Première exploitation de la faille RSTP dans QuickTime

Fin novembre 2007, une alerte concernant une vulnérabilité dans le lecteur multimédia de la pomme Quick Time était signalée par les éditeurs de sécurité, une semaine après cette découverte, les premiers codes permettant d'exploiter ce problème débarquent…

Ladite vulnérabilité résulte d'un débordement de tampon présent au niveau du traitement d'une réponse RTSP avec une en-tête « Content-Type » excessivement longue.

Le problème a été détecté par un chercheur polonais, spécialisé dans la recherche de vulnérabilité, Krystian Kloskowski. Depuis la publication de cette découverte, l'exploit permettant d'utiliser cette faille pour attaquer un poste est dans la nature.

D'après l'éditeur Symantec, plusieurs attaques sont déjà en route, sur son blog il indique suivre le développement de cette affaire, une nouvelle publication de l'éditeur donnant plus de détails notamment sur l'ampleur du phénomène devrait donc suivre…

Rappelons que cette faille concerne les versions les plus récentes de Quick Time, la 7.2 et la 7.3 (les versions précédentes sont également susceptibles d'être touchées par cette vulnérabilité). Selon le FrSirt, elle est rapidement passée du statut de POC (Proof of concept) à celui de code exploitable. Pour l'instant, seules les versions Quick Time pour Windows sont susceptibles d'être touchées.

Symantec explique que ce code utilise l'approche IFRAME. Un code IFRAME permet à un navigateur (ndlr : Internet Explorer, Firefox, Opera et Safari sont faillibles) d'ouvrir une nouvelle fenêtre afin de visiter un site Web, souvent déguisé en site pornographique, qui contient un code malveillant.

Pour l'instant, Symantec indique que les sites utilisés par les cybercriminels téléchargent un fichier baptisé Downloader sur les machines cibles.

Apple n'a toujours pas publié de correctifs pour Quick Time, mais il existe au moins deux façons de se protéger. Les utilisateurs concernés et les administrateurs de réseau peuvent arrêter le support du protocole RSTP par le lecteur (ndlr : Quick Time Control Panel / Preference Panel/ File Types / Advanced -> MIME Settings et décocher l'option stream RSTP dans l'option Streaming Movie Option). Ils peuvent également filtrer les activités sortantes utilisant les ports RSTP et les ports TCP 554 et UDP 6970-6999.

En attendant, la publication d'un correctif, la protection la plus avancée contre une attaque tirant parti de la vulnérabilité QuickTime RTSP, consiste à désactiver la prise en charge du protocole RSTP par le lecteur d'Apple et à bloquer le port TCP 554 et les ports UDP 6970 à 6999.