

Apple corrige « le bug RTSP » dans QuickTime

Découverte pour la première fois le 10 janvier 2008 par le chercheur Luigi Auriemma, la faille a été par la suite confirmée par les éditeurs de sécurité.

À l'époque, Auriemma avait publié la POC (proof of concept) faisant ainsi la démonstration d'une attaque.

Pour contaminer sa cible, le hacker devait d'abord obliger un internaute à regarder un fichier vidéo au format QuickTime contenant un morceau de code malveillant.

Le correctif publié hier, mercredi 6 février 2008, corrige la version 7.4.1 de QuickTime et adresse les systèmes Mac OS X et Windows.

Selon Apple, elle corrige le problème qui se posait lorsque QuickTime essayait d'ouvrir une connexion RTSP avec un serveur dont le port 554 était fermé.

Face à ce refus, QuickTime tentait de se connecter vers le port 80 en utilisant donc le protocole HTTP. Seulement, ledit serveur retournait un code d'erreur s'affichant dans la barre d'état de QuickTime. Ce qui pouvait provoquer un buffer overflow (dépassement de la mémoire tampon).

« Le correctif publié par la pomme corrige également un ancien problème, une incompatibilité entre QuickTime 7.4 et Adobe Premiere et Effects », explique en marge de cette publication un porte-parole de Cupertino.

Précisons qu'il s'agit là de la cinquième mise à jour publiée par Apple depuis octobre 2007. Ce sont les chercheurs indépendants et les éditeurs qui mettent la pression sur les éditeurs de lecteurs multimédias afin de réduire les risques de piratage des machines en ligne. Rappelons que Apple est en passe de devenir une cible privilégiée des cybercriminels ([lire notre article](#)), c'est ce que l'on appelle, la rançon de la gloire !