Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 07 février 2002
N° CERTA-2002-AVI-024

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Microsoft Office v.X pour Mac OS X

Gestion du document

Référence	CERTA-2002-AVI-024
Titre	Vulnérabilité dans Microsoft Office v.X pour Mac OS X
Date de la première version	07 février 2002
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-002
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

- Perte de données ;
- Déni de service.

2 Systèmes affectés

Microsoft Office v.X pour Mac OS X.

3 Résumé

Une vulnérabilité dans la gestion des PID (Product Identifier) permet à utilisateur distant mal intentionné, par le biais de requêtes IP spécifiques, d'interrompre les applications Office d'une machine cible.

4 Description

Chaque version de Microsoft Office v.X possède un numéro unique d'identification (PID). Lors du lancement d'une application Office sur une machine, ce numéro est transmis sur le réseau IP dans le but de vérifier que deux licences identiques ne sont pas utilisées simultanement. Dans cette éventualité, l'application est automatiquement

fermée (sans sauvegarde des données) sur les deux postes possédant le même PID. Ce numéro PID est également transmis à intervalles réguliers.

Une vulnérabilité dans la gestion de certains paquets PID permet à un utilisateur distant mal intentionné, par le biais de requêtes IP judicieusement composées d'interrompre le service `Network PID` de la machine cible. L'interruption de ce service entraîne la fermeture sans sauvegarde de l'application Office.

5 Contournement provisoire

Bloquer le port 2222 sur le garde barrière pour éviter les attaques provenant de l'extérieur.

6 Solution

Télécharger le correctif sur le site Microsoft :
http://www.microsoft.com/mac/download

7 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS02-002.asp

Gestion détaillée du document

07 février 2002 version initiale.