

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-2007-AVI-308>

---

### Gestion du document

Référence	CERTA-2007-AVI-308
Titre	Multiples vulnérabilités dans Apple QuickTime
Date de la première version	12 juillet 2007
Date de la dernière version	–
Source(s)	Avis de sécurité Apple 305947 du 11 juillet 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

- QuickTime 7.2 ainsi que les versions antérieures.

## 3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le lecteur multimédia Apple QuickTime. L'exploitation de ces dernières peut entraîner un dysfonctionnement de l'application, voire l'exécution de code arbitraire à distance sur le système vulnérable.

## 4 Description

- Plusieurs vulnérabilités ont été identifiées dans le lecteur multimédia Apple QuickTime. Parmi celles-ci :
- l'application ne manipulerait pas correctement les vidéos au format H. 264. Ce problème peut ainsi provoquer une corruption de la mémoire.

- l'application ne manipulerait pas correctement les fichiers au format .m4v. Ce problème peut ainsi provoquer un débordement d'entier.
- l'application ne manipulerait pas correctement les fichiers au format SMIL. Ce problème peut ainsi provoquer un débordement d'entier.
- les vérifications de sécurité (permissions) peuvent être contournées, dans QuickTime pour Java. L'exploitation de cette vulnérabilité, comme les précédentes, peut entraîner, sous certaines conditions, l'exécution de code arbitraire à distance sur le système vulnérable.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Apple du 11 juillet 2007 :  
<http://docs.info.apple.com/article.html?artnum=305947>
- Bulletin de sécurité iDefense du 11 juillet 2007 :  
<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=556>
- Référence CVE CVE-2007-2295 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2295>
- Référence CVE CVE-2007-2296 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2296>
- Référence CVE CVE-2007-2392 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2392>
- Référence CVE CVE-2007-2393 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2393>
- Référence CVE CVE-2007-2394 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2394>
- Référence CVE CVE-2007-2396 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2396>
- Référence CVE CVE-2007-2397 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2397>
- Référence CVE CVE-2007-2402 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2402>

## Gestion détaillée du document

12 juillet 2007 version initiale.