Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 12 décembre 2012
N° CERTA-2012-AVI-722

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Windows DirectPlay

Gestion du document

Référence	CERTA-2012-AVI-722
Titre	Vulnérabilité dans Microsoft Windows DirectPlay
Date de la première version	12 décembre 2012
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS12-082 du 11 décembre 2012
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 Server 2003
– Microsoft Windows Server 2003 Service Pack 2
– Microsoft Windows Server 2003 Itanium Service Pack 1
– Microsoft Windows Server 2003 Itanium Service Pack 2
– Microsoft Windows Server 2003 x64 Edition
– Microsoft Windows Server 2003 x64 Edition Service Pack 2
– Microsoft Windows XP Media Center Edition 2005 Service Pack 3
– Microsoft Windows XP Professional x64 Edition Service Pack 2
– Microsoft Windows XP Service Pack 3
– Microsoft Windows XP Tablet PC Edition 2005 Service Pack 3
– Windows 7 32-bit
– Windows 7 32-bit Service Pack 1
– Windows 7 x64

- Windows 7 x64 Service Pack 1
- Windows 8 32-bit
- Windows 8 64-bit
- Windows Server 2008 R2 Itanium
- Windows Server 2008 R2 Itanium Service Pack 1
- Windows Server 2008 R2 x64
- Windows Server 2008 R2 x64 Service Pack 1
- Windows Server 2008 32-bit
- Windows Server 2008 32-bit Service Pack 2
- Windows Server 2008 Itanium
- Windows Server 2008 Itanium Service Pack 2
- Windows Server 2008 x64
- Windows Server 2008 x64 Service Pack 2
- Windows Server 2012
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Vista x64 Edition Service Pack 1
- Windows Vista x64 Edition Service Pack 2

3 Résumé

Une vulnérabilité a été corrigée dans *Microsoft Windows DirectPlay*. Elle permet à un attaquant d'exécuter du code arbitraire à distance au moyen d'un document *Office* spécialement conçu avec du contenu intégré.

4 Solution

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

5 Documentation

- Bulletin de sécurité Microsoft MS12-082 du 11 décembre 2012 :
  http://technet.microsoft.com/fr-fr/security/bulletin/ms12-082
- Référence CVE CVE-2012-1537
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-1537

Gestion détaillée du document

12 décembre 2012 version initiale.