



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-261

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Microsoft Schannel

---

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-261>

---

### Gestion du document

|                             |   |
|-----------------------------|---|
| Référence                   | CERTA-2007-AVI-261                                      |
| Titre                       | Vulnérabilité dans Microsoft Schannel                   |
| Date de la première version | 13 juin 2007  |
| Date de la dernière version | –   |
| Source(s)                   | Bulletin de sécurité Microsoft MS07-031 du 13 juin 2007 |
| 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 ;
- déni de service à distance.

## 2 Systèmes affectés

- Windows 2000 Service Pack 4 ;
- Windows XP Service Pack 2 ;
- Windows XP Professionnel édition x64 ;
- Windows Server 2003 Service Pack 1 et Service Pack 2 ;
- Windows Server 2003 (édition x64 et Itanium) Service Pack 1 et Service Pack 2 ;

## 3 Résumé

Une vulnérabilité dans Microsoft Schannel permet l'exécution de code arbitraire ou d'un déni de service à distance.

## 4 Description

Le composant Schannel implémente les protocoles d'authentification SSL (*Secure Sockets Layer*) et TLS (*Transport Layer Security*). Cette vulnérabilité qualifiée de critique par Microsoft permet à une personne distante malintentionnée d'exécuter du code arbitraire ou de réaliser un déni de service par le biais d'une page web spécialement conçue.

## 5 Solution

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

## 6 Documentation

- Bulletin de sécurité Microsoft MS07-031 du 13 juin 2007 :  
<http://www.microsoft.com/france/technet/securite/MS07-031.mspx>  
<http://www.microsoft.com/technet/security/Bulletin/MS07-031.mspx>
- Référence CVE CVE-2007-2218 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-2218>

## Gestion détaillée du document

**13 juin 2007** version initiale.