

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : iTunes : débordement de variable dans la gestion des listes de lecture

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-2005-AVI-016>

Gestion du document

Référence	CERTA-2005-AVI-016
Titre	iTunes : débordement de variable dans la gestion des listes de lecture
Date de la première version	18 janvier 2005
Date de la dernière version	-
Source(s)	Bulletin 01.43 de iDefense CVE : CAN-2005-0043
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 à distance de code arbitraire.

2 Systèmes affectés

Le logiciel iTunes dans la version 4.7. Les versions inférieures peuvent l'être aussi.

3 Résumé

Un débordement de variable affectant la gestion des URLs placés dans les listes de lecture du logiciel iTunes autorise l'exécution de code arbitraire.

4 Description

Le logiciel iTunes est un logiciel destiné à l'écoute de morceaux de musique. En particulier, il permet de manipuler des *listes de lecture* qui regroupent un certain nombre de morceaux.

Les listes de lecture sont des fichiers dont le nom porte l'extension `.pls` ou `.m3u`. Ces fichiers contiennent notamment des URLs permettant de désigner les morceaux de musique regroupés dans la liste.

Une mauvaise gestion de la longueur de ces URLs permet à un utilisateur mal intentionné de concevoir une liste de lecture contenant des URLs habilement constituées qui feront s'exécuter du code arbitraire avec les droits de l'utilisateur qui lance le logiciel `iTunes`.

Les listes de lecture peuvent être téléchargées par le logiciel `iTunes`. Cela permet à l'individu mal intentionné de proposer sur un site WEB par exemple ou dans n'importe quel système d'échange des listes de lectures malicieuses.

5 Contournement provisoire

Vérifier les listes de lecture venant d'endroits peu sûrs avant de les ouvrir avec `iTunes`. Se méfier en particulier des listes de lecture comprenant des URLs très longs.

6 Solution

La version 4.7.1 de `iTunes` publiée par Apple corrige la faille de sécurité.

7 Documentation

- correctif de sécurité :
<http://www.apple.com/fr/itunes/download>

Gestion détaillée du document

18 janvier 2005 version initiale.