

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du plug-in Media de Microsoft

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-2006-AVI-071>

Gestion du document

Référence	CERTA-2006-AVI-071
Titre	Vulnérabilité du plug-in Media de Microsoft
Date de la première version	14 février 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-006 du 14 février 2006
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 1 et Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows XP Professionnel Édition x64 et Microsoft Windows Server 2003 Édition x64 ;
- Microsoft Windows Server 2003 Édition x64.

3 Résumé

Une vulnérabilité du *plug-in Media* de Microsoft permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur le système vulnérable.

4 Description

Le *plug-in Media* de Microsoft permet à des navigateurs autre que Internet Explorer d'afficher du contenu de type vidéo lisible par ce *plug-in*. Une erreur dans le contrôle de la taille d'un champs par ce composant permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire par le biais d'un contenu vidéo malicieusement construit.

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 MS06-006 du 14 février 2006 :
<http://www.microsoft.com/france/technet/securite/MS06-006.mspx>
<http://www.microsoft.com/technet/security/Bulletin/MS06-006.mspx>
- Référence CVE CAN-2006-0005 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0005>

Gestion détaillée du document

14 février 2006 version initiale.