



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 16 décembre 2004
N° CERTA-2004-AVI-401

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du pare-feu Microsoft Windows XP SP2

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-2004-AVI-401>

Gestion du document

Référence	CERTA-2004-AVI-401
Titre	Vulnérabilité du pare-feu Microsoft Windows XP SP2
Date de la première version	16 décembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft du 14 décembre 2004
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

- Contournement de la politique de sécurité ;
- atteinte à la confidentialité des données ;
- atteinte à l'intégrité des données.

2 Systèmes affectés

- Microsoft Windows XP Home Edition Service Pack 2 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Tablet PC Edition 2005 ;
- Microsoft Windows XP Media Center Edition Service Pack 2.

3 Résumé

Un défaut de configuration du pare-feu de Microsoft Windows XP Service Pack 2 permet à un utilisateur mal intentionné de contourner la politique de sécurité mise en place sur le système.

4 Description

La configuration par défaut de Microsoft Windows XP autorise le partage de fichiers et d'imprimante.

Un système se connectant à l'Internet au moyen d'un modem et d'une ligne téléphonique standard ou RNIS, va engendrer une table routage qui sera interpréter de manière incorrecte par le pare-feu de Microsoft Windows XP Service Pack2.

Cette mauvaise gestion provoque une incohérence dans la définition des paramètres de sécurité, le pare-feu considère que la zone Internet fait partie de la zone *Intranet local*. Un utilisateur mal intentionné peut alors porter atteinte à la confidentialité et/ou à l'intégrité des données partagées par le système vulnérable.

5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. Documentation).

6 Documentation

- Bulletin de sécurité Microsoft :
<http://support.microsoft.com/kb/886185>

Gestion détaillée du document

16 décembre 2004 version initiale.