Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 09 avril 2008
N° CERTA-2008-AVI-191

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité du client DNS de Microsoft Windows

Gestion du document

Référence	CERTA-2008-AVI-191
Titre	Vulnérabilité du client DNS de Microsoft Windows
Date de la première version	09 avril 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-020 du 08 avril 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 ;
- atteinte à la confidentialité des données.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Professionnel Édition x64 ;
- Microsoft Windows XP Professionnel Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2003 Service Pack 1 ;
- Microsoft Windows Server 2003 Service Pack 2 ;
- Microsoft Windows Server 2003 Édition x64 ;
- Microsoft Windows Server 2003 Édition x64 Service Pack 2 ;
- Microsoft Windows Server 2003 avec SP1 pour les systèmes Itanium ;
- Microsoft Windows Server 2003 avec SP2 pour les systèmes Itanium ;
- Microsoft Windows Vista ;
- Microsoft Windows Vista Édition x64.

3 Résumé

Une vulnérabilité a été identifiée dans le client DNS de Microsoft Windows. Elle permettrait à une personne malveillante d'usurper une réponse DNS légitime, afin de tromper le système et l'amener à contacter une machine non légitime.

4 Description

Une vulnérabilité a été identifiée dans le client DNS de Microsoft Windows. Il s'agit du client en charge de la résolution des noms de machines en adresses IP.

La vulnérabilité permettrait à une personne malveillante d'usurper une réponse DNS légitime en prédisant les valeurs de transaction du client.

Cette mauvaise réponse serait alors interprétée sur le système vulnérable qui pourrait rediger une partie de son trafic vers une adresse IP non légitime.

5 Solution

Se référer au bulletin de sécurité MS08-020 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-020 du 08 avril 2008 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS08-020.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS08-020.mspx
- Référence CVE CVE-2008-0087 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0087

Gestion détaillée du document

09 avril 2008 version initiale.