



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 octobre 2009
N° CERTA-2009-AVI-432

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Windows Media Player

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-432>

Gestion du document

Référence	CERTA-2009-AVI-432
Titre	Vulnérabilité dans Microsoft Windows Media Player
Date de la première version	14 octobre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-052 du 13 octobre 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 Media Player 6.4 sur les plateformes ;
– *Microsoft Windows* 2000 SP4 ;
– *Microsoft Windows XP* SP2, SP3, et *XP Professional x64 Edition* SP2 ;
– *Microsoft Windows Server* 2003 SP2 et et x64 SP2.

3 Résumé

Une vulnérabilité de *Microsoft Windows Media Player* lors de la lecture de fichiers ASF permet à un utilisateur malveillant d'exécuter du code arbitraire à distance.

4 Description

Microsoft Windows Media Player présente une vulnérabilité de type débordement de mémoire. Cette vulnérabilité est exploitable par un utilisateur malveillant au moyen d'un fichier au format ASF spécialement conçu. La lecture de ce fichier malveillant par un utilisateur permet l'exécution de code arbitraire et la prise du contrôle complet sur le système vulnérable.

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 MS09-052 du 13 octobre 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-052.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS09-052.msp>
- Référence CVE CVE-2009-2527 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-2527>

Gestion détaillée du document

14 octobre 2009 version initiale.