

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité NetBIOS sous Windows 9x, NT et 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-080>

Gestion du document

Référence	CERTA-2000-AVI-080
Titre	Vulnérabilité NetBIOS sous Windows 9x, NT et Me
Date de la première version	01 décembre 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

2 Systèmes affectés

- Microsoft Windows 9x ;
- Microsoft Windows Millenium Edition ;
- Microsoft NT 4 (Server, Terminal Server et Workstation).

3 Résumé

Un utilisateur mal intentionné peut, par le biais de paquets TCP/IP malformés, provoquer un déni de service sur une machine distante.

4 Description

Une vulnérabilité à été découverte dans les systèmes NT4, 95, 98, 98SE et ME dans l'exploitation du protocole NetBIOS.

Une succession de paquets TCP/IP malformés peut entraîner un blocage temporaire ou complet des fonctionnalités réseau de la machine cible obligeant son redémarrage.

Cette vulnérabilité ne peut être exploitée que si le port 139 (NetBios session - Partage de ressources) est ouvert sur la machine cible.

5 Contournement provisoire

Il est possible de bloquer l'exploitation de cette vulnérabilité depuis Internet en stoppant le trafic NetBIOS à la périphérie du réseau interne.

6 Solution

Correctif pour NT4 :

<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25114>

Solution pour Windows 95, 98 et Me :

Aucun correctif n'est proposé par Microsoft.

Il est uniquement recommandé de désactiver le partage de fichiers et d'imprimantes :

<http://www.microsoft.com/technet/support/kb.asp?ID=199346>

Bloquer les ports NetBIOS (135, 137 et 139) sur le pare-feu.

7 Documentation

Bulletin de sécurité Microsoft MS00-091 :

<http://www.microsoft.com/technet/security/bulletin/ms00-091.asp>

Faq Microsoft :

<http://www.microsoft.com/technet/security/bulletin/fq00-091.asp>

Gestion détaillée du document

01 décembre 2000 version initiale.