Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 19 octobre 2000
N° CERTA-2000-AVI-063

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités dans les composants de Microsoft Windows

Gestion du document

Référence	CERTA-2000-AVI-063
Titre	Vulnérabilités dans les composants de Microsoft Windows
Date de la première version	19 octobre 2000
Date de la dernière version	–
Source(s)	NTBugTraq Bulletins de sécurité Microsoft
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

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

1 Risques

- Déni de service sur Microsoft Netmeeting Shared Desktop,
- Exécution de code arbitraire à cause d'Hyper Terminal

2 Systèmes affectés

- Microsoft Netmeeting 3.01 sous Windows NT et 2000
- Hyper Terminal
  - Windows 98;
  - Windows98SE;
  - Windows Millenium Edition (ME);
  - et Windows 2000.

3 Résumé

Il existe des vulnérabilités dans *Hyper Terminal*, un composant de Windows proposé par défaut lors de son installation, et *Netmeeting* qui est un composant gratuit des systèmes Microsoft, permettant de faire de la visio-conférence et du travail à distance.

4 Description

- Microsoft *Netmeeting* est un outil de visio-conférence dont la composante *Shared Desktop* permet à la maintenance de prendre la main à distance sur une machine.
  Un utilisateur distant peut, en envoyant un certains type de paquets vers sa victime sur le port de communication de *Netmeeting* pendant que le logiciel fonctionne, faire monter la charge du processeur jusqu'au blocage du logiciel à la fin de son attaque.
  Il se peut que le gestionnaire des tâches de Windows, n'ai pas accès à la tâche en court, et qu'il faille un autre outils ne faisant pas partie intégrante du système, ou redémarrer la machine, pour arrêter l'effet de l'attaque.
- *Hyper Terminal* est un outil ressemblant à `telnet` installé sur les systèmes Windows 98, 98SE, ME, NT et 2000, et c'est le client répondant par défaut à l'URL `telnet://` pour les systèmes Windows 98, 98SE et ME.
  Un utilisateur mal intentionné peut, à l'aide d'un lien telnet vers une URL malformée dissimulé par exemple dans une page web ou un mail, générer un dépassement de mémoire sur la machine qui lance le client telnet, et ainsi exécuter du code sur cette machine.

5 Contournement provisoire

Filtrer le port 1270 ou bloquer selon les besoins, avec un garde-barrière, afin d'éviter ce type d'attaque.
Supprimer Hyper Terminal, et utiliser telnet ou un équivalent pour se connecter à un serveur telnet.

6 Solution

Appliquer le correctif Microsoft :

- Pour Netmeeting pour Windows 2000 (il n'y a pas encore de correctif pour Windows NT4) :
  http://www.microsoft.com/Downloads/Release/Release.asp?ReleaseID=25029
- Pour Hyper Terminal pour Windows 98 et 98SE :
  http://download.microsoft.com/download/win98/Update/12395/W98/EN-US/274548USA8.EXE
- Hyper Terminal pour Windows ME :
  http://download.microsoft.com/download/winme/Update/12395/WinMe/EN-US/274548USAM.EXE
- Windows 2000 (Gold et SP1 compris) :
  http://www.microsoft.com/download/release.asp?releaseid=25112

7 Documentation

Les bulletins de sécurité de Microsoft et leur FAQ :

- Pour Netmeeting :
  - http://www.microsoft.com/technet/security/bulletin/ms00-077
    et
  - http://www.microsoft.com/technet/security/bulletin/fq00-077
- Pour Hyper Terminal
  - http://www.microsoft.com/technet/security/bulletin/ms00-079
    et
  - http://www.microsoft.com/technet/security/bulletin/fq00-079

Gestion détaillée du document

19 octobre 2000 version initiale.