

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans les services de certificats Active Directory de Microsoft Windows

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-359>

Gestion du document

Référence	CERTA-2011-AVI-359
Titre	Vulnérabilité dans les services de certificats Active Directory de Microsoft Windows
Date de la première version	15 juin 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS11-051 du 14 juin 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

Injection de code indirecte à distance.

2 Systèmes affectés

- Windows Server 2003 pour systèmes 32 bits Service Pack 2 ;
- Windows Server 2003 pour systèmes x64 Service Pack 2 ;
- 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 ;
- Windows Server 2008 R2 pour systèmes x64 et Windows Server 2008 R2 pour systèmes x64 Service Pack 1.

3 Résumé

Une vulnérabilité dans les serveurs Microsoft peut être exploitée pour réaliser une injection de code indirecte à distance.

4 Description

Une vulnérabilité dans les services de certificats Active Directory des serveurs Microsoft peut être exploitée pour réaliser une injection de code indirecte à distance. Il est possible pour un attaquant, en poussant un utilisateur à ouvrir un lien spécialement conçu, d'exécuter des commandes arbitraires avec les privilèges de l'utilisateur.

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 MS11-051 du 14 juin 2011 :
<http://www.microsoft.com/france/technet/security/Bulletin/MS11-051.msp>
<http://www.microsoft.com/technet/security/Bulletin/MS11-051.msp>
- Référence CVE CVE-2011-1264 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1264>

Gestion détaillée du document

15 juin 2011 version initiale.