



Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE  
PREMIER MINISTRE

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

Paris, le 10 novembre 2009  
N° CERTA-2009-AVI-493

Affaire suivie par :  
CERTA

## AVIS DU CERTA

### Objet : Vulnérabilité dans Microsoft 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-2009-AVI-493>

---

### Gestion du document

Référence	CERTA-2009-AVI-493
Titre	Vulnérabilité dans Microsoft Active Directory
Date de la première version	10 novembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-066 du 10 novembre 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

Déni de service à distance.

## 2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Windows XP Service Pack 2 et 3 ;
- Windows XP Professionel Édition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 ;
- Windows Server 2003 Édition x64 Service Pack 2 ;
- Windows Server 2003 Service Pack 2 pour systèmes Itanium ;
- Windows Server 2008 pour systèmes 32 bits et Windows Server 2008 pour systèmes 32 bits Service Pack 2 ;
- Windows Server 2008 pour systèmes x64 et Windows Server 2008 pour systèmes x64 Service Pack 2.

## 3 Résumé

Une vulnérabilité dans Microsoft Active Directory permet à une personne malintentionnée de provoquer un déni de service à distance.

## 4 Description

Une erreur dans la gestion de la pile permet à une personne distante malintentionnée de provoquer un déni de service de Microsoft Active Directory lors de l'exécution de certaines requêtes *LDAP* ou *LDAPS*. Cette vulnérabilité n'affecte que les contrôleurs de domaine exécutant Active Directory Application Mode (*ADAM*) ou Active Directory Lightweight Directory Service (*AD LDS*).

## 5 Solution

Se référer au bulletin de sécurité Microsoft MS09-066 pour l'obtention des correctifs (cf. section Documentation).

## 6 Documentation

- Bulletin de sécurité Microsoft MS09-066 du 10 novembre 2009 :  
<http://www.microsoft.com/france/technet/security/Bulletin/MS09-066.msp>  
<http://www.microsoft.com/technet/security/Bulletin/MS09-066.msp>
- Référence CVE CVE-2009-1928 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1928>

## Gestion détaillée du document

**10 novembre 2009** version initiale.