

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans Windows Media Player

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-2007-AVI-358>

Gestion du document

Référence	CERTA-2007-AVI-358
Titre	Vulnérabilités dans Windows Media Player
Date de la première version	14 août 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-047 du 14 août 2007
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 7.1 pour Windows 2000 SP4 ;
- Windows Media Player 9 pour Windows 2000 SP4 ;
- Windows Media Player 9 pour Windows XP SP2 ;
- Windows Media Player 10 pour Windows XP SP2 ;
- Windows Media Player 10 pour Windows XP Professionnel Édition X64 (SP2 comprise) ;
- Windows Media Player 10 pour Windows 2003 Server SP1, SP2 et Édition X64 (SP2 comprise) ;
- Windows Media Player 11 pour Windows XP Professionnel Édition X64 (SP2 comprise) ;
- Windows Media Player 11 pour Windows Vista, y compris l'Édition X64.

3 Résumé

Deux vulnérabilités ont été identifiées dans le lecteur multimédia Windows Media Player. La lecture de fichiers spécialement construits et qui exploiteraient ces failles provoquerait ainsi l'exécution de code arbitraire sur la machine ayant une version vulnérable.

4 Description

Deux vulnérabilités ont été identifiées dans le lecteur multimédia Windows Media Player. Le traitement des fichiers d'apparence, ou *skins* ne serait pas correctement effectué par le lecteur. Ces fichiers ont une extension WMZ ou WMD.

Une personne malveillante pourrait exploiter l'une ou l'autre de ces deux vulnérabilités pour exécuter du code arbitraires sur le système ayant une version vulnérable.

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 MS07-047 du 14 août 2007 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS07-047.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-047.msp>
- Référence CVE CVE-2007-3035 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3035>
- Référence CVE CVE-2007-3037 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3037>

Gestion détaillée du document

14 août 2007 version initiale.