Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 08 août 2000
N° CERTA-2000-AVI-025

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité de Windows 9x avec le protocole IPX

Conditions d'utilisation de ce document : http://www.certa.ssi.gouv.fr/certa/apropos.html
Dernière version de ce document : http://www.certa.ssi.gouv.fr/site/CERTA-2000-AVI-025

Gestion du document

Référence	CERTA-2000-AVI-025
Titre	Vulnérabilité de Windows 9x avec le protocole IPX
Date de la première version	08 août 2000
Date de la dernière version	–
Source(s)	Bulletin de Sécurité Microsoft Avis du 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

Congestion de réseau, déni de service.

2 Systèmes affectés

Windows 95 et Windows 98 seconde édition équipés du protocole IPX

3 Résumé

Le protocole IPX de Windows 95 et Windows 98 traite les paquets dont la source est une adresse de diffusion (*broadcast*)au lieu de les ignorer. Un correctif a été mis au point pour corriger cette erreur.

4 Description

IPX est un protocole de communication réseau développé par Novell. Comme dans le protocole TCP/IP, la notion de diffusion (*broadcast*) existe sous IPX. Une adresse de diffusion est une adresse faisant référence à tout le réseau. Lorsqu'elle est utilisée comme adresse de destination d'un paquet, le paquet est envoyé à tout le réseau.

Une erreur dans la façon de traiter les paquets « Ping » IPX a été découverte dans l'implémentation de ce protocole sous Windows 9x.

Une machine vulnérable qui reçoit un paquet IPX ping ayant pour adresse source l'adresse de diffusion du réseau, va envoyer une réponse à tout le réseau au lieu de rejeter le paquet.

De plus si l'émetteur de ce paquet utilise une adresse de diffusion comme destination, toutes les machines vulnérables renverront une réponse à tout le réseau. Ceci aura pour conséquence de générer un trafic dont l'importance sera proportionnelle au nombre de machines vulnérables sur le réseau.

En conséquence, on peut observer pendant quelques secondes une surcharge brutale du trafic sur le réseau.

Enfin, une machine qui reçoit un paquet de réponse à un ping IPX qu'elle a elle-même émis (car elle se situe dans l'adresse de diffusion), tente de le traiter, ce qui peut engendrer un blocage du système. Il faut redémarrer la machine.

Nota : La plupart des routeurs filtrent le protocole IPX, ce qui rend les attaques provenant de l'extérieur d'un réseau, et donc d'internet, moins probables.

IPX n'est pas installé par défaut sous Windows 98

5 Solution

Appliquer les correctifs concernant le protocole IPX pour les système Windows 95 et Windows 98 (version US) :

- Pour Windows 98 :
  http://download.microsoft.com/download/win98/Update/8982/W98/EN-US/265334USA8.EXE
- Pour Windows 95 :
  http://download.microsoft.com/download/win95/Update/8982/W95/EN-US/265334US5.EXE

6 Documentation

- Bulletin de sécurité de Microsoft :
  http://www.microsoft.com/technet/security/bulletin/ms00-054.asp
- FAQ concernant le bulletin MS00-054 de Microsoft
  http://www.microsoft.com/technet/security/bulletin/fq00-054.asp
- Article Q269523 de la Base de Connaissances de Microsoft concernant le bulletin MS00-054
  http://www.microsoft.com/technet/support/kb.asp?ID=265334

Gestion détaillée du document

08 août 2000 version initiale.