

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Microsoft DirectShow

---

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-273>

---

### Gestion du document

Référence	CERTA-2009-AVI-273
Titre	Multiples vulnérabilités dans Microsoft DirectShow
Date de la première version	15 juillet 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-028 du 14 juillet 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

Exécution de code arbitraire à distance.

## 2 Systèmes affectés

- DirectX 7.0 et DirectX 8.1 sur Windows 2000 SP4 ;
- DirectX 9.0 sur Windows 2000 SP4, Windows XP SP2 et SP3, Windows XP x64 SP2, Windows Server 2003 SP2, Windows Server 2003 x64 SP2 et Windows Server 2003 SP2 Pour Itanium.

## 3 Résumé

Trois vulnérabilités permettant l'exécution de code arbitraire à distance ont été corrigées.

## 4 Description

Trois vulnérabilités impactant DirectShow ont été corrigées. L'une d'elle, publiée sur l'Internet, concerne le traitement de films par la bibliothèque `quartz.dll`. Elles permettent à un utilisateur malveillant d'exécuter du code arbitraire à distance au moyen d'un fichier `QuickTime` spécialement créé.

## 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 MS09-028 du 14 juillet 2009 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-028.msp>  
<http://www.microsoft.com/technet/security/bulletin/MS09-028.msp>
- Référence CVE CVE-2009-1537 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1537>
- Référence CVE CVE-2009-1538 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1538>
- Référence CVE CVE-2009-1539 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1539>

## Gestion détaillée du document

**15 juillet 2009** version initiale.