

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilités de 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-2007-AVI-294>

Gestion du document

Référence	CERTA-2007-AVI-294
Titre	Vulnérabilités de Microsoft Active Directory
Date de la première version	11 juillet 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-039 du 10 juillet 2007
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

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

3 Description

Deux vulnérabilités ont été identifiées dans le service d'annuaire Active Directory de Microsoft. Il permet de représenter et de stocker différentes informations constituant le réseau, sous une forme hiérarchisée d'objets.

Les deux vulnérabilités concernent la validation de requêtes du protocole LDAP (pour *Lightweight Directory Access Protocol*) permettant d'accéder à cet annuaire. Le service LDAP ne vérifierait pas suffisamment le nombre

d'attributs pouvant être convertis qui sont inclus dans la requête. Une personne malveillante distante pourrait ainsi profiter de cette vulnérabilité pour envoyer un tel paquet spécialement construit, afin de perturber le service ou de prendre le contrôle complet du système.

Les ports pouvant être ciblés pour exploiter ces deux vulnérabilités sont avant tout 389/TCP et 3268/TCP, utilisés par défaut pour initier une connexion.

4 Solution

Se référer au bulletin de sécurité MS07-039 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

5 Documentation

- Bulletin de sécurité Microsoft MS07-039 du 10 juillet 2007 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS07-039.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS07-039.msp>
- Référence CVE CVE-2007-0040 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0040>
- Référence CVE CVE-2007-3028 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3028>

Gestion détaillée du document

11 juillet 2007 version initiale.