Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 septembre 2006
N° CERTA-2006-AVI-390

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-2006-AVI-390

Gestion du document

Référence	CERTA-2006-AVI-390
Titre	Multiples vulnérabilités dans Apple QuickTime
Date de la première version	13 septembre 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple 304357 du 12 septembre 2006
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.

2 Systèmes affectés

La version 7.1.3 de QuickTime pour systèmes d'exploitation Apple MacOS X ou Microsoft Windows.

3 Résumé

Plusieurs vulnérabilités ont été identifiées dans Apple QuickTime. Une personne malveillante pourrait construire des fichiers multimédia particuliers, afin d'exécuter des commandes arbitraires sur le système qui ouvrirait ceux-ci avec une version de QuickTime vulnérable.

4 Description

QuickTime est une application fournie par Apple pour lire des fichiers multimédia (musique ou vidéo par exemple).

Plusieurs vulnérabilités ont été identifiées dans ce dernier. Il ne manipulerait pas correctement certains fichiers multimédias dans les formats suivants :

- `H.264`, aussi appelé `MPEG-4 AVC`;
- `FLC`;
- `FlashPix`;
- `SGI`.

Une personne malveillante pourrait construire des fichiers multimédia particuliers, afin d'exécuter des commandes arbitraires sur le système qui ouvrirait ceux-ci avec une version de QuickTime vulnérable.

5 Solution

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

6 Documentation

- Bulletin de sécurité Apple du 12 septembre 2006 :
  http://docs.info.apple.com/article.html?artnum=304357
- Référence CVE CVE-2006-4381 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4381
- Référence CVE CVE-2006-4386 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4386
- Référence CVE CVE-2006-4382 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4382
- Référence CVE CVE-2006-4384 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4384
- Référence CVE CVE-2006-4388 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4388
- Référence CVE CVE-2006-4389 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4389
- Référence CVE CVE-2006-4385 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-4385

Gestion détaillée du document

13 septembre 2006 version initiale.