Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 octobre 2002
N° CERTA-AVI-2002-238

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Problème de permissions sous Windows 2000

Gestion du document

Référence	CERTA-AVI-2002-238
Titre	Problème de permissions sous Windows 2000
Date de la première version	31 octobre 2002
Date de la dernière version	–
Source(s)	–
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 d'un cheval de troie sur la machine.

2 Systèmes affectés

Toutes les versions de Windows 2000, indépendamment des correctifs installés sur la machine.

3 Résumé

Par défaut, le répertoire racine de Windows 2000 est en accès lecture, écriture et exécution pour tous les utilisateurs. Cette politique de sécurité par défaut du répertoire racine peut permettre à un utilisateur mal intentionné d'installer et de faire exécuter un cheval de Troie sur la machine, à l'insu de l'utilisateur.

4 Description

Par défaut dans Windows 2000, le répertoire racine (typiquement C:) est en accès lecture, écriture et exécution pour le groupe "Tout le monde". Un utilisateur mal intentionné ayant accès à la machine peut ainsi déposer un

cheval de Troie dans le répertoire racine portant le nom d'un binaire légitime de Windows (typiquement cmd.exe). Lors de la recherche et de l'exécution d'un fichier, et si cette recherche inclut le répertoire racine, un utilisateur peut alors exécuter un cheval de Troie à son insu, pensant qu'il s'agit du binaire légitime.

5 Solution

Microsoft ne fournit pas de solution sous forme de correctif mais recommande à l'administrateur d'élaborer un système de permissions du répertoire racine s'inspirant de celles de Windows XP, à savoir :

- Administrateur : accès illimité (répertoire courant, sous-répertoires et fichiers) ;
- créateurs propriétaires : accès illimité (sous-répertoires et fichiers) ;
- système : accès illimité (répertoire courant, sous-répertoires et fichiers) ;
- tout le monde : accès en lecture et exécution (répertoire courant seulement).

6 Documentation

Bulletin de sécurité Microsoft MS02-064
http://www.microsoft.com/technet/security/bulletin/MS02-064.asp

Gestion détaillée du document

31 octobre 2002 version initiale.