



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 13 juin 2007  
N° CERTA-2007-AVI-258

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans l'API Win32

---

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-2007-AVI-258>

---

### Gestion du document

Référence	CERTA-2007-AVI-258
Titre	Vulnérabilité dans l'API Win32
Date de la première version	13 juin 2007
Date de la dernière version	–
Source(s)	
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.

## 2 Systèmes affectés

- Windows 2000 Service Pack 4 ;
- Windows XP Service Pack 2 ;
- Windows XP Professionnel Édition x64 ;
- Windows XP Professionnel Édition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 1 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Édition x64 ;
- Windows Server 2003 Édition x64 Service Pack 2 ;
- Windows Server 2003 avec SP1 pour les systèmes Itanium ;
- Windows Server 2003 avec SP2 pour les systèmes Itanium.

### **3 Résumé**

Cette mise à jour de sécurité corrige une vulnérabilité critique en modifiant la façon dont l'API Win32 valide des paramètres.

### **4 Description**

Il existe une vulnérabilité d'exécution de code arbitraire à distance dans la façon dont l'API Win32 valide certains paramètres. Un attaquant pourrait exploiter cette vulnérabilité en créant une page Web qui pourrait permettre l'exécution de code à distance si un utilisateur la consultait. Tout attaquant qui parviendrait à exploiter cette vulnérabilité pourrait prendre le contrôle intégral du système affecté.

### **5 Contournement provisoire**

### **6 Solution**

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

### **7 Documentation**

- Bulletin de sécurité Microsoft MS07-035 du 13 juin 2007 :  
<http://www.microsoft.com/france/technet/securite/MS07-035.mspx>  
<http://www.microsoft.com/technet/security/Bulletin/MS07-035.mspx>
- Référence CVE:  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2219>

### **Gestion détaillée du document**

**13 juin 2007** version initiale.