Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 10 février 2005
N° CERTA-2005-AVI-061

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans la gestion des "tubes nommés" du système Windows XP

Gestion du document

Référence	CERTA-2005-AVI-061
Titre	Vulnérabilité dans la gestion des "tubes nommés" du système Windows XP
Date de la première version	10 février 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-007
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

Atteinte à la confidentialité des données.

2 Systèmes affectés

- Windows XP Service Pack 1 et Microsoft Windows XP Service Pack 2 ;
- Windows XP édition 64-Bit Edition Service Pack 1 (Itanium).

3 Résumé

Une vulnérabilité dans la gestion des "tubes nommés" permet à un utilisateur distant mal intentionné d'obtenir le nom des utilisateurs connectés à un système Microsoft Windows XP vulnérable.

4 Description

Les "tubes nommés" (ou *named pipes*) servent à la communication entre plusieurs processus, soit sur une même machine, soit sur des machines différentes reliées au même réseau.

Une vulnérabilité dans la gestion de ces "tubes nommés" dans les systèmes Microsoft Windows XP permet à un utilisateur mal intentionné d'obtenir le nom des utilisateurs connectés au système vulnérable.

L'exploitation de cette vulnérabilité n'est possible que si le service "Explorateur d'ordinateur" (ou *Computer browser*) est activé.

Il est activé par défaut dans les systèmes Windows XP Service Pack 1, mais il est désactivé par défaut dans les systèmes Windows XP Service Pack 2.

5 Contournement provisoire

- Désactiver le service "Explorateur d'ordinateur" ;
- bloquer les ports 139/tcp et 445/tcp pour limiter les attaques venant de l'extérieur.

6 Solution

Appliquer le correctif proposé par Microsoft (cf. section Documentation).

7 Documentation

Bulletin de sécurité Microsoft MS-05-007 du 08 février 2005 :
http://www.microsoft.com/technet/security/bulletin/MS05-007.mspx

Gestion détaillée du document

10 février 2005 version initiale.