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 septembre 2009
N° CERTA-2009-AVI-372

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Multiples vulnérabilités dans TCP/IP sous Windows

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-2009-AVI-372

Gestion du document

Référence	CERTA-2009-AVI-372
Titre	Multiples vulnérabilités dans TCP/IP sous Windows
Date de la première version	09 septembre 2009
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS09-048 du 08 septembre 2009
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 ;
- déni de service à distance.

2 Systèmes affectés

- *Microsoft Windows 2000* Service Pack 4 ;
- *Microsoft Windows 2003* Service Pack 2 ;
- *Microsoft Windows 2003 x64 Edition* Service Pack 2 ;
- *Microsoft Windows 2003 with SP2 for Itanium-based Systems* ;
- *Microsoft Windows Vista* ;
- *Microsoft Windows Vista* Service Pack 1 ;
- *Microsoft Windows Vista* Service Pack 2 ;
- *Microsoft Windows Vista x64 Edition* ;
- *Microsoft Windows Vista x64 Edition* Service Pack 1 ;
- *Microsoft Windows Vista x64 Edition* Service Pack 2 ;
- *Microsoft Windows Server 2008 for 32-bit Systems* ;
- *Microsoft Windows Server 2008 for 32-bit Systems* Service Pack 2 ;

– *Microsoft Windows Server 2008 for x64-based Systems* ;
– *Microsoft Windows Server 2008 for x64-based Systems* Service Pack 2 ;
– *Microsoft Windows Server 2008 for Itanium-based Systems* ;
– *Microsoft Windows Server 2008 for Itanium-based Systems* Service Pack 2.

3 Résumé

De multiples vulnérabilités dans l'implémentation de `TCP/IP` sous *Microsoft Windows* permettent d'exécuter du code arbitraire ou de réaliser un déni de service à distance.

4 Description

De multiples vulnérabilités ont été découvertes dans l'implémentation de `TCP/IP` sous *Microsoft Windows* :

– un déni de service à distance est possible dû à la façon dont *Microsoft Windows* gère un nombre excessif de connexions `TCP`. Cette vulnérabilité est amplifiée lorsque la taille de la fenêtre a une valeur proche de 0 (CVE-2008-4609) ;
– une exécution de code arbitraire à distance est possible car la pile `TCP/IP` de *Microsoft Windows* ne nettoie pas correctement les informations d'état (CVE-2009-1925) ;
– un déni de service à distance est possible du fait d'une erreur dans la gestion des paquets ayant une taille de fenêtre proche de 0 (CVE-2009-1926).

5 Solution

Se référer au bulletin de sécurité *Microsoft* MS09-048 pour l'obtention des correctifs (cf. section Documentation).

6 Documentation

– Bulletin de sécurité Microsoft MS09-048 du 08 septembre 2009 :
http://www.microsoft.com/france/technet/security/Bulletin/MS09-048.mspx
http://www.microsoft.com/technet/security/Bulletin/MS09-048.mspx
– Référence CVE CVE-2008-4609 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4609
– Référence CVE CVE-2009-1925 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1925
– Référence CVE CVE-2009-1926 :
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1926

Gestion détaillée du document

09 septembre 2009 version initiale.