

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités des LPC sous Windows 2000 et NT

---

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-055>

---

### Gestion du document

Référence	CERTA-2000-AVI-055
Titre	Vulnérabilités des LPC sous Windows 2000 et NT
Date de la première version	04 octobre 2000
Date de la dernière version	–
Source(s)	Bulletin 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

- Accès aux privilèges de l'administrateur en local ;
- Déni de service.

## 2 Systèmes affectés

- Microsoft Windows NT 4.0 ;
- Windows 2000.

## 3 Résumé

Dans les systèmes d'exploitation Microsoft, les moyens de communication entre les processus élémentaires et les programmes d'une même machine sont fournis par les LPC (Local Procedure Call).

Plusieurs vulnérabilités ont été découvertes dans ces mécanismes :

- Deux vulnérabilités ouvrent un accès aux privilèges administrateur ;
- Deux vulnérabilités ouvrent un déni de service.

## **4 Description**

### **4.1 Accès aux privilèges l'administrateur en local**

Chaque processus possédant différents privilèges, un utilisateur mal intentionné peut leurrer, en modifiant ou en créant un processus, un processus privilégié afin de récupérer des droits d'accès supérieurs.

### **4.2 Déni de service**

Un utilisateur mal intentionné peut, par le biais de nombreuses requêtes LPC malformées, entraîner un déni de service de la machine locale par épuisement de la mémoire disponible.

### **4.3 Remarque**

Les LPC sont uniquement utilisées en local. De ce fait aucune exploitation de ces vulnérabilités ne peut être effectuée à distance.

## **5 Solution**

Correctif pour Windows NT 4.0 Workstation, Server et Server Entreprise Edition (VERSION US) :  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24650>

Nota : Les correctifs pour Windows NT4 Server et Terminal Server Edition ne sont pas disponibles.

Correctif pour Windows 2000 (VERSION US) :  
<http://www.microsoft.com/Downloads/Release.asp?ReleaseID=24649>

## **6 Documentation**

Bulletin de sécurité Microsoft :  
<http://www.microsoft.com/technet/security/bulletin/ms00-070.asp>

## **Gestion détaillée du document**

**04 octobre 2000** version initiale.