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 juillet 2008
N° CERTA-2008-AVI-353

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité DNS dans Microsoft Windows

Gestion du document

Référence	CERTA-2008-AVI-353
Titre	Vulnérabilité DNS dans Microsoft Windows
Date de la première version	09 juillet 2008
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS08-037 du 08 juillet 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

Contournement de la politique de sécurité.

2 Systèmes affectés

- Microsoft Windows 2000 Service Pack 4 ;
- Microsoft Windows 2000 Server Service Pack 4 ;
- Microsoft Windows XP Service Pack 2 ;
- Microsoft Windows XP Service Pack 3 ;
- Microsoft XP Professional x64 Edition ;
- Microsoft XP Professional x64 Edition Service Pack 2 ;
- 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 SP1 et SP2 pour systèmes Itanium ;
- Microsoft Windows Server 2008 (systèmes 32-bit et x64).

3 Résumé

Deux vulnérabilités ont été identifiées sur les mises en œuvre DNS sous Windows. Elles impliquent le client ainsi que le serveur. L'exploitation de ces dernières permet sous certaines conditions de corrompre le cache et de rediriger le trafic d'utilisateurs vers des systèmes illégitimes.

4 Description

Deux vulnérabilités ont été identifiées sur les mises en œuvre DNS sous Windows. La première concerne la mise en œuvre des requêtes DNS émises par un client ou un serveur. Le port source étant prévisible, il suffit sous certaines conditions, pour forger une réponse malveillante, de deviner l'identifiant de transaction (dont la génération a fait l'objet d'un correctif décrit dans MS08-020). Cette mesure n'est pas suffisante. Une seconde vulnérabilité concerne l'opération de mise en cache pour le serveur DNS. Ce dernier accepte sous certaines conditions de mettre en cache des réponses malveillantes. Les détails précis de cette vulnérabilité ne sont cependant pas connus à la date de rédaction de cet avis.

5 Solution

Se référer au bulletin de sécurité MS08-037 de Microsoft pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

- Bulletin de sécurité Microsoft MS08-037 du 08 juillet 2008 :
  http://www.microsoft.com/france/technet/security/Bulletin/MS08-037.mspx
  http://www.microsoft.com/technet/security/Bulletin/MS08-037.mspx
- Référence CVE CVE-2008-1447 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1447
- Référence CVE CVE-2008-1454 :
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-1454
- Bloc-notes de Microsoft SVRD, "MS08-037 : More entropy for the DNS resolver" :
  http://blogs.technet.com/swi/archive/2008/07/08/ms08-037-more-entropy-in-the-dns-resolver.aspx

Gestion détaillée du document

09 juillet 2008 version initiale.