

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le protocole NBNS sous Windows NT et 2000

---

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-021>

---

### Gestion du document

Référence	CERTA-2000-AVI-021
Titre	Vulnérabilité dans le protocole NBNS sous Windows NT et 2000
Date de la première version	28 juillet 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 dans les services de noms sous NetBIOS.

## 2 Systèmes affectés

- Windows Workstation ;
- Windows NT 4.0 Server ;
- Windows NT 4.0 Server, Entreprise Edition ;
- Windows NT 4.0 Server, Terminal Server Edition ;
- Windows 2000.

## 3 Résumé

Le protocole NBNS (pour *NetBIOS Name Server*) fait partie de la famille des protocoles *NetBios over TCP/IP* (NBT). Il est implémenté pour le service WINS (*Windows Internet Name Server*) dans les systèmes Windows.

Une vulnérabilité y a été décelée. Elle permet à un individu mal intentionné d'empêcher à un serveur WINS de répondre à des requêtes provenant d'une machine possédant un nom donné.

## 4 Description

Par conception, le protocole NBNS entre en jeu dans la résolution des conflits de noms sous Windows. C'est aussi, par conception, un protocole sans authentification il est donc sujet à l'usurpation d'identité (*spoofing*).

Un individu mal intentionné peut, par manipulations des mécanismes de Conflit de Nom (*Name Conflict*) et Libération de Nom (*Name Release*), faire interpréter par une autre machine que son nom est en conflit. Selon le cas, cela peut avoir deux conséquences différentes :

- La machine ne peut plus enregistrer son nom sur le réseau
- La machine libèrera son nom, alors qu'elle avait déjà été enregistrée sous ce nom sur le réseau.

Dans les deux cas, elle ne répondra plus à des requêtes envoyées à ce nom.

## 5 Solution

Indépendamment de cette vulnérabilité, les packets UDP sur le port 137 provenant de l'extérieur du réseau (notamment internet) doivent être bloqués par un garde-barrière (ou *firewall*)

Microsoft distribue un correctif qui permet à l'administrateur de configurer une machine afin qu'elle n'accepte que des datagrammes de conflit de nom en réponse directe à des requêtes d'enregistrement de nom. Ce correctif permet aussi à l'administrateur de configurer ses machines pour qu'elle rejettent tous les datagrammes de libération de nom.

Le correctif pour Windows 2000 est à l'adresse suivante :

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=23370>

A ce jour, il n'y a pas de correctif pour Windows NT.

## 6 Documentation

- Le bulletin de Sécurité de Microsoft :  
<http://www.microsoft.com/technet/security/bulletin/ms00-047.asp>
- LA FAQ du bulletin de Sécurité de Microsoft :  
<http://www.microsoft.com/technet/security/bulletin/fq00-047.asp>
- les RFC :
  - 1001 : Protocol Standard for a NetBIOS Service on a TCP/UDP Transport : Concepts and Methods
  - 1002 : Protocol Standard for a NetBIOS Service on a TCP/UDP Transport : Detailed Specification
- La liste officielle de Microsoft contenant les mises à jour concernant la sécurité :  
[http://www.microsoft.com/downloads/default.asp?Search=Keyword&Value='security\\_patch'&OpSysID=1](http://www.microsoft.com/downloads/default.asp?Search=Keyword&Value='security_patch'&OpSysID=1)

## Gestion détaillée du document

28 juillet 2000 version initiale.