

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans Apple 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-2010-AVI-147>

Gestion du document

Référence	CERTA-2010-AVI-147
Titre	Multiples vulnérabilités dans Apple iTunes
Date de la première version	31 mars 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Apple HT4105 du 30 mars 2010
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 ;
- atteinte à la confidentialité des données ;
- élévation de privilèges.

2 Systèmes affectés

Apple iTunes versions antérieures à 9.1.

3 Résumé

Plusieurs vulnérabilités découvertes dans iTunes peuvent être exploitées par un utilisateur malintentionné afin de compromettre le système ou d'entraver son bon fonctionnement.

4 Description

De multiples vulnérabilités ont été découvertes dans iTunes :

- plusieurs erreurs dans les modules ColorSync et ImageIO peuvent conduire à une fuite de données ou de l'exécution de code arbitraire, notamment par le biais d'images spécialement conçues ;
- un fichier MP4 importé spécialement conçu entraîne la création d'une boucle infinie dans iTunes, provoquant ainsi un déni de service à distance ;
- une erreur dans le paquet d'installation d'iTunes pour Windows peut provoquer une élévation de privilèges.

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 HT4105 du 30 mars 2010 :
<http://support.apple.com/kb/HT4105>
- Référence CVE CVE-2009-2285 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2285>
- Référence CVE CVE-2010-0040 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0040>
- Référence CVE CVE-2010-0041 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0041>
- Référence CVE CVE-2010-0042 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0042>
- Référence CVE CVE-2010-0043 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0043>
- Référence CVE CVE-2010-0531 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0531>
- Référence CVE CVE-2010-0532 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0532>

Gestion détaillée du document

31 mars 2010 version initiale.