Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 06 novembre 2001
N° CERTA-2001-AVI-137

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de UPnP sous Windows

Gestion du document

Référence	CERTA-2001-AVI-137
Titre	Vulnérabilité de UPnP sous Windows
Date de la première version	06 novembre 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-054
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.

2 Systèmes affectés

- Windows 98 ;
- Windows ME ;
- Windows XP.

3 Résumé

Un utilisateur distant mal intentionné peut, par le biais de requêtes UPnP habilement composées, réaliser un déni de service sur la machine cible.

4 Description

Le service UPnP (Universal Plug and Play) est un service permettant de découvrir automatiquement de nouveaux équipements réseau. Ce service est disponible sur divers équipements: imprimantes, etc.

Une vulnérabilité de la gestion des requêtes UPnP de Windows peut entraîner un déni de service sur la machine cible, si un utilisateur mal intentionné transmet des requêtes spécifiquement construites.

Nota : Sur Windows ME et XP, UPnP est installé par défaut. Il est installé sur Windows 98 lors de la mise en place du client de partage de connexion internet.

5 Contournement provisoire

Filtrer les ports 1900 et 5000 (TCP et UDP) au niveau du garde barrière, pour éviter les attaques provenant de l'extérieur.

6 Solution

Télécharger le correctif sur le site Microsoft :

- Microsoft Windows 98 et 98SE :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=33592
- Microsoft Windows ME et XP :
  http://www.microsoft.com/Windowsupdate

7 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-054.asp

Gestion détaillée du document

06 novembre 2001 version initiale.