



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 09 septembre 2009  
N° CERTA-2009-AVI-371

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans Windows Media Format

---

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-371>

---

### Gestion du document

Référence	CERTA-2009-AVI-371
Titre	Vulnérabilités dans Windows Media Format
Date de la première version	09 septembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-047 du 08 septembre 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

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Service Pack 3 ;
- Microsoft Windows XP Professional x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 2 ;
- Microsoft Windows Server 2003 x64 Edition Service Pack 2 ;
- Microsoft Windows Vista ;
- Microsoft Windows Vista Service Pack 1 ;
- Microsoft Windows Vista Service Pack 2 ;
- Microsoft Windows Vista x64 Edition ;
- Microsoft Windows Vista x64 Edition Service Pack 1 ;
- Microsoft Windows Vista x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2008 for 32-bit Systems ;

- *Microsoft Windows Server 2008 for 32-bit Systems Service Pack 2* ;
- *Microsoft Windows Server 2008 for x64-based Systems* ;
- *Microsoft Windows Server 2008 for x64-based Systems Service Pack 2*.

### 3 Résumé

Deux vulnérabilités dans *Windows Media Format* permettent l'exécution de code arbitraire à distance.

### 4 Description

Deux vulnérabilités ont été découvertes dans *Windows Media Format* :

- les fichiers au format ASF ne sont pas correctement traités (CVE-2009-2498) ;
- les métadonnées des fichiers au format MP3 ne sont pas correctement traitées (CVE-2009-2499).

Ces deux vulnérabilités permettent l'exécution de code arbitraire à distance.

### 5 Solution

Se référer au bulletin de sécurité *Microsoft* MS09-047 pour l'obtention des correctifs (cf. section Documentation).

### 6 Documentation

- Bulletin de sécurité Microsoft MS09-047 du 08 septembre 2009 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-047.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS09-047.msp>
- Référence CVE CVE-2009-2498 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2498>
- Référence CVE CVE-2009-2499 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2499>

## Gestion détaillée du document

09 septembre 2009 version initiale.