qui ont les mêmes clés de chiffrement et associations (handshake), d'insérer des données corrompues et ensuite faire une renégociation pour que les connexions interagissent. **Pour contrer ce bug, Apple a modifié Transport Secure** pour que par défaut, lors de la renégociation, les certificats serveurs présentés soit les mêmes que ceux présentés lors de connexion initiale.

Correctif Heartbleed sur les équipements WiFi

La firme de Cupertino avait indiqué la semaine dernière que ses solutions n'étaient pas touchées par la vulnérabilité Heartbleed, en utilisant une version ancienne et non affectée d'OpenSSL. Or, **Apple vient de publier une mise à jour pour ses bornes WiFi, Airport Extreme et Time Capsule qui règle des problèmes liés à SSL/TLS**. Sans donner de précision sur la finalité de la correction, les experts en sécurité estiment que ce correctif porte sur la faille Heartbleed. Apple a confirmé à nos confrères de MacWorld l'information en soulignant que le correctif s'adresse « ***aux dernières générations des stations AirPort Extreme et AirPort Time Capsule (juin 2013)*** ».

En complément :

Faille de sécurité béante sur iPhone
Heartbleed : McAfee met en ligne un outil de test dédié