



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité
des systèmes d'information
CERTA

Paris, le 07 février 2008
N° CERTA-2008-ALE-001-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité dans Apple QuickTime

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2008-ALE-001>

Gestion du document

Référence	CERTA-2008-ALE-001-002
Titre	Vulnérabilité dans Apple QuickTime
Date de la première version	11 janvier 2008
Date de la dernière version	07 février 2008
Source(s)	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

Exécution de code arbitraire à distance.

2 Systèmes affectés

Apple QuickTime version 7.3.1.70.

3 Résumé

Une vulnérabilité affectant Apple QuickTime permet à un individu malveillant d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité dans le logiciel multimédia Apple QuickTime permet à une personne malintentionnée l'exécution de code arbitraire à distance via un dépassement de mémoire tampon lors d'une tentative infructueuse de lecture d'un fichier via le protocole *Real Time Streaming Protocol (RTSP)*.

Une fonctionnalité de QuickTime permet de basculer automatiquement du protocole *RTSP* au protocole *HTTP* lorsque le port par défaut *RTSP* n'est pas joignable (554/tcp et 554/udp). Une page d'erreur spécialement conçue pour le protocole *HTTP* permet l'exploitation de cette vulnérabilité. Des codes d'exploitation ont été diffusés sur l'Internet.

Cette vulnérabilité concerne les machines ayant une version QuickTime à jour, et indépendamment du système d'exploitation installé.

5 Contournement provisoire

Parmis les contournements provisoires, on note :

- Vérifier que la prise en charge des liens *RTSP* est désactivée dans QuickTime en décochant la case Édition -> Préférences -> Préférences de QuickTime -> Types de fichiers -> Enchaînement - séquence en temps réel -> Descripteur de flux RTSP;

Cette option, qui n'est pas activée par défaut, ne comble en rien la vulnérabilité mais permet de d'éviter l'ouverture de lien malveillant par QuickTime.

- vérifier la politique de filtrage des flux sortants. QuickTime essaie de se connecter au serveur sur différents ports (rtsp : 554 puis HTTP : 80), mais la politique de filtrage peut influencer ce passage. Ainsi, si les flux sortants vers les ports 554/TCP et 554/UDP sont filtrés et engendrent une absence de réponse dans un intervalle de temps suffisant, QuickTime n'effectue plus la tentative de connexion en HTTP.
- utiliser un lecteur alternatif.

6 Solution

Mise à jour du 07 février 2008 :

Apple a corrigé cette vulnérabilité dans la version 7.4.1 de QuickTime, mentionnée dans l'avis CERTA-2008-AVI-059.

7 Documentation

- Avis du CERTA CERTA-2008-AVI-059 du 07 février 2008 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2008-AVI-059/>
- Note de vulnérabilité de l'US-CERT VU#112179 du 10 janvier 2008 :
<http://www.kb.cert.org/vuls/id/112179>
- Référence CVE CVE-2008-0234 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0234>

Gestion détaillée du document

11 janvier 2008 version initiale.

14 janvier 2008 précisions concernant le filtrage.

07 février 2008 correction apportée par Apple dans la version 7.4.1 de QuickTime.