



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 15 septembre 2010
N° CERTA-2010-AVI-437

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-2010-AVI-437>

Gestion du document

Référence	CERTA-2010-AVI-437
Titre	Vulnérabilité dans Microsoft Active Directory
Date de la première version	15 septembre 2010
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS10-068 du 14 septembre 2010
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

- Élévation de privilèges ;
- exécution de code arbitraire à distance.

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 *Microsoft Active Directory* permet à un attaquant d'exécuter du code arbitraire à distance avec des privilèges élevés.

4 Description

Une erreur dans le traitement des messages LDAP (*Lightweight Directory Access protocol*) par LSASS (*Local Security Authority Subsystem Service*), permet à un attaquant, authentifié auprès du serveur LSASS, qui exploiterait cette vulnérabilité, d'élever son niveau de privilèges et d'exécuter du code arbitraire 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 MS10-068 du 14 septembre 2010 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS10-068.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS10-068.msp>
- Référence CVE CVE-2010-0820 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0820>

Gestion détaillée du document

15 septembre 2010 version initiale.