

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans le noyau Windows et LSASS

---

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-2004-AVI-395>

---

### Gestion du document

Référence	CERTA-2004-AVI-395
Titre	Vulnérabilité dans le noyau Windows et LSASS
Date de la première version	15 décembre 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité MS04-044 de 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

Elévation de privilèges.

## 2 Systèmes affectés

- Microsoft Windows NT Server 4.0 Service Pack 6a ;
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6 ;
- Microsoft Windows 2000 Service Pack 3 et Service Pack 4 ;
- Microsoft Windows XP 64-Bit Edition Service Pack 1 ;
- Microsoft Windows XP 64-Bit Edition Version 2003 ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 64-Bit Edition.

Les systèmes d'exploitation Microsoft Windows 98, Windows 98 SE et Windows Millenium Edition ne sont pas concernés par ces vulnérabilités.

### **3 Résumé**

Deux vulnérabilités sont présentes dans certaines versions de Microsoft Windows :

- Les LPC (Local Procedure Call) sont des systèmes de communication locaux inter-processus utilisés par les systèmes Windows. Une vulnérabilité de type débordement de mémoire a été découverte dans la mise en œuvre des LPC permettant à un individu local préalablement authentifié d'élever ses privilèges (vulnérabilité CVE CAN-2004-0893) ;
- une seconde vulnérabilité dans la validation des jetons d'identité utilisés par le service LSASS (Local Security Authority Subsystem Service) permet à un utilisateur local d'élever ses privilèges et de prendre possession du système (vulnérabilité CVE CAN-2004-0894).

### **4 Solution**

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

### **5 Documentation**

- Bulletin de sécurité Microsoft MS04-044 du 14 décembre 2004 :  
<http://www.microsoft.com/technet/security/bulletin/MS04-044.msp>
- Référence CVE CAN-2004-0893 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0893>
- Référence CVE CAN-2004-0894 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0894>

## **Gestion détaillée du document**

**15 décembre 2004** version initiale.