Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 24 décembre 2001
N° CERTA-2001-AVI-165

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de UPnP sous Windows

Gestion du document

Référence	CERTA-2001-AVI-165
Titre	Vulnérabilité de UPnP sous Windows
Date de la première version	24 décembre 2001
Date de la dernière version	–
Source(s)	Bulletin Microsoft MS01-059
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 de code arbitraire ;
- Déni de service.

2 Systèmes affectés

- Windows 98 ;
- Windows 98 SE ;
- Windows Millenium Edition ;
- Windows XP.

3 Résumé

Un utilisateur distant mal intentionné peut, par le biais de requêtes UPnP habilement composées, exécuter du code arbitraire ou entraîner 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 machine utilisant le service UPnP transmet une requête « M-SEARCH » afin de connaître les ressources UPnP du réseau. Les machines proposant de telles ressources (exemple : imprimantes) transmettent une requête « NOTIFY ».

Deux vulnérabilités ont été découvertes dans le service UPnP.

La première vulnérabilité permet, pas le biais d'un débordement de pile dans la gestion des requêtes « NOTIFY », d'exécuter du code arbitraire sur la machine cible (avec les privilèges « SYSTEM » sous Windows XP).

La seconde vulnérabilité permet, par le biais d'une mauvaise gestion des requêtes « NOTIFY », de réaliser un déni de service en consommant toutes les ressources de la machine cible.

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 :

- Windows 98/98SE :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=34991
- Windows ME :
  http://download.microsoft.com/download/winme/Update/22940/WinMe/EN-US/314757USAM.EXE
- Windows XP :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=34951

7 Documentation

Bulletin Microsoft :
http://www.microsoft.com/technet/security/bulletin/MS01-059.asp

Gestion détaillée du document

24 décembre 2001 version initiale.