



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 15 octobre 2008  
N° CERTA-2008-AVI-505

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans la gestion mémoire 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-505>

---

### Gestion du document

Référence	CERTA-2008-AVI-505
Titre	Vulnérabilité dans la manipulation mémoire Windows
Date de la première version	15 octobre 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-064 du 14 octobre 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

- Contournement de la politique de sécurité ;
- élévation de privilèges.

## 2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Service Pack 3 ;
- Microsoft XP Professional x64 Edition ;
- Microsoft XP Professional x64 Edition Service Pack 2 ;
- Windows Vista ;
- Windows Vista Service Pack 1 ;
- Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 Service Pack 2 ;
- Microsoft Windows Server 2003 x64 Edition ;
- Microsoft Windows Server 2003 x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 SP1 et SP2 pour systèmes Itanium ;
- Microsoft Windows Server 2008 (systèmes 32-bit et x64, y compris pour systèmes Itanium).

### **3 Résumé**

Une vulnérabilité a été identifiée dans le gestionnaire de mémoire Windows, et en particulier dans la gestion des descripteurs d'adresses virtuelles (VAD). Cette vulnérabilité peut être exploitée par une personne locale afin d'élever ses privilèges.

### **4 Description**

Une vulnérabilité a été identifiée dans le gestionnaire de mémoire Windows, et en particulier dans la gestion des descripteurs d'adresses virtuelles (VAD) utilisés pour représenter l'espace d'adressage mémoire d'un processus.

Cette vulnérabilité peut être exploitée par une personne locale afin d'élever ses privilèges à ceux d'administrateur du système.

### **5 Solution**

Se référer au bulletin de sécurité MS08-064 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

### **6 Documentation**

- Bulletin de sécurité Microsoft MS08-064 du 14 octobre 2008 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-064.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS08-064.msp>
- Référence CVE CVE-2008-4036 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4036>

### **Gestion détaillée du document**

**15 octobre 2008** version initiale.