



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 novembre 2011  
N° CERTA-2011-AVI-624

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-2011-AVI-624>

---

### Gestion du document

Référence	CERTA-2011-AVI-624
Titre	Vulnérabilité dans Microsoft Active Directory
Date de la première version	09 novembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-086 du 08 novembre 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

- Contournement de la politique de sécurité ;
- élévation de privilèges.

## 2 Systèmes affectés

- Active Directory en mode application (ADAM), Windows XP Service Pack 3 ;
- ADAM, Windows XP Édition Professionnelle x64 Service Pack 2 ;
- Active Directory et ADAM, Windows Server 2003 Service Pack 2 ;
- Active Directory et ADAM, Windows Server 2003 Édition x64 Service Pack 2 ;
- Active Directory, Windows Server 2003 avec Service Pack 2 pour systèmes Itanium ;
- Active Directory Lightweight Directory Service (AD LDS), Windows Vista Service pack 2 ;
- AD LDS, Windows Vista Édition x64 Service Pack 2 ;
- Active Directory et AD LDS, Windows Server 2008 32 bits et Windows Server 2008 32 bits Service Pack 2 ;
- Active Directory et AD LDS, Windows Server 2008 système x64 et Windows Server 2008 x64 Service Pack 2 ;
- AD LDS, Windows 7 pour systèmes 32 bits ;

- AD LDS, Windows 7 pour systèmes x64 ;
- Active Directory et AD LDS, Windows Server 2008 R2 pour systèmes x64.

### **3 Résumé**

Une vulnérabilité dans *Active Directory* permet de contourner la politique de sécurité et d'élèver ses privilèges.

### **4 Description**

Une vulnérabilité existe dans *Active Directory* lorsque *LDAPS (LDAP sur SSL)* est utilisé. Un attaquant, ayant en sa possession un certificat expiré, peut utiliser celui-ci pour s'authentifier sur le domaine avec les privilèges du compte associé.

### **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 MS11-086 du 08 novembre 2011 :  
<http://technet.microsoft.com/fr-fr/security/bulletin/MS11-086>  
<http://technet.microsoft.com/en-us/security/bulletin/MS11-086>
- Référence CVE CVE-2011-2014 :  
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2014>

## **Gestion détaillée du document**

**09 novembre 2011** version initiale.