

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans 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-2005-AVI-436>

Gestion du document

Référence	CERTA-2005-AVI-436
Titre	Multiples vulnérabilités dans Quicktime
Date de la première version	04 novembre 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple #302772 du 02 novembre 2005
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

- Déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Apple Quicktime 6.x ;
- Apple Quicktime 7.x.

3 Résumé

De nombreuses vulnérabilités découvertes dans l'application Quicktime d'Apple permettent à un utilisateur distant mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire.

4 Description

L'application Quicktime d'Apple est un lecteur multimédia.

- Deux vulnérabilités de type débordement d’entier permettent à un utilisateur distant mal intentionné d’exécuter du code arbitraire au moyen d’un fichier vidéo .mov malicieusement construit ;
- une vulnérabilité dans la gestion de certains attributs d’un fichier video permet à une personne distante de causer un déni de service ;
- une vulnérabilité de type débordement de mémoire dans PictureViewer peut être exploitée au moyen d’un fichier PICT malicieusement constitué afin d’exécuter du code arbitraire à distance.

5 Solution

Mettre à jour Apple Quicktime avec la version 7.0.3, disponible à l’adresse suivante :
<http://www.apple.com/support/downloads/quicktime703.html>

6 Documentation

- Bulletin de sécurité Apple #302772 du 02 novembre 2005 :
<http://docs.info.apple.com/article.html?artnum=302772>
- Apple Quicktime 7.0.3 :
<http://www.apple.com/support/downloads/quicktime703.html>
- Référence CVE CAN-2005-2753 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2753>
- Référence CVE CAN-2005-2754 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2754>
- Référence CVE CAN-2005-2755 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2755>
- Référence CVE CAN-2005-2756 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2756>

Gestion détaillée du document

04 novembre 2005 version initiale.