Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 mars 2007
N° CERTA-2007-AVI-112

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Apple QuickTime

Gestion du document

Référence	CERTA-2007-AVI-112
Titre	Multiples vulnérabilités dans Apple QuickTime
Date de la première version	07 mars 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité 305149 du 06 mars 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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

Les versions de QuickTime antérieures à 7.1.5, pour Apple Mac OS ou Microsoft Windows.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans le logiciel Apple QuickTime. Elles permettraient à une personne malveillante qui les exploiteraient de perturber l'application, voire d'exécuter des commandes arbitraires sur le système ayant une version vulnérable.

4 Description

Plusieurs vulnérabilités ont été identifiées dans le lecteur multimedia Apple QuickTime. Elles concernent une mauvaise manipulation de fichiers aux formats suivants :

- *3rd Generation Partnership Project* (extensions de fichier : `.3gp` ou `.3g2`). Il s'agit d'un format de vidéos compressées prévues pour être diffusées sur les réseaux mobiles dits de troisième génération (3G).
- *MIDI*, ou *Musical Instrument Digital Interface* (extension `.smf`). Il s'agit d'un format destiné intialement à faire communiquer les instruments électroniques.
- *Quicktime* (extension : `.mov`). Il s'agit d'un format permettant de regrouper plusieurs types de données (texte, video ou audio par exemple).
- *PICT* (extension : `.pct`). Il s'agit d'un format vectoriel interne au fonctionnement de Macintosh.
- *QTIF*, ou *Quicktime Image File Format* (extension : `.qif`). Il s'agit d'un format permettant de regrouper plusieurs images compressées.

Ces vulnérabilités permettraient à une personne malveillante qui les exploiteraient de perturber l'application, voire d'exécuter des commandes arbitraires sur le système ayant une version vulnérable.

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 du 06 mars 2007 :
  http://docs.info.apple.com/article.html?artnum=305149
- Bulletin de sécurité iDefense du 05 mars 2007 :
  http://www.idefense.com/application/poi/display?id=486
- Référence CVE CVE-2006-4965 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4965
- Référence CVE CVE-2007-0711 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0711
- Référence CVE CVE-2007-0712 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0712
- Référence CVE CVE-2007-0713 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0713
- Référence CVE CVE-2007-0714 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0714
- Référence CVE CVE-2007-0715 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0715
- Référence CVE CVE-2007-0716 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0716
- Référence CVE CVE-2007-0717 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0717
- Référence CVE CVE-2007-0718 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0718

Gestion détaillée du document

07 mars 2007 version initiale.