

Apple corrige le bug critique touchant QuickTime

Dès son apparition le problème avait été jugé « critique » par la majorité des éditeurs de sécurité et touchait à la fois PC et Mac.

Les sites communautaires de partage de vidéo, certains utilisent QuickTime, s'étaient également plaints de cette faille. Cette dernière permettait en effet à du code malveillant de s'activer sur des systèmes vulnérables, et par conséquent menaçait de nombreux utilisateurs.

Les chercheurs indépendants qui ont participé au 'mois des bugs' dans les logiciels de la pomme peuvent donc se féliciter. Car si l'initiative est jugée « inacceptable et dangereuse » par l'industrie du soft, les ingénieurs rebelles sortent victorieux.

Dans le détail, ce bug concerne la façon dont Quick Time utilise le RTSP (Real Time Streaming Protocol), le protocole de diffusion en temps réel de la vidéo ou du son.

Profitant de ce problème, un attaquant pouvait -après avoir créé une chaîne de caractères (String) RTSP spéciale dans un fichier Quick Time- provoquer un « Buffer Overflow » ou « dépassement de la mémoire tampon », sur l'ordinateur cible.

LMH, surnom désignant l'un des ingénieurs à l'origine de cette découverte, avait expliqué : « le risque est de se retrouver avec un système compromis par un attaquant distant capable de faire ce qu'il veut sur la machine. Cette intrusion peut-être amorcée à partir de JavaScript, de Flash, de liens classiques, de fichiers QTL (Quick Time Media Link) et de toutes les extensions permettant d'ouvrir Quick Time. »

Apple a publié des correctifs pour les versions : QuickTime 7.1.3 sur Mac OS X v10.3.9, Mac OS X Server v10.3.9, Mac OS X v10.4.8, Mac OS X Server v10.4.8, Windows XP/2000.