Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 20 septembre 2001
N° CERTA-2001-AVI-096

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Serveurs DNS Microsoft : corruption de cache possible.

Gestion du document

Référence	CERTA-2001-AVI-096
Titre	Serveurs DNS Microsoft : corruption de cache possible.
Date de la première version	20 septembre 2001
Date de la dernière version	–
Source(s)	Note d'incident IN-2001-11 du CERT/CC
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;
- Usurpation d'identité.

2 Systèmes affectés

- Microsoft Windows NT Server version 4.0;
- Microsoft Windows 2000 Datacenter Server;
- Microsoft Windows 2000 Advanced Server;
- Microsoft Windows 2000 Server.

3 Résumé

Un mauvais paramétrage par défaut des serveurs DNS sous Windows NT et Windows 2000 permet à un utilisateur mal intentionné de corrompre le cache des serveurs DNS au moyen d'informations erronées renvoyées par un serveur DNS hostile.

4 Description

Le DNS (Domain Name System) est un mécanisme utilisé pour la résolution de nom de machines (exemple : www.certa.ssi.gouv.fr) en adresse IP et vice-versa.

Un utilisateur mal intentionné peut configurer un serveur hostile pour renvoyer des informations erronées à des serveurs DNS vulnérables. Ces informations erronées permettront alors de substituer une adresse illégitime à une adresse légitime.

Par ce biais, il est ainsi possible de provoquer un déni de service en renvoyant une erreur ou de rediriger le trafic vers un site hostile à l'insu de l'utilisateur. Le site hostile peut alors intercepter, modifier ou falsifier des informations.

5 Solution

Un article de la base de connaissances Microsoft indique le paramétrage permettant de prévenir la corruption du cache DNS :

http://support.microsoft.com/support/kb/articles/Q241/3/52.ASP

6 Documentation

Note d'incident IN-2001-11 du CERT/CC :
http://www.cert.org/incident_notes/IN-2001-11.html

Gestion détaillée du document

20 septembre 2001 version initiale.