Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 27 novembre 2000
N° CERTA-2000-AVI-077

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans le lecteur multimédia Windows

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-2000-AVI-077

Gestion du document

Référence	CERTA-2000-AVI-077
Titre	Vulnérabilité dans le lecteur multimédia Windows
Date de la première version	27 novembre 2000
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft (MS00-090)
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.

2 Systèmes affectés

Plates-formes sous Windows 9x, NT, 2000 ou Millenium Edition utilisant le lecteur multimédia version 6.4 ou 7.

3 Résumé

Deux vulnérabilités présentes dans les versions 6.4 et 7 du lecteur multimédia de Windows permettent, à un concepteur malicieux d'un site internet ou par le biais d'un fichier transmis par mél ou tout autre moyen, d'exécuter du code arbitraire sur une machine distante.

4 Description

4.1 Fichiers au format .ASX

Les fichiers au format ASX (Active Stream Redirector) permettent à un utilisateur de visionner des séquences multimédia à distance par internet.

Le lecteur multimédia ne vérifie pas correctement certaines variables d'environnement concernant les fichiers ASX. Un concepteur de site internet mal intentionné peut concevoir un fichier ASX provoquant un débordement de pile et exécuter du code arbitraire sur la machine distante.

Les versions 6.4 et 7 du lecteur multimédia sont concernées par cette vulnérabilité.

4.2 Fichiers au format .WMS

Les fichiers au format WMS permettent de personaliser l'apparence du lecteur multimédia.

Un script malicieux placé dans un tel fichier permet de faire exécuter du code sur le poste distant avec les privilèges de ce dernier.

Cette vulnérablité n'affecte que la version 7 du lecteur multimédia, installée par défaut sous Windows Millenium Edition.

5 Solution

Correctif pour la version 6.4 :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=26069

Correctif pour la version 7 :
http://www.microsoft.com/Downloads/Release.asp?ReleaseID=26067

6 Documentation

Bulletin de sécurité Microsoft
http://www.microsoft.com/technet/security/bulletin/ms00-090.asp

Faq Microsoft
http://www.microsoft.com/technet/security/bulletin/fq00-090.asp

Gestion détaillée du document

27 novembre 2000 version initiale.