

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans IPX/SPX de Microsoft sous Windows 9x/ME

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-058>

Gestion d document

Référence	CERTA-2000-AVI-058
Titre	Vulnérabilité dans IPX/SPX de Microsoft sous Windows 9x/ME
Date de la première version	12 octobre 2000
Date de la dernière version	–
Source(s)	Bulletin 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 Risque

Déni de service par amplification de trafic.

2 Systèmes affectés

Windows 9x et Millenium Edition.

3 Résumé

Une vulnérabilité dans l'implémentation d'IPX/SPX par Microsoft (NWLINK) permet à un utilisateur mal intentionné de déclencher une « tempête » de *broadcast*, et de désactiver les services répondant aux requêtes dans ce protocole.

4 Description

Le protocole IPX/SPX sous Microsoft Windows inclue un service appelé *NMPI* (Name Management Protocol on IPX, supplantant NBNS en l'absence du protocole NetBIOS) qui répond à la requête de n'importe quelle adresse

réseau. La vulnérabilité de IPX réside dans le fait que ce service ne filtre pas les adresses réseau correctement. Si l'adresse source est une adresse de *broadcast*, il répondra à tout le réseau, et entraînera une réponse de toutes les autres machines du réseau.

Le trafic du réseau peut augmenter considérablement dans de tels cas, et des machines peuvent être bloquées par l'exploitation de cette vulnérabilité. Pour débloquer les machines, il faudra les redémarrer.

5 Contournement provisoire

IPX/SPX est installé par défaut lors de l'installation de Windows 95 si la machine contient une carte réseau. Il n'est pas installé par défaut sur Windows 98 et Millenium Edition.

Si vous n'utilisez pas IPX/SPX sur votre réseau, supprimez ce protocole de toutes vos machines.

Filtrez ce protocole à l'aide de votre garde-barrière.

6 Solution

Appliquer le correctif de Microsoft (Version US) sur toutes les machines utilisant ce protocole.

<http://download.microsoft.com/download/win95/Update/11974/EN-US/273727USA5.EXE>

<http://download.microsoft.com/download/win98/Update/11974/EN-US/273727USA8.EXE>

<http://download.microsoft.com/download/winMe/Update/11974/EN-US/273727USAM.EXE>

7 Documentation

- Le bulletin de sécurité de Microsoft :
<http://www.microsoft.com/technet/security/bulletin/MS00-073.asp>
- La FAQ concernant ce bulletin :
<http://www.microsoft.com/technet/security/bulletin/fq00-073.asp>
- Un article concernant la description technique de IPX/SPX :
<http://support.microsoft.com/support/kb/articles/q203/0/51.asp>

Gestion détaillée du document

12 octobre 2000 version initiale.