Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 03 octobre 2002
N° CERTA-2002-AVI-219

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les fonctions de décompression des dossiers sous Windows

Gestion du document

Référence	CERTA-2002-AVI-219
Titre	Vulnérabilités dans les fonctions de décompression des dossiers sous Windows
Date de la première version	03 octobre 2002
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS02-054
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 ;
- déni de service.

2 Systèmes affectés

- Microsoft Windows 98 avec le service Pack Plus ;
- Microsoft Windows Me ;
- Microsoft Windows XP.

3 Résumé

Deux vulnérabilités présentes dans l'utilitaire de décompression des dossiers sous Windows permettent d'exécuter du code arbitraire ou d'entraîner un déni de service sur la machine cible.

4 Description

Les versions affectées de Windows disposent d'un utilitaire permettant de compresser les répertoires au format `zip` afin de bénéficier de plus d'espace disque.

Cet utilitaire permet également d'employer ces répertoires compressés de manière transparente pour l'utilisateur.

Deux vulnérabilités ont été découvertes dans cet utilitaire.

Une mauvaise interprétation des noms de fichiers longs par l'utilitaire de décompression permet à un utilisateur mal intentionné d'exécuter du code arbitraire ou d'effectuer un déni de service de l'explorateur au moyen d'un dossier compressé judicieusement composé.

La seconde vulnérabilité permet de forcer la décompression des fichiers dans un emplacement spécifique, par exemple Dossier Démarrage, dans le but de faire exécuter ultérieurement ces fichiers.

Ces deux vulnérabilités ne peuvent être exploitées à distance. Cependant, il est possible de proposer un dossier dangereux à un utilisateur soit par le biais d'une page Web le proposant en téléchargement, soit par envoi de mél.

5 Solution

Appliquer le correctif disponible en téléchargement sur le site de Microsoft (consulter la section documentation).

6 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS02-054.asp

Gestion détaillée du document

03 octobre 2002 version initiale.