

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Multiples vulnérabilités des systèmes Microsoft 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-2005-AVI-138>

---

### Gestion du document

Référence	CERTA-2005-AVI-138
Titre	Multiples vulnérabilités des systèmes Microsoft Windows
Date de la première version	13 avril 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-018 du 12 avril 2005
Pièce(s) jointe(s)	

TAB. 1 – Gestion du document

Une gestion de version détaillée se trouve à la fin de ce document.

## 1 Risque

- Elévation de privilèges ;
- déni de service.

## 2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 3 & 4 ;
- Microsoft Windows XP Service Pack 1 & 2 ;
- Microsoft Windows XP 64-bit Edition Service Pack 1 (Itanium) ;
- Microsoft Windows XP 64-bit Edition Version 2003 (Itanium) ;
- Microsoft Windows Server 2003 ;
- Microsoft Windows Server 2003 pour systèmes Itanium ;
- Microsoft Windows 98 et 98 Second Edition.

## 3 Résumé

De nombreuses vulnérabilités découvertes dans le noyau Windows de Microsoft permettent à un utilisateur mal intentionné d'élever ses privilèges ou d'effectuer un déni de service sur le système vulnérable.

## 4 Description

- CAN-2005-0060 : une vulnérabilité présente lors de la manipulation des polices de caractères permet à un utilisateur local d'élever ses privilèges afin d'obtenir les droits de l'administrateur ;
- CAN-2005-0061 & CAN-2005-0550 : deux vulnérabilités du noyau permettent à un utilisateur local mal intentionné d'élever ses privilèges afin d'obtenir les droits de l'administrateur (CAN-2005-0061) ou d'effectuer un déni de service de figer le système et de le forcer à redémarrer automatiquement (CAN-2005-0550) ;
- CAN-2005-0551 : une vulnérabilité présente dans le sous-système win32 (CSRSS.exe) permet à un utilisateur local d'élever ses 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 de Microsoft MS05-018 du 12 avril 2005:  
<http://www.microsoft.com/technet/security/bulletin/MS05-018.mspx>
- Référence CVE CAN-2004-0060 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0060>
- Référence CVE CAN-2004-0061 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0061>
- Référence CVE CAN-2004-0550 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0550>
- Référence CVE CAN-2004-0551 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2004-0551>

## Gestion détaillée du document

13 avril 2005 version initiale.