Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 29 mai 2000
N° CERTA-2000-AVI-004

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans le protocole du service explorateur d'ordinateurs sous Windows NT et Windows 2000

Gestion du document

Référence	CERTA-2000-AVI-004
Titre	Vulnérabilité dans le protocole du service explorateur d'ordinateurs sous Windows NT et Windows
Date de la première version	29 mai 2000
Date de la dernière version	–
Source(s)	Avis CA-2000-06 du CERT/CC Microsoft Security Bulletins CERT IST
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

- Microsoft Windows NT 4.0 ;
- Microsoft Windows 2000.

3 Résumé

Deux vulnérabilités ont été découvertes dans le protocole de l'« explorateur d'ordinateurs » (computer browser protocol), utilisé par exemple par le « voisinage réseau ».

Ces vulnérabilités permettent à un utilisateur mal intentionné de rendre invisible tout un sous-réseau aux explorateurs d'ordinateurs voire de permettre des dénis de services.

4 Description

L'explorateur permet à un serveur d'identifier dans un réseau les machines sous windows (ou utilisant Samba) et les ressources qu'elles partagent.

La première vulnérabilité affecte les systèmes Windows NT et Windows 2000 et permet à un utilisateur mal intentionné de couper la fonction « explorateur d'ordinateurs » du maître explorateur du sous-réseau dans lequel il se trouve. Il peut aussi promouvoir sa propre machine au rang de « maître explorateur » . Ces actions ont pour conséquence de rendre invisible dans « l'explorateur d'ordinateur » de windows tous les ordinateurs de son sous-réseau, ainsi que toutes les ressources partagées par ces machines.

La seconde vulnérabilité ne touche que les systèmes sous Windows NT et permet à un utilisateur mal intentionné de surcharger le trafic réseau en fausses annonces, ce qui cause des problèmes dans les tables du « maître explorateur », et peut ralentir ou bloquer d'autres services par la diminution de la bande passante.

5 Solution

Microsoft met à disposition un correctif concernant ces vulnérabilités de l'explorateur d'ordinateurs sous Windows NT 4.0 et 2000 (Versions US) aux adresses suivantes :

- Windows NT 4.0 Workstation, Server, et Server, Enterprise Edition :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21397
- Windows 2000 :
  http://www.microsoft.com/Downloads/Release.asp?ReleaseID=21298

6 Documentation

1° Bulletin de sécurité Microsoft MS00-036 du 25 mai 2000
http://www.microsoft.com/technet/security/bulletin/ms00-036.asp .

2° FAQ concernant le bulletin MS00-036 de Microsoft
http://www.microsoft.com/technet/security/bulletin/fq00-036.asp .

3° Article de la Knowledge Base - Q262694 - de Microsoft à propos des vulnérabilités de l'explorateur d'ordinateurs sur le réseau Windows
http://www.microsoft.com/technet/support/kb.asp?ID=262694 .

4° Article de la Knowledge Base - Q263307 - de Microsoft à propos des vulnérabilités de l'explorateur d'ordinateurs sur le réseau Windows
http://www.microsoft.com/technet/support/kb.asp?ID=263307

Gestion détaillée du document

29 mai 2000 version initiale.