



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 décembre 2010
N° CERTA-2010-AVI-596

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Movie Maker

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-596>

Gestion du document

Référence	CERTA-2010-AVI-596
Titre	Vulnérabilité dans Microsoft Movie Maker
Date de la première version	15 décembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-093 du 14 décembre 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.

2 Systèmes affectés

- Movie Maker 2.6 pour Microsoft Windows Vista Service Pack 1 et 2 ;
- Movie Maker 2.6 pour Microsoft Windows Vista édition x64 Service Pack 1 et 2.

3 Résumé

Une vulnérabilité dans Movie Maker 2.6 pour Microsoft Windows Vista peut permettre à un attaquant d'exécuter du code arbitraire à distance.

4 Description

Une vulnérabilité dans le traitement des fichiers DLL par Movie Maker 2.6 pour Microsoft Windows Vista peut permettre l'exécution de code arbitraire à distance. Elle nécessite l'ouverture par un utilisateur d'un fichier Windows Movie Maker (.mswmm) dans un système de fichiers distant ou un partage WebDAV dans lequel l'attaquant a placé une bibliothèque DLL spécialement conçue.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS10-093 du 14 décembre 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-093.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-093.msp>
- Référence CVE CVE-2010-3967 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3967>

Gestion détaillée du document

15 décembre 2010 version initiale.