

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités 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-AVI-301>

---

### Gestion du document

Référence	CERTA-2008-AVI-301
Titre	Multiples vulnérabilités dans Apple QuickTime
Date de la première version	10 juin 2008
Date de la dernière version	–
Source(s)	Note de sécurité KB HT1991 Apple du 10 juin 2008
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

- Les versions d'Apple QuickTime antérieures à 7.5.

## 3 Résumé

Plusieurs vulnérabilités affectent le lecteur multimédia Apple QuickTime. L'exploitation de ces dernières peut conduire à l'exécution de code arbitraire sur le poste vulnérable ou à un dysfonctionnement du lecteur.

## 4 Description

Plusieurs vulnérabilités affectent le lecteur multimédia Apple QuickTime :

- l'application ne manipule pas correctement certains fichiers image au format PICT, en particulier leurs structures `PixData`. Cela peut provoquer sous certaines conditions un débordement de pile ;

- l'application ne manipule pas correctement des contenus multimédias encodés par AAC (*Advanced Audio Coding*). L'exploitation de cette vulnérabilité peut entraîner une corruption de la mémoire.
- l'application ne manipule pas correctement certains contenus multimédias nécessitant des codecs video In-deo.

## 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Apple 106704 du 10 juin 2008 :  
<http://docs.info.apple.com/article.html?artnum=106704>
- Note de sécurité KB HT1991 Apple du 10 juin 2008 :  
<http://support.apple.com/kb/HT1991>
- Référence CVE CVE-2008-1581 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1581>
- Référence CVE CVE-2008-1582 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1582>
- Référence CVE CVE-2008-1583 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1583>
- Référence CVE CVE-2008-1584 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1584>
- Référence CVE CVE-2008-1585 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1585>

## Gestion détaillée du document

**10 juin 2008** version initiale.