Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 octobre 2010
N° CERTA-2010-AVI-485

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le service de partage réseau de Media Player

Gestion du document

Référence	CERTA-2010-AVI-485
Titre	Vulnérabilité dans le service de partage réseau de Media Player
Date de la première version	13 octobre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-075 du 12 octobre 2010
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

- Windows Media Player sur Windows Vista Service Pack 1 et Service Pack 2 ;
- Windows Media Player sur Windows Vista x64 Edition Service Pack 1 et Service Pack 2 ;
- Windows Media Player sur Windows 7 pour les systèmes 32 bits ;
- Windows Media Player sur Windows 7 pour les systèmes 64 bits.

3 Résumé

Une vulnérabilité présente dans le service de partage réseau de `Microsoft Windows Media Player` permet à un utilisateur d'exécuter du code arbitraire à distance. La configuration par défaut de ce service rend cette vulnérabilité exploitable uniquement depuis le réseau local.

4 Description

Une vulnérabilité a été identifiée dans le service de partage réseau du lecteur multimédia `Windows Media Player`. La réception d'un paquet *RTSP* spécialement conçu peut provoquer une exécution de code à distance.

En configuration par défaut, cette attaque ne peut être menée que depuis le réseau local. Sur les systèmes `Windows Vista, Windows 7 professionnel, entreprise` et `ultimate`, le service de partage n'est pas activé par défaut. Par contre, il est en service sur les autres versions de `Windows 7`.

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 MS10-075 du 12 octobre 2010 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS10-075.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS10-075.mspx
- Référence CVE CVE-2010-3225 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3225

Gestion détaillée du document

13 octobre 2010 version initiale.