

# Apple corrige encore des bogues dans QuickTime

Pour la seconde fois en deux mois et la quatrième depuis le début de l'année, Apple offre à sa communauté un correctif pour son lecteur multimédia QuickTime.

Selon *ComputerWorld*, « ce patch corrige des vulnérabilités permettant à un attaquant de subtiliser des données personnelles à sa cible. »

Cette mise à jour de sécurité est destinée à la version 7.1.6 de QuickTime. Elle intervient quelques jours après la publication d'un correctif de 17 patches.

Apple corrige notamment deux bogues dans la façon dont le logiciel gère le Java et permet l'exécution de code malveillant.

« QuickTime pour Java présente un problème d'implémentation susceptible d'autoriser l'installation ou la manipulation d'objets hors des limites de la mémoire tampon allouée. En poussant un utilisateur à une page Web contenant une applet Java construite de manière malveillante, un attaquant peut déclencher le problème, qui peut conduire à l'exécution de code quelconque. Cette mise à jour résout le problème en réalisant des validations supplémentaires sur les applets Java », précise Apple

La seconde vulnérabilité que corrige cette publication permet à un voyou de la toile d'accéder à des données stockées dans la mémoire de l'ordinateur cible. Des informations qui sont particulièrement sensibles comme des mots de passe sont donc menacées.

« QuickTime pour Java présente un problème de conception qui autorise la lecture de la mémoire de votre navigateur Web par un applet Java. En poussant un utilisateur à une page Web contenant une applet Java construite de manière malveillante, un attaquant peut déclencher le problème, qui peut conduire à la divulgation d'informations sensibles. Cette mise à jour résout le bogue en effaçant la mémoire avant d'autoriser son utilisation par des applets Java » indique la pomme dans un communiqué.

Le 1er mai 2007, Apple a publié de nouvelles versions de son lecteur pour Mac OS X et Windows afin de corriger une vulnérabilité découverte par un hacker lors de la conférence canadienne CanSecWest.

Rappelons pour l'anecdote que le white hat à l'origine de cette trouvaille a empoché 10.000 dollars.

Peu avant cet événement Apple publiait deux correctifs de sécurité, le 5 mars et le 23 janvier.

Ce correctif qui est téléchargeable sur [le site de Apple](#) est disponible pour les versions Mac et Windows du lecteur. Plus d'informations sur [ce lien](#).