

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans iTunes

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-098>

Gestion du document

Référence	CERTA-2009-AVI-098
Titre	Vulnérabilités dans iTunes
Date de la première version	18 mars 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple HT3487 du 12 mars 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

- Déni de service à distance ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

Apple iTunes versions inférieures à 8.1.

3 Résumé

Deux vulnérabilités présentes dans iTunes permettent à un individu malveillant de réaliser un déni de service et d'atteindre à la confidentialité des données à distance.

4 Description

Deux vulnérabilités ont été découvertes dans iTunes :

- la première (CVE-2009-0016) concerne un manque de validation d'un paramètre présent dans l'en-tête des messages au format DAAP (*Digital Audio Access Protocol*). Un individu malveillant exploitant cette vul-

nérabilité peut réaliser un déni de service à distance au moyen d'un message au format *DAAP* spécialement construit. Cette vulnérabilité affecte uniquement les versions pour Windows d'iTunes.

- la seconde vulnérabilité (CVE-2009-0146) affecte une fonctionnalité d'iTunes. Un individu malveillant peut récupérer les données de connexion au moyen d'une baladodiffusion (*podcast*) spécialement construite.

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 HT3487 du 12 mars 2009 :
<http://support.apple.com/kb/HT3487>
- Référence CVE CVE-2009-0016 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0016>
- Référence CVE CVE-2009-0143 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0143>

Gestion détaillée du document

18 mars 2009 version initiale.