Quick Time : gros pépin dans le lecteur de la pomme

Ce problème résulte d'un débordement de tampon présent au niveau du traitement d'une réponse RTSP avec une entête « Content-Type » excessivement longue, ce qui pourrait être exploité par des attaquants afin d'exécuter des commandes arbitraires en incitant un utilisateur à visiter une page Web spécialement conçue.

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.

L'information a également été confirmée par l'US-CERT (United States Computer Emergency Readiness Team), le service de sécurité informatique du Département de la Sécurité intérieure des États-Unis. Ce qui illustre la dangerosité de cette faille.

Selon l'US Cert : les utilisateurs concernés et les administrateurs de réseau peuvent arrêter le support du protocole RSTP (ndlr : Quick Time Control Panel / Preference Panel/ File Types / Advanced -> MIME Settings et décocher l'option stream RSTP dans l'option Streaming Movie Option)

À la rédaction de cette actualité, Apple n'avait toujours pas publié de correctifs.

Plus d'informations sont disponibles sur ces deux liens:

– FrSirt

– US Cert