Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 14 novembre 2007
N° CERTA-2007-AVI-490

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du serveur DNS de Microsoft Windows

Gestion du document

Référence	CERTA-2007-AVI-490
Titre	Vulnérabilité du serveur DNS de Microsoft Windows
Date de la première version	14 novembre 2007
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS07-062 du 13 novembre 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

Contournement de la politique de sécurité.

2 Systèmes affectés

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

3 Résumé

Une vulnérabilité a été identifiée dans la génération des identifiants de transaction DNS. Cette dernière pourrait être exploitée par une personne malveillante pour répondre à une requête DNS d'un système vulnérable, afin de rediriger la victime vers une autre adresse que celle retournée par le serveur DNS légitime.

4 Description

Une vulnérabilité a été identifiée dans la méthode de génération des identifiants de transaction DNS. Ce procédé n'est pas complètement aléatoire, et pourrait permettre à une personne malveillante de prédire certaines valeurs de ces identifiants.

Cette personne pourrait alors utiliser un outil cherchant à répondre à une requête DNS d'un système vulnérable, afin de rediriger la victime vers une autre adresse (IP) que celle retournée par le serveur DNS légitime. Cette nouvelle adresse peut correspondre à un site de *phishing* ou contenant des codes malveillants par exemple.

5 Solution

Se référer au bulletin de sécurité MS07-062 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS07-062 du 13 novembre 2007 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS07-062.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS07-062.mspx
- Référence CVE CVE-2007-3898 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-3898

Gestion détaillée du document

14 novembre 2007 version initiale.