



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 10 septembre 2008  
N° CERTA-2008-AVI-455

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-2008-AVI-455>

---

### Gestion du document

Référence	CERTA-2008-AVI-455
Titre	Multiples vulnérabilités dans Quicktime
Date de la première version	10 septembre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple #HT3027 du 09 septembre 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

- Apple Quicktime 7.x.

## 3 Résumé

De multiples vulnérabilités découvertes dans l'application Quicktime d'Apple permettent à un utilisateur distant malintentionné de provoquer un déni de service ou d'exécuter du code arbitraire.

## 4 Description

Plusieurs vulnérabilités de type débordement de mémoire, corruption de mémoire, mémoire non initialisée, pointeurs invalides ou encore un manque de contrôle en lecture peuvent être exploitées à distance afin de provoquer l'arrêt inopiné de l'application ou d'exécuter du code arbitraire.

## 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 #3027 du 09 septembre 2008 :  
<http://support.apple.com/kb/HT3027>
- Référence CVE CVE-2008-3614 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3614>
- Référence CVE CVE-2008-3615 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3615>
- Référence CVE CVE-2008-3624 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3624>
- Référence CVE CVE-2008-3625 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3625>
- Référence CVE CVE-2008-3626 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3626>
- Référence CVE CVE-2008-3627 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3627>
- Référence CVE CVE-2008-3628 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3628>
- Référence CVE CVE-2008-3629 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3629>
- Référence CVE CVE-2008-3635 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-3635>

## Gestion détaillée du document

**10 septembre 2008** version initiale.