

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-2009-AVI-206>

Gestion du document

Référence	CERTA-2009-AVI-206
Titre	Multiples vulnérabilités dans Apple QuickTime
Date de la première version	03 juin 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple HT3591 du 01 juin 2009
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Apple QuickTime pour les versions antérieures à 7.6.2.

Les systèmes d'exploitation peuvent être indifféremment Apple Mac OS X ou Microsoft Windows.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le lecteur multimédia Apple QuickTime. L'exploitation de celles-ci permet à une personne malveillante de perturber le service, voire d'exécuter du code arbitraire sur le système vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans le lecteur multimédia Apple QuickTime. Ce dernier ne manipulerait pas correctement certains formats de fichiers, comme les données vidéo de type Sorenson 3, les fichiers compressés par FLI/FLC, les images compressées par PSD ou aux formats PICT et JP2.

L'exploitation de ces vulnérabilités peut être réalisée avec des fichiers spécialement construits puis insérés dans des pages Web. Cela permet à une personne malveillante, à distance, de perturber le service, voire d'exécuter du code arbitraire sur le système vulnérable.

5 Solution

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

6 Documentation

- Note de sécurité Apple HT3591 du 01 juin 2009 :
<http://support.apple.com/kb/HT3591>
- Note de sécurité Apple HT3520 du 01 juin 2009 :
<http://support.apple.com/kb/HT3520>
- Bulletin de sécurité Apple 106704 du 01 juin 2009 :
<http://docs.info.apple.com/article.html?artnum=106704>
- Référence CVE CVE-2009-0010 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0010>
- Référence CVE CVE-2009-0185 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0185>
- Référence CVE CVE-2009-0188 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0188>
- Référence CVE CVE-2009-0951 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0951>
- Référence CVE CVE-2009-0952 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0952>
- Référence CVE CVE-2009-0953 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0953>
- Référence CVE CVE-2009-0954 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0954>
- Référence CVE CVE-2009-0955 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0955>
- Référence CVE CVE-2009-0956 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0956>
- Référence CVE CVE-2009-0957 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0957>

Gestion détaillée du document

03 juin 2009 version initiale.