iPhone : une vulnérabilité menace les utilisateurs

À l'origine, la mise à jour du firmware de l'iPhone (v1.1.1 et précédentes) avait pour but de mettre un terme au déverrouillage « illégal » de l'iPhone permettant d'utiliser le combiné sur tous les opérateurs. Mais cet MAJ contient aussi une vulnérabilité.

Cette faille Tiff a été exploitée par les hackers et permet en théorie de débloquer l'iPhone, mais elle peut également être utilisée de façon malveillante. Concrètement, la lecture d'une image malformée au format Tiff peut provoquer un buffer overflow (débordement tampon) et par conséquent autoriser l'écriture de script et son exécution sur le système.

D'après le célèbre hacker HD Moore, l'exploitation de cette faille Tiff, pourrait également permettre à un pirate d'écouter les discussions de l'utilisateur mais aussi prendre des photos ou bien encore le localiser. Un code permettant d'exploiter la faille est également disponible sur la Toile.

Reste que si le risque est bien réel, la vulnérabilité n'est pas si facile à exploiter, car le pirate doit tout de même persuader l'utilisateur d'ouvrir avec son navigateur Safari l'image malformée.

Selon nos informations, Apple travaille sur la version 1.1.2 du firmware.

« Les propriétaires d'iPhones 'débloqués' sont particulièrement en danger, car l'installation de la dernière version du firmware n'est pas possible pour eux, la faille restera donc présente dans leur navigateur même après qu'Apple ait publié un correctif » a déclaré Franck Chartier, responsable Marketing des Editions Profil.

Une solution pour contrer la faille Tiff

De son côté, l'éditeur de solutions de sécurité BitDefender annonce l'intégration dans ses solutions de sécurité de signatures, d'un outil permettant la détection des fichiers Tiff déformés.