Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 13 octobre 2004
N° CERTA-2004-AVI-338

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité des répertoires compressés sous Windows

Gestion du document

Référence	CERTA-2004-AVI-338
Titre	Vulnérabilité des répertoires compressés sous Windows
Date de la première version	13 octobre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS04-034 du 12 octobre 2004
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

- Déni de service ;
- exécution de code arbitraire à distance.

2 Systèmes affectés

- Microsoft Windows XP ;
- Microsoft Windows XP Service Pack 1 ;
- Microsoft Windows XP 64-Bit Edition Service Pack 1 ;
- Microsoft Windows XP 64-Bit Edition version 2003 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 64-Bit Edition.

3 Résumé

Une vulnérabilité dans la gestion des répertoires compressés 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 pile est présent dans la bibliothèque `zipfldr.dll` permettant la manipulation des répertoires compressés.
Un utilisateur mal intentionné peut, via l'utilisation d'un répertoire compressé contenant un fichier habilement constitué, réaliser un déni de service ou exécuter du code arbitraire sur la plate-forme 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 MS04-034 du 12 octobre 2004 :
  http://www.microsoft.com/technet/security/bulletin/MS04-034.mspx
- Référence CVE CAN-2004-0575 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0575

Gestion détaillée du document

13 octobre 2004 version initiale.