

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du langage de commande Windows XP

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-2002-AVI-273>

Gestion du document

Référence	CERTA-2002-AVI-273
Titre	Vulnérabilité du langage de commande Windows XP
Date de la première version	19 décembre 2002
Date de la dernière version	–
Source(s)	Avis Foundstone Research Labs
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 ;
- déni de service.

2 Systèmes affectés

Microsoft Windows XP.

3 Résumé

Une vulnérabilité dans une fonction d'extraction d'attributs de fichier audio permet à un utilisateur mal intentionné de réaliser un déni de service ou d'exécuter du code arbitraire à distance.

4 Description

Un débordement de tampon a été découvert dans l'une des fonctions d'extraction d'attributs de fichier audio (extensions ".mp3" et ".wma"). Un utilisateur mal intentionné peut créer habilement un fichier audio et le placer

sur une page internet, dans un dossier partagé, ou l'envoyer dans un courrier électronique au format HTML. Lors du simple passage de la souris au dessus de ce fichier, la fonction vulnérable du langage de commande Windows XP est appelée, et le code malicieux exécuté.

Note: Cette vulnérabilité concerne le langage de commande de Windows XP et non le lecteur windows Media Player.

5 Solution

Consulter le bulletin MS02-072 de Microsoft pour connaître la disponibilité des correctifs.

6 Documentation

Bulletin de sécurité Microsoft MS02-072 :

<http://www.microsoft.com/technet/security/bulletin/MS02-072.asp>

Gestion détaillée du document

19 décembre 2002 version initiale.