



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 12 décembre 2007  
N° CERTA-2007-AVI-539

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le format de fichier 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-2007-AVI-539>

---

### Gestion du document

Référence	CERTA-2007-AVI-539
Titre	Vulnérabilité dans le format de fichier Windows Media
Date de la première version	12 décembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-068 du 11 décembre 2007
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 ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- Module d'exécution du format Windows Media 7.1 ;
- Module d'exécution du format Windows Media 9 pour :
  - Windows 2000 Service Pack 4 ;
  - Windows XP Service Pack 2.
- Module d'exécution du format Windows Media 9.5 pour :
  - Windows XP Service Pack 2 ;
  - Windows XP Professionnel Edition x64 ;
  - Windows XP Professionnel Edition x64 Service Pack 2 ;
  - Windows Server 2003 Service Pack 1 ;
  - Windows Server 2003 Service Pack 2 ;
  - Windows Server 2003 Edition x64 ;
  - Windows Server 2003 Edition x64 Service Pack 2.

- Module d'exécution du format Windows Media 9.5 Edition x64 pour :
  - Windows XP Professionnel Edition x64 ;
  - Windows XP Professionnel Edition x64 Service Pack 2 ;
  - Windows Server 2003 Edition x64 ;
  - Windows Server 2003 Edition x64 Service Pack 2.
- Module d'exécution du format Windows Media 11 pour :
  - Windows XP Service Pack 2 ;
  - Windows XP Professionnel Edition x64 ;
  - Windows XP Professionnel Edition x64 Service Pack 2 ;
  - Windows Vista ;
  - Windows Vista Edition x64.
- Windows Media Services 9.1 pour :
  - Windows Server 2003 Service Pack 1 et Service Pack 2 ;
  - Windows Server 2003 Edition x64 y compris Service Pack 2 compris.

### 3 Résumé

Une vulnérabilité a été identifiée dans le traitement de certains fichiers média (ASF pour *Advanced Streaming Format*) par le module Windows Media Format Runtime. Cette vulnérabilité pourrait être exploitée par une personne malveillante par le biais d'un fichier spécialement construit, afin d'exécuter du code arbitraire sur le système.

### 4 Description

Une vulnérabilité a été identifiée dans le traitement de certains fichiers média (.ASF pour *Advanced Streaming Format*) par le module Windows Media Format Runtime. Ce format est utilisé pour le stockage et les échanges de données vidéo et audio. Cela implique en particulier les bibliothèques suivantes : `wmasf.dll` et `wmserver.dll`, et concernent notamment les extensions de type `.asf`, `.wmv` et `.wma`.

Cette vulnérabilité pourrait être exploitée par une personne malveillante par le biais d'un fichier spécialement construit et inséré dans une page Web ou un courriel, afin d'exécuter du code arbitraire sur le système.

### 5 Solution

Se référer au bulletin de sécurité MS07-068 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

### 6 Documentation

- Bulletin de sécurité Microsoft MS07-068 du 11 décembre 2007 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS07-068.mspx>  
<http://www.microsoft.com/technet/security/Bulletin/MS07-068.mspx>
- Référence CVE CVE-2007-0064 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0064>
- Avis de sécurité CERTA-2006-AVI-550 du 13 décembre 2006 :  
<http://www.certa.ssi.gouv.fr/site/CERTA-2006-AVI-550/>
- Microsoft Windows Media - Spécification ASF (*Advanced Systems Format*) :  
<http://www.microsoft.com/windows/windowsmedia/fr/format/asfspec.aspx>
- La différence entre les fichiers ASF et WMV/WMA :  
<http://support.microsoft.com/kb/284094/fr>

## Gestion détaillée du document

12 décembre 2007 version initiale.