



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

**S . G . D . S . N**  
Agence nationale de la sécurité  
des systèmes d'information  
CERTA

Paris, le 14 avril 2004  
N° CERTA-2004-AVI-126

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités dans Microsoft Windows

---

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-126>

---

### Gestion du document

Référence	CERTA-2004-AVI-126
Titre	Multiples vulnérabilités dans Microsoft Windows
Date de la première version	14 avril 2004
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS04-011
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 à distance ;
- Elévation de privilèges ;
- Déni de service.

## 2 Systèmes affectés

- Microsoft Windows NT Workstation 4.0 Service Pack 6a ;
- Microsoft Windows NT Server 4.0 Service Pack 6a ;
- Microsoft Windows NT Server 4.0 Terminal Server Edition Service Pack 6.0 ;
- Microsoft Windows 2000 Service Pack 2 à 4 ;
- Microsoft Windows XP et Microsoft Windows XP Service Pack 1 ;
- Microsoft Windows XP 64-Bit Edition Service Pack 1 ;
- Microsoft Windows XP 64-Bit Edition Version 2003 ;
- Microsoft Windows Server 2003 ;
- Microsoft NetMeeting ;
- Microsoft Windows 98, 98SE, ME.

### 3 Résumé

Microsoft a publié des correctifs pour 14 vulnérabilités affectant les systèmes d'exploitation Windows.

### 4 Description

- Une vulnérabilité dans le service LSASS (Local Security Authority Subsystem Service) permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur la machine cible.
- Une vulnérabilité dans le service LDAP (Lightweight Directory Access Protocol) permet de réaliser à distance un déni de service.
- Une vulnérabilité dans le protocole PCT (Private Communication Transport) permet à un attaquant distant de réaliser une élévation de privilèges prenant ainsi le contrôle de la machine cible.
- Une vulnérabilité dans WinLogon (Windows Logon Process) permet de d'exécuter du code arbitraire à distance et une élévation de privilèges.
- Une vulnérabilité dans les informations de fichiers d'images de type Metafile (WMF et EMF) rend possible l'exécution de code arbitraire et la prise de contrôle de la machine cible à distance.
- Une vulnérabilité dans le protocole d'aide HSC (Help and Support Center) permet, à distance, l'exécution de code arbitraire ainsi que la prise de contrôle de la machine cible par élévation de privilèges.
- Une vulnérabilité de Utility Manager permet à un utilisateur possédant un compte sur la machine cible de lancer des applications avec les privilèges system.
- Une vulnérabilité de Windows Management permet à un utilisateur possédant un compte sur une machine Microsoft Windows XP d'exécuter des programmes avec les privilèges system.
- Une vulnérabilité de LDT (Local Descriptor Table) permet de réaliser une élévation de privilèges sur la machine cible.
- Une vulnérabilité dans le protocole H. 323 permet, par l'envoi de paquets judicieusement composés, d'exécuter du code arbitraire sur la machine cible avec les privilèges system.
- Une vulnérabilité de la machine virtuelle MS-DOS (VDM) permet à un utilisateur possédant un compte sur la machine vulnérable de réaliser une élévation de privilèges.
- Une vulnérabilité dans l'interface Negotiate SSP (Negotiate Security Support) permet à un utilisateur distant mal intentionné de prendre le contrôle de la machine cible par élévation de privilèges.
- Une vulnérabilité dans la bibliothèque SSL (Microsoft Secure Sockets Layer) permet à un utilisateur distant de réaliser un déni de service.
- Une vulnérabilité de la bibliothèque ASN.1 permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire sur la machine cible.

### 5 Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs :  
<http://www.microsoft.com/technet/security/bulletin/MS04-011.msp>

### 6 Documentation

Références CVE :

- LSASS Vulnerability - CAN-2003-0533 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0533>
- LDAP Vulnerability - CAN-2003-0663 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0663>
- PCT Vulnerability - CAN-2003-0719 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0719>
- Winlogon Vulnerability - CAN-2003-0806 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0806>
- Metafile Vulnerability - CAN-2003-0906 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0906>

- Help and Support Center Vulnerability - CAN-2003-0907 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0907>
- Utility Manager Vulnerability - CAN-2003-0908 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0908>
- Windows Management Vulnerability - CAN-2003-0909 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0909>
- Local Descriptor Table Vulnerability - CAN-2003-0910 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0910>
- H.323 Vulnerability - CAN-2004-0117 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0117>
- Virtual DOS Machine Vulnerability - CAN-2004-0118 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0118>
- Negotiate SSP Vulnerability - CAN-2004-0119 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0119>
- SSL Vulnerability - CAN-2004-0120 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0120>
- ASN.1 Vulnerability - CAN-2004-0123 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0123>

## **Gestion détaillée du document**

**14 avril 2004** version initiale.