

Affaire suivie par :  
CERTA

## AVIS DU CERTA

**Objet : Vulnérabilité de Netmon sous Windows NT server et Windows 2000 server**

---

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-067>

---

### Gestion du document

Référence	CERTA-2000-AVI-067
Titre	Vulnérabilité de Netmon sous Windows NT server et Windows 2000 server
Date de la première version	02 novembre 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

- Exécution de code arbitraire avec privilèges administrateur;
- Déni de service.

## 2 Systèmes affectés

Windows NT server et 2000 server

## 3 Résumé

Plusieurs débordements de mémoire dans l'utilitaire *NetMon* permettent à un utilisateur mal intentionné de bloquer le système ou d'exécuter du code sur la machine sur laquelle l'administrateur utilise les fonctions d'analyse d'enregistrements de l'utilitaire *NetMon* sous windows NT server et 2000 server.

## 4 Description

NetMon est un utilitaire d'analyse réseau livré dans sa version de base avec les Système Windows NT 4.0 et 2000 servers, et dans une version un peu plus complète dans les versions 1.2 et 2.0 du logiciel SMS (*Systems Management Server*). Cet utilitaire comprend des fonctions d'analyse de protocole que l'administrateur peut effectuer sur une capture faite au préalable sur son réseau. Ces fonctions d'analyse sont sujettes à des débordements de mémoire. Un utilisateur mal intentionné peut avoir envoyé des trames habilement conçues pour soit bloquer le système, soit exécuter du code avec les privilèges de l'administrateur.

## 5 Solution

Appliquer le correctif de Microsoft :

- Pour Windows NT 4.0 Server et Enterprise Edition Service Pack 6a :  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25487>
- Pour Windows 2000 Server et Datacenter Server Gold ou Service Pack 1 :  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25485>
- Pour Windows NT 4.0 terminal Server Service Pack 6, correctif encore non disponible.
- Pour les systèmes ayant SMS 1.2 Service Pack 4, le correctif :  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25505>
- Pour SMS 2.0 gold, Service Pack 1 ou 2 :  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=25514>

## 6 Documentation

Bulletin de sécurité et FAQ de Microsoft :

<http://www.microsoft.com/technet/security/bulletin/ms00-083.asp>

<http://www.microsoft.com/technet/security/bulletin/fq00-083.asp>

## Gestion détaillée du document

02 novembre 2000 version initiale.