

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilités dans le noyau 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-2009-AVI-220>

---

### Gestion du document

Référence	CERTA-2009-AVI-220
Titre	Vulnérabilités dans le noyau Windows
Date de la première version	10 juin 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-025 du 09 juin 2009
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

Élévation de privilèges.

## 2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 et Service Pack 3 ;
- Microsoft Windows XP Professional x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 2 ;
- Microsoft Windows Server 2003 x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2003 pour systèmes Itanium Service Pack 2 ;
- Microsoft Windows Vista ;
- Microsoft Windows Vista Service Pack 1 ;
- Microsoft Windows Vista Service Pack 2 ;
- Microsoft Windows Vista x64 Edition ;
- Microsoft Windows Vista x64 Edition Service Pack 1 ;
- Microsoft Windows Vista x64 Edition Service Pack 2 ;
- Microsoft Windows Server 2008 pour systèmes 32 bits ;

- *Microsoft Windows Server 2008* pour systèmes 32 bits Service Pack 2 ;
- *Microsoft Windows Server 2008* pour systèmes x64 ;
- *Microsoft Windows Server 2008* pour systèmes x64 Service Pack 2 ;
- *Microsoft Windows Server 2008* pour systèmes Itanium ;
- *Microsoft Windows Server 2008* pour systèmes Itanium Service Pack 2.

### 3 Résumé

Quatre vulnérabilités dans le noyau de *Microsoft Windows* permettent une élévation de privilèges.

### 4 Description

Quatre vulnérabilités ont été découvertes dans le noyau de *Microsoft Windows* :

- les modifications dans certains objets du noyau ne sont pas correctement validées (CVE-2009-1123) ;
- les pointeurs transmis depuis le mode utilisateur ne sont pas suffisamment vérifiés (CVE-2009-1124) ;
- les arguments passés à un appel système spécifique ne sont pas correctement contrôlés (CVE-2009-1125) ;
- les arguments transmis au noyau depuis le mode utilisateur sont mal validés (CVE-2009-1126).

L'exploitation de ces vulnérabilités permet une élévation de privilèges.

### 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 MS09-025 du 09 juin 2009 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-025.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS09-025.msp>
- Référence CVE CVE-2009-1123 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1123>
- Référence CVE CVE-2009-1124 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1124>
- Référence CVE CVE-2009-1125 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1125>
- Référence CVE CVE-2009-1126 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1126>

## Gestion détaillée du document

**10 juin 2009** version initiale.