



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 09 février 2011  
N° CERTA-2011-AVI-060

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Active Directory

---

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-2011-AVI-060>

---

### Gestion du document

Référence	CERTA-2011-AVI-060
Titre	Vulnérabilité dans Active Directory
Date de la première version	09 février 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-005 du 8 février 2011
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 à distance.

## 2 Systèmes affectés

- Windows Server 2003 SP 2 ;
- Windows Server 2003 x64 SP2 ;
- Windows Server 2003 IA64 SP2.

## 3 Résumé

Une vulnérabilité dans Microsoft Windows Active Directory peut être exploitée par une personne malveillante pour provoquer un déni de service à distance.

## 4 Description

Une vulnérabilité a été corrigée dans Microsoft Windows Active Directory. Cette vulnérabilité est due à une mauvaise validation des noms du service principal (SPN). Cette vulnérabilité peut être exploitée par une personne malveillante pour provoquer un déni de service à distance.

## **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 MS11-005 du 08 février 2011 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-005.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS11-005.msp>
- Référence CVE CVE-2011-0040 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0040>

## **Gestion détaillée du document**

**09 février 2011** version initiale.