Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 septembre 2009
N° CERTA-2009-AVI-378

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-378

Gestion du document

Référence	CERTA-2009-AVI-378
Titre	Multiples vulnérabilités dans Apple QuickTime
Date de la première version	10 septembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple HT3859 du 09 septembre 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.

2 Systèmes affectés

Apple QuickTime versions antérieures à 7.6.4.

3 Résumé

De multiples vulnérabilités dans *Apple Quicktime* permettent à une personne malintentionnée d'exécuter du code arbitraire à distance.

4 Description

Plusieurs vulnérabilités ont été identifiées dans *Apple Quicktime* :
- une faille de type corruption de mémoire dans le traitement de fichiers `H264` (CVE-2009-2202) ;
- un débordement de mémoire dans le traitement de fichiers vidéo `MPEG4` (CVE-2009-2203) ;
- un débordement de mémoire dans le traitement de fichiers `FlashPix` (CVE-2009-2798) ;

– un débordement de mémoire dans le traitement de fichiers `H264` (CVE-2009-2799).

L'ouverture d'un fichier spécialement conçu peut ainsi entraîner l'exécution de code arbitraire sur le poste vulnérable.

5 Solution

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

6 Documentation

– Bulletin Apple HT3859 du 09 septembre 2009 :
  http://support.apple.com/kb/HT3859
– Référence CVE CVE-2009-2202 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2202
– Référence CVE CVE-2009-2203 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2203
– Référence CVE CVE-2009-2798 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2798
– Référence CVE CVE-2009-2799 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2799

Gestion détaillée du document

10 septembre 2009 version initiale.