



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 30 mai 2007  
N° CERTA-2007-AVI-233

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : 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-233>

---

### Gestion du document

Référence	CERTA-2007-AVI-233
Titre	Vulnérabilités dans Apple QuickTime
Date de la première version	30 mai 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple 305531
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 ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

*QuickTime* version 7.1.6 pour MacOS X et Windows.

## 3 Résumé

Deux vulnérabilités affectant *QuickTime* permettent l'exécution de code arbitraire à distance et une atteinte à la confidentialité des données.

## 4 Description

Deux vulnérabilités ont été découvertes dans *QuickTime* pour MacOS X et Windows.

La première de ces vulnérabilités est due à une mauvaise manipulation des applets Java par *QuickTime*. Un utilisateur malintentionné peut, en incitant sa victime à visiter une page Web spécifiquement constituée, exécuter du code arbitraire à distance (CVE-2007-2388).

La seconde affecte également les applets Java. Un utilisateur malintentionné peut, par le biais d'une page Web spécifiquement constituée, accéder à la mémoire utilisée par le navigateur de sa victime (CVE-2007-2389).

## 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 305531 :  
<http://docs.info.apple.com/article.html?artnum=305531>
- Référence CVE CVE-2007-2388 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2388>
- Référence CVE CVE-2007-2389 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2389>

## Gestion détaillée du document

**30 mai 2007** version initiale.