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 mai 2007
N° CERTA-2007-ALE-010-002

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité de Microsoft DNS Server

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-ALE-010`

Gestion du document

Référence	CERTA-2007-ALE-010-002
Titre	Vulnérabilité de Microsoft DNS Server
Date de la première version	16 avril 2007
Date de la dernière version	09 mai 2007
Source(s)	Avis de sécurité Microsoft 935964 du 12 avril 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 Service Pack 4 ;
– Microsoft Windows Server 2003 Service Pack 1 ;
– Microsoft Windows Server 2003 Service Pack 2.

3 Résumé

Une vulnérabilité a été identifiée dans Microsoft DNS Server. Un débordement de tampon est possible via l'interface `RPC` (pour *Remote Procedure Call*). Cette vulnérabilité permet d'exécuter du code arbitraire à distance avec les droits de l'utilisateur local `SYSTEM`.

4 Description

Une vulnérabilité a été identifiée dans Microsoft DNS Server. Un débordement de tampon est possible via des appels `RPC` (pour *Remote Procedure Call*). Cette vulnérabilité permet d'exécuter du code arbitraire à distance avec les droits de l'utilisateur local `SYSTEM`.

Elle peut être exploitée via les ports `RPC`, de 1024 à 5000 (TCP ou UDP) ou, par un utilisateur authentifié, via les ports 445/TCP et 139/TCP.

Le trafic des serveurs DNS devrait être limité aux ports dédiés, i.e. 53 TCP/UDP. Cependant, dans de nombreux cas, les serveurs DNS Microsoft sont utilisés dans les réseaux locaux, et cumulent d'autres services (FTP, HTTP, etc.). Ils peuvent aussi être installés par défaut avec un Active Directory. Tout ceci contribue à rendre le filtrage de ces machines difficiles à maîtriser.

Des codes d'exploitation sont actuellement largement diffusés sur l'Internet. Cette vulnérabilité a été évoquée dans le bulletin d'actualité CERTA-2007-ACT-015.

L'avis CERTA-2007-AVI-209 sorti le 09 mai 2007 signale la publication de correctifs détaillés dans le bulletin de sécurité Microsoft MS07-029.

5 Contournement provisoire

Quelques contournements sont possibles pour limiter les risques :

1° Modifier dans la clé de registre suivante

```
HKLM\SYSTEM\CurrentControlSetService\Services\DNS\Parameters
```

la valeur du paramètre `RpcProtocol` :

- la valeur 4 permet d'interdire la gestion et la configuration distante du serveur DNS par RPC ou WMI. Cependant, cela est toujours possible localement, ou par un accès Terminal Serveur.
- la valeur 0 désactive toute possibilité de gestion DNS par RPC (administration locale et configuration). Ce choix est donc fortement recommandé dans la mesure du possible.

2° Vérifier la politique de filtrage vis-à-vis des serveurs DNS `Microsoft`, et notamment les règles qui concernent le trafic à destination des ports TCP ou UDP 445, 139 et de 1024 à 5000. Si ceux-ci ne sont pas nécessaires, ils doivent être bloqués.

3° Utiliser des outils de surveillance périphériques à jour (renifleurs, ou sondes de détection d'intrusions), et analyser les journaux du serveur, afin de déterminer toute activité suspecte.

6 Solution

Se référer au bulletin de sécurité Microsoft MS07-029 pour l'application des correctifs (cf. Documentation).

7 Documentation

- Avis CERTA-2007-AVI-209 du 09 mai 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-AVI-209/
- Bulletin Microsoft MS07-029 du 08 mai 2007 :
  http://www.microsoft.com/france/technet/security/bulletin/ms07-029.mspx
  http://www.microsoft.com/technet/security/bulletin/ms07-029.mspx
- Avis de sécurité Microsoft 935964 du 12 avril 2007 :
  http://www.microsoft.com/technet/security/advisory/935964.mspx
- Document du CERTA CERTA-2007-ACT-015 du 13 avril 2007 :
  http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-015.pdf
- Alerte de sécurité de l'US-CERT TA07-103A du 13 avril 2007 :
  http://www.us-cert.gov/cas/techalerts/TA07-103A.html
- Référence CVE CVE-2007-1748 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-1748

Gestion détaillée du document

16 avril 2007 version initiale.
20 avril 2007 ajout de la surveillance du port 139/TCP et ajout de la référence au bulletin de sécurité de Microsoft.
09 mai 2007 ajout des références aux bulletins MS07-029 et CERTA-2007-AVI-209.