

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-2007-ALE-001>

Gestion du document

Référence	CERTA-2007-ALE-001
Titre	Vulnérabilité dans Apple Quicktime
Date de la première version	04 janvier 2007
Date de la dernière version	24 janvier 2007
Source(s)	Annnonce du "Month of Apple Bugs" MOAB-01-01-2007
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 ;
- déni de service à distance.

2 Systèmes affectés

Apple Quicktime versions 7.1.3 et antérieures.

3 Résumé

Une vulnérabilité dans Apple Quicktime permet à un utilisateur distant de provoquer un déni de service ou d'exécuter du code arbitraire.

4 Description

Un manque de contrôle sur les liens ou URL de type `rtsp://` permet à un utilisateur distant mal intentionné de provoquer un déni de service ou d'exécuter du code arbitraire dans le contexte de l'utilisateur de l'application QuickTime vulnérable. L'exploitation de la vulnérabilité peut se faire par le biais d'un lien `rtsp://` directement ou bien par le biais d'un fichier `.qt1` construit de façon particulière.

5 Contournement provisoire

5.1 Sous Microsoft Windows :

- Désactiver la prise en charge des liens `rtsp://` dans Quicktime en décochant la case Préférences de Quicktime -> Types de fichiers -> Diffusion -> Descripteur de flux RTSP;
- supprimer l'association de Quicktime avec les fichiers `.qt1` en supprimant la clef de registre : `HKEY_CLASSES_ROOT\.qt1`.

5.2 Sous Apple MacOS X :

- Désactiver la prise en charge des liens `rtsp://` dans QuickTime en décochant la case Préférences de Quicktime -> Avancé -> Réglages MIME -> Diffusion -> Descripteur de flux RTSP;
- ne pas ouvrir les fichiers de type `.qt1` dans la mesure où il n'y a pas de moyen simple d'enlever l'association de ces fichiers avec QuickTime, il convient de ne pas ouvrir les fichiers `.qt1` avec QuickTime.

6 Solution

Appliquer le correctif 2007-001 fourni par Apple le 23 janvier 2007.

7 Documentation

- Annonce du "Month of Apple Bugs" MOAB-01-01-2007 :
<http://projects.info-pull.com/moab/MOAB-01-01-2007.html>
- Référence CVE CAN-2007-0015 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2007-0015>
- Mise à jour de sécurité Apple 2007-001 du 23 janvier 2007 :
<http://docs.info.apple.com/article.html?artnum=304989-fr>

Gestion détaillée du document

04 janvier 2007 version initiale.

24 janvier 2007 ajout de la mise à jour Apple.