



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 11 juin 2008  
N° CERTA-2008-AVI-307

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Microsoft DirectX

---

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-2008-AVI-307>

---

### Gestion du document

Référence	CERTA-2008-AVI-307
Titre	Vulnérabilités dans Microsoft DirectX
Date de la première version	11 juin 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-033 du 10 juin 2008
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 ;
- DirectX 8.1 ;
- DirectX 9.0 ;
- DirectX 10.0.

Toutes les versions de Microsoft Windows utilisant l'une de ces versions de DirectX sont potentiellement affectées.

## 3 Résumé

Deux vulnérabilités ont été identifiées dans Microsoft DirectX. Elles peuvent être exploitées à distance par le biais d'un fichier multimédia spécialement conçu afin d'exécuter du code arbitraire sur le système vulnérable.

## 4 Description

Deux vulnérabilités ont été identifiées dans la collection de bibliothèques Microsoft DirectX utilisée par différentes applications :

- le Codec MJPEG de Windows ne manipule pas correctement les flux MJPEG inclus dans des fichiers multimédias de type AVI (*Audio Video Interleave* ou ASF (*Advanced Systems Format*)) ;
- les fichiers de type SAMI (*Synchronized Accessible Media Interchange*) ne seraient pas correctement manipulés, et en particulier les propriétés de la variable *Class Name*.

## 5 Solution

Se référer au bulletin de sécurité MS08-033 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Microsoft MS08-033 du 10 juin 2008 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-033.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS08-033.msp>
- Note de sécurité ZDI-08-040 du 10 juin 2008 :  
<http://www.zerodayinitiative.com/advisories/ZDI-08-040>
- Référence CVE CVE-2008-0011 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0011>
- Référence CVE CVE-2008-1444 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1444>

## Gestion détaillée du document

**11 juin 2008** version initiale.