

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités d'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-544>

Gestion du document

Référence	CERTA-2007-AVI-544
Titre	Multiples vulnérabilités d'Apple QuickTime
Date de la première version	14 décembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité QuickTime du 13 décembre 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

- Apple QuickTime versions antérieures à 7.3.1.

3 Résumé

De multiples vulnérabilités dans Apple QuickTime permettent d'effectuer un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

De multiples vulnérabilités affectent QuickTime :

- la première, CVE-2007-6166, décrite dans l'alerte CERTA-2007-ALE-017 concerne la prise en charge des flux RTSP ;

- la seconde, CVE-2007-4706, concerne la gestion des fichiers de liens QuickTime (possédant l'extension QTL). Cette vulnérabilité pourrait permettre à un utilisateur distant d'exécuter du code arbitraire ou de réaliser un déni de service par le biais d'un débordement de mémoire ;
- la dernière, CVE-2007-4707, concerne le composant Flash media handler de QuickTime. Ce composant est sujet à de multiples vulnérabilités dont certaines permettent à un utilisateur distant d'exécuter du code arbitraire. Le correctif fourni par Apple consiste à n'activer ce composant que pour des vidéos existantes et de confiance au format QuickTime.

5 Solution

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

6 Documentation

- Bulletin de sécurité QuickTime du 13 décembre 2007 :
<http://docs.info.apple.com/article.html?artnum=307176>
- Alerte du CERTA CERTA-2007-ALE-017 du 27 novembre 2007 :
<http://www.certa.ssi.gouv.fr/site/CERTA-2007-ALE-017/>
- Référence CVE CVE-2007-6166 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6166>
- Référence CVE CVE-2007-4706 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4706>
- Référence CVE CVE-2007-4707 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-4707>

Gestion détaillée du document

14 décembre 2007 version initiale.