

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le traitement de fichiers 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-2009-AVI-326>

Gestion du document

Référence	CERTA-2009-AVI-326
Titre	Vulnérabilités dans le traitement de fichiers Windows Media
Date de la première version	12 août 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-038 du 11 août 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 et 3 ;
- Microsoft Windows XP Professionnel Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 2 ;
- Microsoft Windows Server 2003 Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2003 avec SP2 pour systèmes Itanium ;
- Microsoft Windows Vista, Windows Vista Service Pack 1 et Windows Vista Service Pack 2 ;
- Microsoft Windows Vista Édition x64, Windows Vista Édition x64 Service Pack 1 et Windows Vista Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes 32 bits et Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes x64 et Windows Server 2008 pour systèmes x64 Service Pack 2 ;

- Microsoft Windows Server 2008 pour systèmes Itanium et Windows Server 2008 pour systèmes Itanium Service Pack 2 ;

3 Résumé

Deux vulnérabilités dans le traitement de fichiers *Windows Media* permettent à une personne distante malintentionnée d'exécuter du code arbitraire.

4 Description

Deux vulnérabilités dans le traitement de fichiers *Windows Media* ont été découvertes. Des erreurs dans le traitement des fichiers *AVI* permettent à une personne malveillante d'exécuter du code arbitraire à distance via un fichier spécialement conçu.

5 Solution

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

6 Documentation

- Bulletin de sécurité Microsoft MS09-038 du 11 août 2009 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-038.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS09-038.msp>
- Référence CVE CVE-2009-1545 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1545>
- Référence CVE CVE-2009-1546 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1546>

Gestion détaillée du document

12 août 2009 version initiale.