



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 juillet 2001
N° CERTA-2001-AVI-083

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Débordement de mémoire de 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-2001-AVI-083>

Gestion du document

Référence	CERTA-2001-AVI-083
Titre	Débordement de mémoire de Windows Media Player
Date de la première version	27 juillet 2001
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS01-042
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

Microsoft Windows Media player 7.1 7 et 6.4. Les versions précédentes sont peut-être vulnérables, mais ne sont plus maintenues par Microsoft.

3 Résumé

Un débordement de mémoire dans la gestion des fichiers .NSC par Windows Média Player permet à un utilisateur mal intentionné d'exécuter du code arbitraire sur la machine de la victime.

4 Description

Les fichiers avec l'extension en .NSC sont utilisés pour configurer les paramètres qui définissent les stations de flux audio pour Media Player.

Un utilisateur mal intentionné peut, par le biais de fichiers de ce type, faire effectuer un débordement de mémoire à Windows Média Player. Il peut ainsi exécuter du code sur la machine victime.

Ce type de fichier peut être exécuté automatiquement lors de la visualisation d'une page web. Il peut être aussi être exécuté automatiquement au travers d'un mél au format HTML ou d'une pièce jointe, c'est pourquoi il faut absolument appliquer les recommandations de la note d'information du CERTA concernant le mél, CERTA-2001-INF-002 : Mesures de prévention relatives à la messagerie.

5 Solution

- Pour la version 6.4 et 7.1 (Version Anglaise/US), appliquer le correctif de Microsoft :
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=31459>
- Pour la version 7, Microsoft recommande de passer à la version 7.1 de Windows Media Player.

6 Documentation

Bulletin de sécurité Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS01-042.asp>

Gestion détaillée du document

27 juillet 2001 version initiale.