

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-2008-AVI-025>

Gestion du document

Référence	CERTA-2008-AVI-025
Titre	Vulnérabilités dans Apple QuickTime
Date de la première version	16 janvier 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple 307301 du 15 janvier 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, pour les versions antérieures à 7.4.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans Apple QuickTime. Elles permettraient, exploitées par le biais de fichiers multimédia spécialement construits, d'exécuter des commandes arbitraires sur le système ayant un lecteur vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans Apple QuickTime. Elles concernent les fichiers multimédia au format vidéo Sorenson 3 et les images PICT, ainsi que la manipulation des informations Macintosh Resource d'un fichier vidéo ou l'analyse des atomes de description d'images (IDSC).

Ces vulnérabilités peuvent être exploitées par le biais de fichiers multimédia spécialement construits. La lecture de ceux-ci pourrait alors permettre d'exécuter du code arbitraire sur le système ayant une version de QuickTime vulnérable.

5 Solution

Se référer au bulletin de sécurité Apple 307301 pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Apple 307301-fr du 15 janvier 2008 :
<http://docs.info.apple.com/article.html?artnum=307301-fr>
- Référence CVE CVE-2007-0031 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0031>
- Référence CVE CVE-2008-0032 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0032>
- Référence CVE CVE-2008-0033 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0033>
- Référence CVE CVE-2008-0033 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0033>
- Référence CVE CVE-2008-0036 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0036>

Gestion détaillée du document

16 janvier 2008 version initiale.