

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité du service Kerberos de Microsoft

---

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-305>

---

### Gestion du document

Référence	CERTA-2005-AVI-305
Titre	Multiples vulnérabilités du service Kerberos de Microsoft
Date de la première version	10 août 2005
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS05-042 du 09 août 2005
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

- Déni de service ;
- atteinte à la confidentialité des données.

## 2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 1 et Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professional x64 Edition ;
- Microsoft Windows Server 2003 et Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 (systèmes Itanium) et Microsoft Windows Server 2003 Service Pack 1 (systèmes Itanium) ;
- Microsoft Windows Server 2003 x64 Edition.

## 3 Résumé

De multiples vulnérabilités présentes dans le service Kerberos de Microsoft Windows permettent à un utilisateur mal intentionné de provoquer un déni de service ou de porter atteinte à la confidentialité des données de la machine vulnérable.

## 4 Description

Le service Kerberos de Windows présente deux vulnérabilités :

- La première vulnérabilité (CAN-2005-1981) permet à un utilisateur mal intentionné du réseau local de provoquer un déni de service sur le système d'authentification des utilisateurs d'un contrôleur de domaine par le biais d'un message malicieusement construit.
- La deuxième vulnérabilité (CAN-2005-1982) permet à un utilisateur mal intentionné du réseau local de porter atteinte à la confidentialité des données en substituant un contrôleur de domaine par son propre serveur.

## 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 MS05-042 du 09 août 2005 :  
<http://www.microsoft.com/technet/security/Bulletin/MS05-042.msp>
- Référence CVE CAN-2005-1981 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1981>
- Référence CVE CAN-2005-1982 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1982>

## Gestion détaillée du document

10 août 2005 version initiale.