

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans LSASS de 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-2008-AVI-010>

---

### Gestion du document

Référence	CERTA-2008-AVI-010
Titre	Vulnérabilité dans LSASS de Windows
Date de la première version	09 janvier 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-002 du 08 janvier 2008
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 ;
- Elévation de privilèges ;
- contournement de la politique de sécurité.

## 2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Windows XP Service Pack 2 ;
- Windows XP Professional x64 Edition ;
- Windows XP Professional x64 Edition Service Pack 2 ;
- Windows Server 2003 Service Pack 1 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 x64 Edition ;
- Windows Server 2003 x64 Edition Service Pack 2 ;
- Windows Server 2003 pour systèmes Itanium (SP1 et SP2).

### **3 Résumé**

Le service LSASS de Microsoft Windows (*Local Security Authority Subsystem Service*) ne manipulerait pas correctement certaines requêtes d'appel LPC (*Local Procedure Call*). Un utilisateur local pourrait ainsi profiter de cette vulnérabilité pour élever ses privilèges et exécuter du code avec des droits plus élevés que ceux qui lui ont été attribués.

### **4 Description**

Le service LSASS de Microsoft Windows (*Local Security Authority Subsystem Service*) ne manipulerait pas correctement certaines requêtes d'appel LPC (*Local Procedure Call*). Un utilisateur local pourrait ainsi profiter de cette vulnérabilité pour élever ses privilèges et exécuter du code avec des droits plus élevés que ceux qui lui ont été attribués.

### **5 Solution**

Se référer au bulletin de sécurité MS08-002 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

### **6 Documentation**

- Bulletin de sécurité Microsoft MS08-002 du 08 janvier 2008 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-002.mspix>  
<http://www.microsoft.com/technet/security/Bulletin/MS08-002.mspix>
- Référence CVE CVE-2007-5352 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5352>

### **Gestion détaillée du document**

**09 janvier 2008** version initiale.