

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-2008-AVI-079>

Gestion du document

Référence	CERTA-2008-AVI-079
Titre	Vulnérabilité dans Microsoft Active Directory
Date de la première version	13 février 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-003 du 12 février 2008
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 ;
- contournement de la politique de sécurité.

2 Systèmes affectés

- Windows 2000 Service Pack 4 ;
- Windows XP Professional Service Pack 2 ;
- Windows XP Professional Edition x64 (SP2 compris) ;
- Windows Server 2003 Service Pack 1 et Service Pack 2 ;
- Windows Server 2003 Edition x64 (SP2 compris) ;
- Windows Server 2003 pour les systèmes Itanium (SP1 et SP2).

3 Résumé

Une vulnérabilité a été identifiée dans la mise en oeuvre d'Active Directory sur des systèmes d'exploitation Microsoft Windows. Elle existe également pour Active Directory en mode application (ADAM). Elle permettrait à une personne malveillante distante d'empêcher le système de répondre et de redémarrer.

4 Description

Une vulnérabilité a été identifiée dans la mise en oeuvre d'Active Directory sur des systèmes d'exploitation Microsoft Windows. Il s'agit des services d'autorisation et d'authentification centralisés sous Windows. En mode application, ou ADAM, le service est un LDAP (*Lightweight Directory Access Protocol*). Il serait également vulnérable.

Le service ne gère pas correctement certaines requêtes LDAP. Cette vulnérabilité peut être exploitée par une personne distante sous certaines conditions pour perturber le système, comme l'empêcher de répondre ou le redémarrer.

5 Solution

Se référer au bulletin de sécurité MS08-003 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-003 du 12 février 2008 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS08-003.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS08-003.msp>
- Référence CVE CVE-2008-0088 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0088>

Gestion détaillée du document

13 février 2008 version initiale.