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 juin 2006
N° CERTA-2006-AVI-238

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Microsoft Windows Media Player

Gestion du document

Référence	CERTA-2006-AVI-238
Titre	Vulnérabilité de Microsoft Windows Media Player
Date de la première version	14 juin 2006
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS06-024 du 13 juin 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 ;
- déni de service.

2 Systèmes affectés

- Microsoft Windows Media Player version 10 sur les plates-formes Microsoft Windows Server 2003 SP1 et x64 Edition, Microsoft Windows XP SP1, SP2 et x64 Edition ;
- Microsoft Windows Media Player version 9 sur les plates-formes Microsoft Windows Server 2003, Microsoft Windows XP SP2 et SP1 et Microsoft Windows 200 SP4 ;
- Microsoft Windows Media Player versions 7.1 sur les plates-formes Microsoft Windows 2000 SP4 ;

Microsoft Windows Media Player version 6.4 n'est pas affecté par cette vulnérabilité.
Les plate-formes Microsoft Windows Server 2003, avec ou sans SP1, sur processeur Itanium ne sont pas affectées par cette vulnérabilité.

3 Description

PNG (`Portable Network Graphics`) est un format d'image utilisé par plusieurs applications Windows telles la messagerie instantanée (MSN messenger) ou l'outil Windows Media Player. Une vulnérabilité dans la gestion des fichiers au format `png` par Microsoft Windows Media Player permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire sur la machine vulnérable. L'exploitation peut se faire au moyen d'un fichier WMZ malicieusement constitué qui peut être envoyé par message électronique ou hébergé sur un site Internet.

4 Contournement provisoire

Un certain nombre de contournements provisoires sont listés dans le bulletin de sécurité Microsoft.

- Deux d'entre eux impliquent la modification de la base de registre Microsoft Windows. Il est très important de tester un tel contournement provisoire avant la mise en production ;
- désenregistrer la bibliothèque partagée `Wmp.dll` ;
- désassocier les extensions `WMZ` à l'aide de Microsoft Windows Explorer.

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 MS06-024 du 13 juin 2006 :
  http://www.microsoft.com/france/technet/securite/MS06-024.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS06-024.mspx
- Référence CVE CVE-2006-0025 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2006-0025

Gestion détaillée du document

14 juin 2006 version initiale.