

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Windows Media

---

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-2012-AVI-010>

---

### Gestion du document

Référence	CERTA-2012-AVI-010
Titre	Vulnérabilités dans Windows Media
Date de la première version	11 janvier 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS12-004 du 10 janvier 2012
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

- Bibliothèque multimedia Windows et DirectShow pour :
  - Windows XP Service Pack 3 ;
  - Windows XP Édition Media Center 2005 Service Pack 3 ;
  - Windows XP Professionnel Édition x64 Service Pack 2 ;
  - Windows Server 2003 Service Pack 2 ;
  - Windows Server 2003 Édition x64 Service Pack 2 ;
  - Windows Server 2003 avec SP2 pour système Itanium ;
  - Windows Vista Service Pack 2 ;
  - Windows Vista Édition x64 Service Pack 2 ;
  - Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
  - Windows Server 2008 pour systèmes x64 Service Pack 2 ;
  - Windows Server 2008 pour systèmes Itanium Service Pack 2 ;

- DirectShow pour :
  - Windows 7 pour systèmes 32 bits ;
  - Windows 7 pour systèmes 32 bits Service Pack 1 ;
  - Windows 7 pour systèmes x64 ;
  - Windows 7 pour systèmes x64 Service Pack 1 ;
  - Windows Server 2008 R2 pour systèmes x64 ;
  - Windows Server 2008 R2 pour systèmes x64 Service Pack 1 ;
  - Windows Server 2008 R2 pour systèmes Itanium ;
  - Windows Server 2008 R2 pour systèmes Itanium Service Pack 1 ;
- Pack TV Windows Media Center pour Windows Vista Édition 32 bits ;
- Pack TV Windows Media Center pour Windows Vista Édition 64 bits.

### 3 Résumé

Deux vulnérabilités permettant l'exécution de code à distance ont été corrigées dans des composants multimedia des systèmes Microsoft Windows.

### 4 Description

Une faille dans le traitement de fichiers au format *MIDI* permet à un attaquant d'exécuter du code à distance au moyen d'un fichier *MIDI* spécialement conçu (CVE-2012-0003). Une deuxième faille affectant le module *DirectShow* permet à une personne malveillante d'exécuter du code à distance au moyen d'un fichier multimédia spécialement conçu (CVE-2012-0004).

### 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 MS12-004 du 11 janvier 2012 :  
<http://technet.microsoft.com/fr-fr/security/bulletin/MS12-004>  
<http://technet.microsoft.com/en-us/security/bulletin/MS12-004>
- Référence CVE CVE-2012-0003 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0003>
- Référence CVE CVE-2012-0004 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0004>

## Gestion détaillée du document

11 janvier 2012 version initiale.